

Regulation of Personal Data Protection and of Reporting Agencies:  
*a Comparison of Selected Countries of Latin America, the United  
States and European Union Countries*

Rafael del Villar  
Alejandro Díaz de León  
Johanna Gil Hubert

First Draft in English

February 2001

## Summary

This paper argues extensively for the development of personal data protection regulatory frames in Latin American countries, based on the principles established by the United Nations Organization, the Organization for Economic Cooperation and Development, and the Council of Europe. In addition, we have found that the United States' experience of over one century and a half with private consumer reporting agencies (herein referred to as Reporting Agencies (RAs)) is particularly significant for the region. Lately some Latin American countries have been promoting personal data protection. These actions should be complemented with regulations that stimulate RAs development.

### 1. Economic aspects

Personal data protection and a person's right to access information about its own person are closely related to individual rights. The benefits a data protection regulation go beyond the individual or consumer whose data are being protected. A regime that properly and effectively protects data, fosters consumers' and firms' confidence in the fair treatment of their personal data, resulting in the expansion of databases and the flow of information to the benefit of non-defaulting consumers and firms as well as the development of the economy. By encouraging the payment of credit and tax obligations, the financial system becomes more stable and tax collection is strengthened.

Consumer credit information and in general all kind of personal data not only help to determine an individual's payment capacity and characteristics, but also affect the overall incentives of economic agents. A consumer is encouraged to meet its obligations when he knows that his noncompliance will be entered into a database that may be accessed — protecting his rights — by several creditors or service suppliers. On the other hand, it is in the interest of non-defaulting consumers that firms or third parties whom they want to deal with have access to their personal data showing that they have duly fulfilled their former obligations. In this way, they will obtain lower prices and better conditions for the purchase of goods and services since firms will incur lower risks and costs. Only consumers who in the past acquired goods or services and have not settled payments due are reluctant to disclose their personal data because it will limit the goods and services they may acquire or raise their prices.

It is inconvenient to set up means enabling the consumer to access his personal data in the possession of data controllers and facilitate its transfer to third parties in order to prove that he complies with his obligations. This would benefit the consumer and encourage competition in the markets. To this end, the RAs are efficient intermediaries between consumers and suppliers of goods and services.

A personal data protection regulatory framework that promotes confidence and the flow of information is quite significant for the financial system because it will stimulate credit development on a healthy basis and make the financial system sounder by encouraging debtors to settle their obligations. This is especially true for Latin America, where the lack

of developed information markets has increased the overdue portfolio and weakened financial institutions, one of the major reasons for panic and recurrent crises. These crises have entailed high social costs, which could have been reduced through strong incentives for the payment of obligations by debtors.

## **2. International Principles On Data Protection Regulation**

The significance of personal data protection regulation has been widely recognized at an international level. 20 years ago, the Organization for Economic Cooperation and Development and the Council of Europe have issued international instruments executed by practically all member countries, with detailed principles on personal data protection. In addition, 10 years ago, the United Nations Organization adopted less detailed but similar principles. These guidelines comprise the information held by both the public and the private sector and are aimed at protecting individual rights and freedom, as well as preventing undue restrictions from being imposed on personal data flow.

Outstanding among the protection principles set forth in those instruments are: (i) the various individual's rights to know, obtain, and dispute his personal information in the possession of data controllers; (ii) limits on data collection, use, and withholding and; (iii) data controllers' obligation to specify the purpose of the processing, keep information quality (accurate and updated), adopt the relevant safety measures, and become liable for the data they control. These organizations recommend countries to enact principles and make them binding and establish proper sanctions and remedies when they are breached.

## **3. Regulatory Frameworks In Latin America, The United States And The European Union**

This section describes regulations and the institutions that support them on personal data protection and RAs available in the United States, the European Union countries and six Latin American countries: Argentina, Brazil, Chile, Colombia, Mexico, and Peru.

First, individuals' right to information and right to privacy set forth in the constitutions of the analyzed Latin American countries are described. Colombian and Peruvian constitutions refer specifically to personal data treatment in connection with individuals' right to privacy. The Argentinean, Brazilian, Chilean, Colombian, and Peruvian constitutions explicitly set forth individuals' right to access and to correct their personal data from public or private databases, and the right to a judicial hearing in the matter of personal data protection (Habeas Data).

The extent of regulations enacted in the analyzed Latin American countries varies considerably. Argentina and Chile have recently approved general personal data protection laws. These laws apply to information held by both the public and private sectors and incorporate the principles and recommendations from the aforementioned international organizations. In addition, they contain several specific provisions on credit information service providers.

As far as the rest of the Latin American countries are concerned, Brazil and Peru have laws regulating the individuals' constitutional access right to information and the Habeas Data.

These countries have public credit bureaus, which in the case of Brazil is operated by the Central Bank and in Peru by the Banking and Insurance Superintendent's Office. It is worth mentioning that Brazil's consumer protection laws contain, too, provisions on consumers' data protection rights. In Colombia there exists a jurisprudence of the Constitutional Court in relation to the Habeas Data. Additionally, financial regulation in that country sets forth certain restrictions on private credit bureaus in connection with data quality, collection, and transfer. In Mexico, regulation focuses on the financial sector and provides for the replacement of the public credit bureau managed by the central bank by a private credit bureau market, and sets forth the process to authorize and operate private credit bureaus.

#### **4. Information Processed And Services Rendered By Credit Bureaus**

The scope of information that may be processed by RAs varies substantially in the analyzed countries. The considerable amount of information handled by RAs in the United States is outstanding (Fair Credit Reporting Act). In the U.S. RAs collect and transfer information on banks and insurance companies, both positive and negative, negative tax information, and other, such as real-estate leasing and personal bankruptcy and insolvency. RAs may collect and transfer individuals' employment, medical and other sensitive data provided they meet additional requirements, such as the consumer's authorization to collect information. Users of the information (agents obtaining the RAs' services) may take no adverse action against the consumer based on the RAs reports until they have delivered a copy of the report to the consumer and advised him of the available means to dispute the data contained in his report (e.g., costless telephone numbers). The RAs in this country may provide services other than those related to credit granting; i.e., they can render services to improve decision making by employers, lessees, and different kinds of service companies.

In Latin American countries the variety of data processed and services provided by these specialized firms are more limited. This is due in part to the sectorial nature of RAs' regulations in these countries. For example, in Mexico credit bureaus are regulated by the financial system laws and may only perform such activities as are aimed at providing information on credits and analogous transactions. In countries like Argentina, Chile, and Peru the scope of data processed by RAs is greater and helps employers, lessees, and financial and non-financial firms to make better decisions. It is worth mentioning that most of the Latin American RAs have started operations relatively recently, especially if compared to the RAs in the United States.

In all the analyzed countries, the RAs may process credit information. In Colombia, Brazil, and Mexico, financial institutions' asset- and liability- related transactions are covered by the "banking secret" (secreto bancario). In Mexico, the responsibility to preserve the banking secret relies on credit bureaus. In Chile the banking secret includes any kind of deposits with banks. The other transactions are subject to reserve and the banks may only disclose them to those proving a legitimate interest and provided it is not anticipated that disclosing the information may cause equity damage to the customer. In Argentina and Peru the banking secret includes only liability- related transactions from the financial system's firms and there are no legal restrictions to obtain or transfer information on asset-related transactions.

It is convenient that RAs process tax information in order to better evaluate individuals and to foster compliance of tax obligations. In the United States, Chile, and Peru, RAs have access to information on defaulting taxpayers. Peru's case is particularly interesting, since the National Tax Administration Superintendent's Office (SUNAT) has entered into a cooperation agreement with private credit bureaus in order to provide them with negative tax information. In return SUNAT has access to information on the financial system and business entities' defaulting customers.

## **5. Actions That A Consumer May Take For His Protection**

A consumer's rights include not only access to data about his person, but also the right to know the recipients of reports on his personal data and to correct this information. In this regard, Brazil, Chile, Colombia, Peru, and the European Union provide the consumer with the right to access and correct information held by any data controller. In the United States the consumer has the right to access and correct information about his person held both by RAs (Fair Credit Reporting Act), and government agencies (Freedom of Information Act). Argentina is in a similar situation to the U.S. since individuals have the constitutional right to access and correct their information from public or private data banks engaged in furnishing reports. In Mexico a consumer's right to access and correct his information is more limited because he does not have the right to get a report about his person even from credit bureaus. Argentina, Chile and Colombia, as well as the United States and the European Union, do also let the consumer know the recipients of information reports on his personal data. In Colombia and the United States this right is restrained to private RAs (in the case of Colombia it only applies to credit bureaus), while in Chile and the European Union this right may be enforced before any data controller.

## **6. Regulation Of Reporting Agencies.**

The development of RAs depends on consumers and firms' confidence in the fairness and proper use of the information contained in their databases. Without the confidence of consumers and data controllers' RAs database development and use would be quite limited. Regulatory and institutional frameworks are essential to create confidence on this market. Consequently, because of the demand by consumer groups and firms for quality and fair treatment of information, the United States has repeatedly amended the Fair Credit Reporting Act.

## **7. Institutional Frameworks**

There is a wide range of designs in the analyzed countries concerning institutions in charge of supervising data protection and RAs development. In the United States, courts play a major role in settling all kinds of disputes, especially those arising in connection with public databases (Freedom of Information Act). Concerning private RAs regulation, there are several competent administrative authorities for the enforcement of the law (Fair Credit Reporting Act), outstanding among which are consumer protection and financial system authorities, among other sectorial authorities. In the European Union, national Personal Data Protection laws are enforced, in the first place, by national control authorities specialized in personal data protection.

The enforcement of data protection in Chile (1999) has been fully entrusted to courts. Pursuant to the new Argentinean law (2000), the administrative control authority has broad powers and faculties similar to those of national control authorities in Europe. Nonetheless, this body lacks independence or even functional autonomy and it is not clear that it has enough resources to effectively comply with its responsibilities. In Brazil, the Consumer Protection and Defense Department of the Ministry of Justice receives and responds to inquiries and claims filed by consumers owing to violations to their personal data rights and has the power to punish data controllers. In Mexico there are four financial system authorities who may intervene on cases involving credit bureaus (Secretaría de Hacienda y Crédito Público (Finance Secretariat), Banco de México, la Comisión Nacional Bancaria y de Valores (National Banking and Securities Commission) y la Comisión Nacional de protección y defensa de los usuarios de los servicios financieros (National Commission for the protection and defense of financial services users). Interpretations on authorities' functions overlap and create power vacuums. In Colombia the Constitutional Court has settled disputes and construed and developed the major regulations on personal data protection through judgments. Despite the above, the Banking Superintendent's Office has played a major role.

## I.- Introduction

For the provision of goods and services and, in general, the conduction of economic transactions, the availability of appropriate information on the involved parties is very helpful. This results in less expensive and risky contracts. Therefore, both goods and services providers and consumers benefit by operating with better information.

The existence of and access to individuals' information is an essential tool to:

- (i) improve (political, social, and business) decision making ;
- (ii) encourage settling debts and complying with all kinds of obligations
- (iii) foster the economy's development, rise productivity, reduce prices and favor the provision of new services (ignoring individuals' relevant and truthful information hampers and increases the risk in making decisions);
- (iv) reduce transaction costs incurred by agents requiring this kind of information; otherwise they have to use more expensive mechanisms to obtain, complete and make information more accurate; and
- (v) encourage domestic and international trade.

When the role of personal data in the economy is analyzed, two fundamental concerns must be considered: privacy protection and the free flow of information. The free flow of information is clearly related to individual rights to freedom of speech and freedom of the press. Besides, the protection of personal information contained in databases bears on the individual right to privacy.

Efforts made to strengthen and preserve the individual's privacy may limit the efficient performance of the economy which requires the flow of information. In this regard, laws and regulations on personal databases must seek privacy protection and at the same time encourage the flow of information that will benefit both consumers and service firms. There seems to be a permanent conflict between these two targets, but it is not so. Although protecting privacy creates real costs for firms, personal data protection fosters consumer and firms' confidence that information will not be unfairly used, thus driving the development of personal databases, which supports the flow of information and a better decision-making process throughout the economy. We must bear in mind that firms incur in large costs when making decisions without updated, truthful and complete information.

Three international instruments on personal data protection are most noteworthy: the guidelines from the Organization for Economic Cooperation and Development (OECD), the Council of Europe Convention, and the United Nations Guidelines. Despite the fact that personal data processing seems to be a new subject owing to the development of communications media, such as the Internet and electronic commerce, the aforementioned instruments are not recent. The OECD and the Council of Europe guidelines were issued early in the eighties, while the United Nations guidelines date back to the early nineties.

Subsequently, current regulations and institution bearing on personal data protection and RAs in six Latin American countries: Argentina, Brazil, Chile, Colombia, Mexico, and Peru are compared. The comparison is strengthened by examining the regulations and institutions in the European Union and the United States, a block of countries with whom Latin American countries keep very close trade and economic cooperation relationships.

## **II.- Economic Considerations On The Treatment Of Personal Data And The Operation Of Reporting Agencies.**

### **II.1.- Non-Defaulting Consumers Want To Disclose Personal Data That Show They Pay Their Obligations**

In order to obtain goods and services at lower prices and under better terms and conditions, consumers try to prove that they are trustful and non-defaulting individuals. A manner of proving it is submitting information on the compliance with conditions agreed upon in previous agreements. The fact that goods and services providers have this kind of information about their consumers in databases would be used to benefit those consumers that do not default. These consumers try to transfer such information to creditors and suppliers, to prove they are trustful (reputation)<sup>1</sup>. If the consumer has the right to request a copy of his personal information in the possession of data controllers (firms), he will find it easier to prove his past performance.

A consumer's right to request both to firms and the government information on the record of his operations is essential. Besides giving the individual the right to modify incorrect or mistaken personal data, to avoid being unfairly discriminated, these rights enable the consumer to use his personal data contained in different databases to engage in transactions for his own benefit.<sup>2</sup> The effectiveness of this right depends on the establishment of expedite and simple mechanisms for consumers to exercise such rights directly or through third parties. Therefore, a simple, accessible and low-cost process must be set up for consumers which, at the same time, is not unduly expensive for firms.

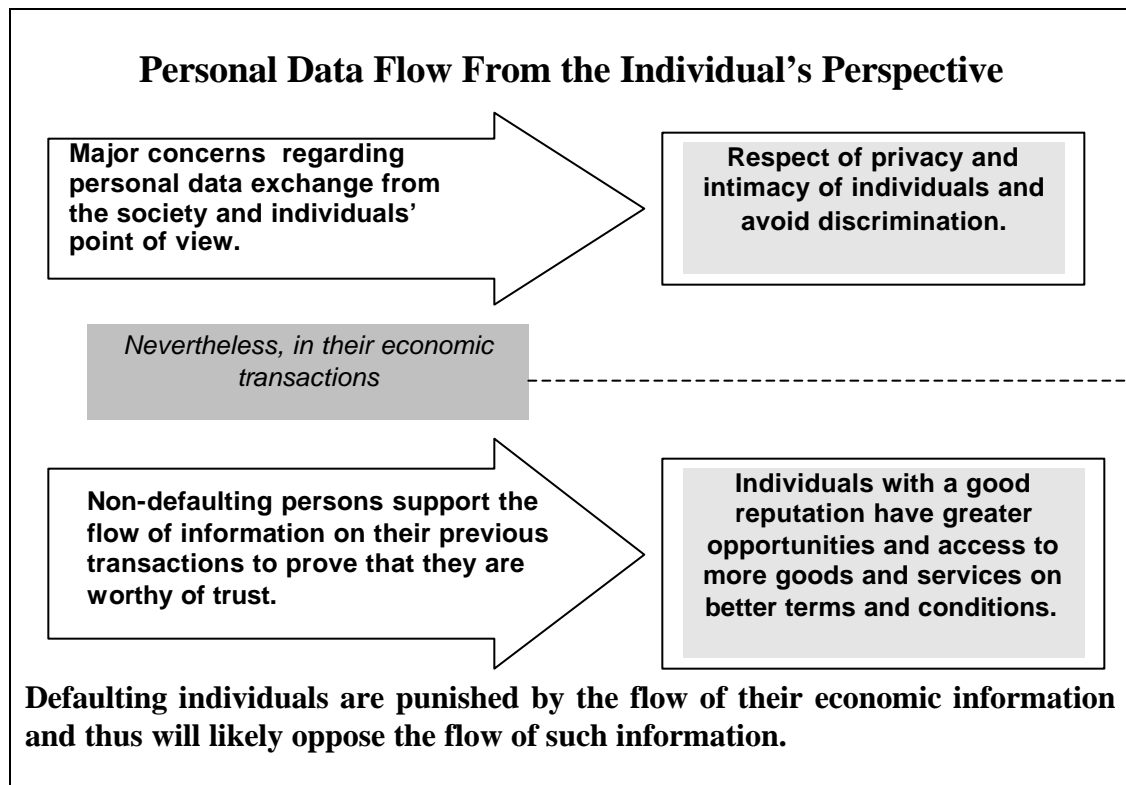
The recognition that consumers have this right, encourages competition and economic efficiency, since an increase in the flow of consumer information lowers an important market barrier entry to new providers of goods and services.

---

<sup>1</sup> Generally only defaulting consumers try to avoid making their credit record known so that they may receive a better treatment than the one they would receive should they disclose their real record.

<sup>2</sup> This does not intend to give consumers the control to eliminate or suppress information at their will, which would have serious repercussions on the quality and use of information, but rather to give them the possibility to be benefited by such information.

**Table 1**



There is a potentially large personal information market that could allow consumers prove their past record. The firms on this market referred to as RAs (Reporting agencies) specialize in collecting and processing information from various sources. It is only natural for RAs to act as intermediaries between the consumer and firms controlling personal databases. In this regard, it is a must that authorities in charge of enforcing data protection compel controllers to observe their obligation to deliver information to consumers.

RAs have a very important social function:

1. RAs reports have a broad credibility because their databases are impartially built. Consumers, on the other hand, have a clear incentive to assemble and transfer only that information which most favors them.
2. Allowing RAs to request consumer information to any data controller favors the integration of such information in complete files.
3. RAs are in a better condition than consumers to determine whether or not to request specific reports to data controllers because they know better information needs of potential receivers or users of the information.

4. RAs add value in many ways. For instance, the manner in which they present the information enables the receiver to more easily evaluate a given consumer.

5. For data controllers sharing information with RAs has many advantages. They may avoid satisfying a large number of individual requests and, besides, they may access RAs services under better conditions since rates and access to services provided by the RAs are more favorable for firms that share their data bases with these agencies.

## **II.2.- Sharing Customer Information Between Firms**

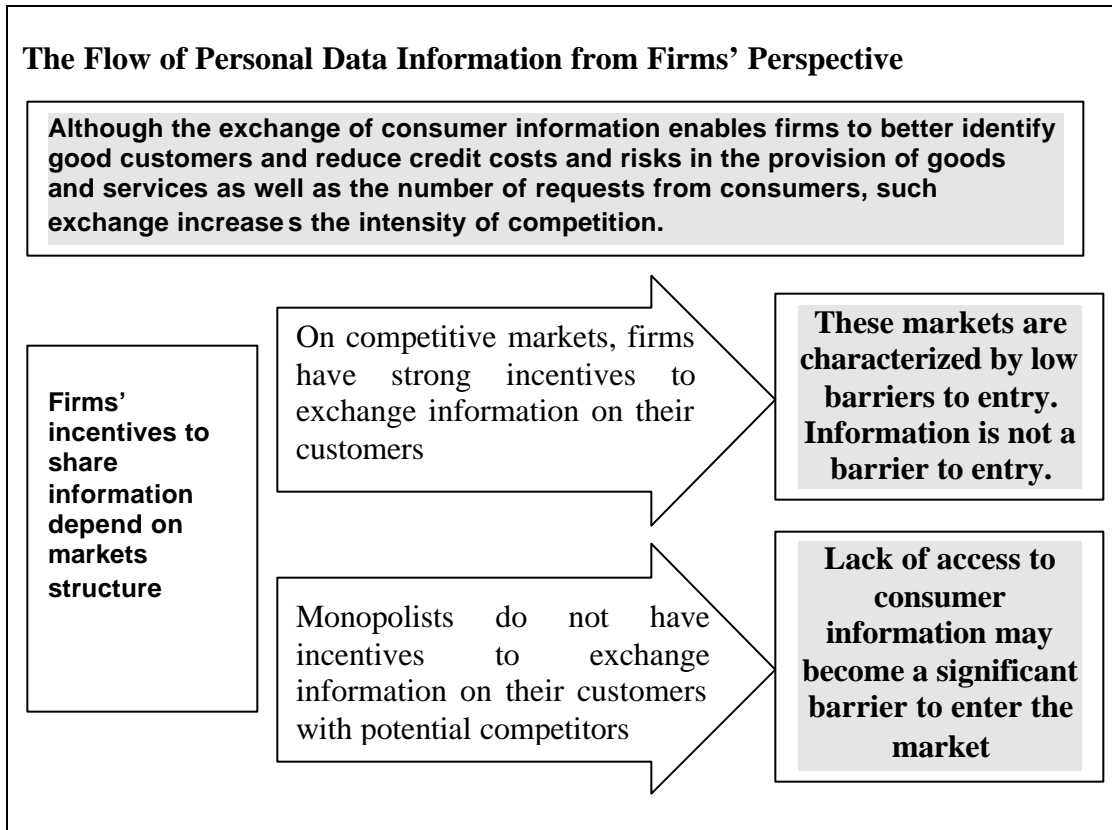
In order to evaluate potential customers firms want to obtain information other than that contained in their own database. Firms look for non-defaulting consumers to reduce risk and increase profitability. Thus, it is only natural that firms seek to share customer information resulting in better decision-making. Because having better information available enables firms to reward non-defaulting consumers and punish defaulting consumers, sharing information induces consumers to avoid default. The reduction in the default rate results in the expansion of markets.

Despite the above, the sharing of information by firms tends to increase competition in the markets and to customer reduce income received from the exclusive use of such information. Therefore, incentives to share information are influenced by the structure of the markets on which firms operate. A market with high competition has a higher incentive to share information between firms with the same or similar economic activity, while on monopolistic markets, the prevailing incentive is generally not to share information. Because Latin American economies are characterized by high concentration levels in many sectors, market concentration is probably a factor inhibiting the development of RAs and the sharing of databases in the region.<sup>3</sup>.

---

<sup>3</sup> Another factor is people relatively low mobility [ITALIAN QUOTE].

**Table 2**



It is worth to mention that in promoting competition in sectors like telecommunications, gas and electricity, dominant firms are frequently forced to share negative information with their competitors because otherwise, defaulting or fraudulent consumers would be able to switch their suppliers without having complied with previously agreed upon obligations, in detriment of the companies in the market.

There is little doubt that sharing information on defaults helps companies reduce risks and generally leads to a greater economic efficiency. The benefits of sharing positive information, information on non-defaulting consumers are less clear. To better evaluate the additional borrowing capacity of a consumer it is convenient to share the level of “debt” the consumer has with different firms. However, sharing information on contracted rates, may cause firms to collude.

\* \* \*

RAs, i.e., firms specialized in reporting on consumers are natural intermediaries between information needs of both consumers and firms. In some countries — in the United States but also in some Latin American countries like Argentina and Chile — RAs have been able to set up broad databases because their operation has gained consumer and users’ confidence. This is partially due to data protection rules that limit the indiscriminate

transfer of such information to third parties. An appropriate regulation should be consistent with a healthy market competition between firms. Given the high concentration of markets in Latin America the sharing of customer information between firms and the development of RAs is not assumed.

## **II.3.- Reporting Agencies And Their Market Structure**

### **II.3.1.- The significance of Reporting Agencies and mainly credit bureaus market development in Latin America**

It is particularly important to promote RAs development since deficient laws<sup>4</sup> and institutions in some countries in the region have caused the proliferation of the “No Pay Culture”. This has resulted in the underdevelopment of the financial system in these countries and in a limited tax collection capacity by these countries’ governments.

### **II.3.2.- Main Factors For The Development Of A Reporting Agencies Market**

In what follows we discuss the factors contributing to the development of RAs.

#### **1. Setting Up An economy Wide Regulation For Data Protection And The Development of RAs**

A data protection regulation that is generally applied to the different sectors of the economy, promotes consistency, the aggregation of information and that RAs provide a greater range of services. In addition, a general regulatory frame abates judicial uncertainty. These conditions incent larger investments in the provision of RAs services.

#### **2. Eliminating Barriers To RAs’ Establishment And Operation And Promoting Competition Between RAs**

Regulatory barriers, provisions hampering RAs’ setting up and operating, are, for instance, expensive, slow or discretionary authorization and/or registration requirements, a regulation inconsistent with modern administration of electronic data files and, in general, an excessive RAs regulation. Although it could be argued that discretionary authorizations for the RAs are justified by fears of misuse of such information we feel that a data protection law is sufficient to protect consumers.

Competition between RAs has significant advantages for the development of both RAs market and the overall economy. RAs compete at different dimensions: price, service, quality, and reputation. Competition between RAs tends to bring benefits in all these dimensions. However, in some Latin American countries dominant RAs have become monopolists.

---

<sup>4</sup> Such is the case of bankruptcy laws and rules on guaranty performance.

### **3. Authorities' Supervision Of RAs**

Authorities' actions should be oriented to create the public's confidence in RAs by timely and efficiently attending consumers' complaints and effectively punishing illegal practices by RAs and/or the users of the information.

### **4. Information Universe To Which RAs Have Access**

It is convenient that RAs have access to personal data held by the public and private sector. The public sector, particularly tax authorities, is a significant potential beneficiary of services provided by RAs. Processing information on defaulting or fraudulent taxpayers encourages individuals compliance with their tax obligations.

### **5. Development of a Nationwide Identification System**

Having a national identification system, like a single social security number for each person, increases the quality of the service provided by the RAs by reducing their mistakes.

## **II.3.3.- Particular Considerations For The Development Of The Credit Bureau Market**

### **1. Significance Of The Impartial Use Of Information By Credit Bureaus**

Because credit bureaus' databases contain information from competing companies or suppliers, the providers of information to these RAs must be guaranteed of the impartial use of information. The mere possibility that a credit bureau favors one company over another in accessing information, discourages the participation in the bureau of the companies that believe they may be discriminated. This factor limits the capacity of credit bureaus to assemble data bases.

Confidence in the bureau increases when the control of the bureau lies on companies that are not themselves users of the information it processes. This corporative structure ensues the best development of the RA market. In addition, since in this situation there are no inherent "conflicts of interest", a less intense regulation and supervision by authorities is necessary, since the likelihood that RAs will have biased operations is practically eliminated.

Despite the clear advantages of this corporative structure, in Brazil and Mexico credit bureaus have been set up by the main banks, which enjoy a dominant position. Following are some explanations of this phenomenon.

1. Banks consider that credit information they hold belongs to them and thus they have the right to control it.
2. Banks integrate into a credit bureau to protect their databases from misuse.
3. Control of the credit bureau is a way to protect banks against potential non-bank competitors.

We believe that the first two arguments would loose validity if a general data protection regulation would be established. Establishing a proper regulatory framework encourages

the development of private credit bureaus by establishing the required conditions to build consumers and users confidence in their operation.

The third explanation of why banks are vertically integrated into credit bureaus will not vanish with the establishment of a proper regulatory framework. As already mentioned, the high economic concentration level in Latin America in several economic sectors discourages the flow of information. This situation must be fought since vertical integration of banks into the credit bureau unnecessarily limits the flow of information in the economy due to three reasons:

- i) The likelihood of the bureau giving preference to banks discourages non-banks becoming a provider or user thereof. This reduces the bureau's capacity to collect broad databases and unnecessarily limits the quality of services offered.
- ii) There is a trend to monopolize the credit bureau market, since banks are reluctant to provide their data bases to bureaus different from their own.
- iii) Distrustful companies that decide not to become users of the banks' credit bureau is either create their own sectorial bureau or continue operating without sharing information.

The effects of vertical integration may be partially counteracted through several actions.

#### **a) Sharing of Certain Information Between Credit Bureaus**

A regulatory measure adopted by authorities in Mexico as a result of banks vertical integration into the credit bureau is to require the sharing of a subset of negative information among bureaus, in order to avoid the market's monopolization of databases arising out of the fact that banks decide to furnish information only to their own bureau. This regulation did not have the desired effect since it was applied late and the information ultimately shared was a small fraction of negative information<sup>5</sup>. The bureau constituted by banks has consolidated to become the sole private credit bureau in this country after two of the three major bureaus in the United States, TRW (currently Experian) and Equifax abandoned the market in 1997 and early in 2000, respectively.

---

<sup>5</sup> Negative information shared is a subset of overdue portfolio information. In the 1997 amendment to the "Reglas Generales a que deberán sujetarse las sociedades de información crediticia a que se refiere el artículo 33 de la Ley para Regular las Agrupaciones Financieras" (General Rules to which credit information associations must be subject set forth in Article 33 of the Law to Regulate Financial Groups), the Finance Secretariat replaced the obligation to share **overdue portfolio information** with the obligation to share **overdue portfolio-related information**. Pursuant to this change, the database that must be exchanged among credit bureaus is significantly lower than the overdue portfolio database because:

- i) For credit card loans (revolving credit) only information on the customer who has failed to make the minimum required payment for 120 calendar days must be shared. (While overdue portfolio is considered that of customers who have not made the minimum required payment for 2 or more invoicing periods; i.e., 60 days);
- ii) For housing loans, information on borrowers must be shared only following 180 calendar days after the due date of the first unpaid amortization. (While overdue portfolio is considered following 90 calendar days after the due date of the first unpaid amortization);
- iii) For the acquisition of durable consumer goods, information on the borrowers must be shared only following 120 calendar days after the due date of the first unpaid amortization, rather than following 90 calendar days as established in the overdue portfolio regulation.

Forcing bureaus to share information among them has major disadvantages. On the one hand, in practice it is difficult for competitors to share information in time and form. On the other hand, there is a free rider problem since in transferring part of their databases to competitors, bureaus benefit their competitors who get a data base for “free”. This tends to diminish bureaus’ efforts to set up databases and may thereby inhibit the market’s development.

***b) Right To Consultation At Wholesale Prices Among RAs***

A measure fostering the development of the credit bureau market is the consultation right among bureaus. This regulation enables a bureau having a small to efficiently compete with larger bureaus.

Rates for these consultation must not be higher than the rates offered by the bureaus to their main users. This is a rule to determine resale rates, which is commonly used in other industries and we consider equally valid to apply it in this context.

***c) Banks Disinvest the Equity Interests they have in Credit Bureaus***

As mentioned before, an effective way to eliminate the “conflicts of interest” of a bureau owned by banks is to prevent banks from having an equity relationship with credit bureaus.

### **III.- Regulatory Framework of Data Protection**

#### ***III.1.- Multinational Organizations Guidelines***

We review personal data protection principles contained in three instrumentalities of multinational organizations, the OECD Guidelines, the Council of Europe Convention, and the United Nations Guidelines. We have also included the analysis of the Canadian Standard Association Model Code for the Protection of Personal Information. These instrumentalities are not recent as the development of communications media such as the Internet would imply: the OECD Guidelines and the Council of Europe Convention were issued in the early eighties while the United Nations Guidelines were published in the early nineties. There is a striking coincidence of the objectives and principles set out in these guidelines.

**Table 3**  
**International Instrumentalities for Personal Data Protection**

	September 1980 <i>OECD</i>	1981 <i>Council of Europe</i>	December 1990 <i>United Nations Organization</i>	March 1996 <i>Canadian Standard Association</i>
<b>International Instrument</b>	<b>Guidelines for Privacy and Transborder Personal Data Flow Protection</b>	<b>Convention for Individuals' Protection in relation to Personal Data Automated Processing</b>	<b>Guidelines for Personal Data Automated Files</b>	<b>Model Code for Personal Data Protection</b>
<b>Scope</b>				
Personal Data	X	X	X	X
Public Sector	X	X	X	
Private Sector	X	X	X	X
<b>Objectives</b>				
Protect privacy and individual freedom	X	X	X	X
Facilitate free personal data flow	X	X	X	X
<b>Principles</b>				
1. Consumer right to access and correction	X	X	X	X
2. Identifying Purposes	X	X	X	X
3. Limiting Collection	X	X	X	X
4. Limiting Use	X	X	X	X
5. Limiting the Withholding of Data	X	X	X	X
6. Data quality; accurate and up-to-date	X	X	X	X
7. Security Measures	X	X	X	X
8. Sanctions and remedies in national laws	X	X	X	
9. Data controllers' accountability	X			X
10. Openness	X			X
11. Exceptions		X	X	

## **1. Consumer or Subject Rights**

An individual must have the right to:

- a) obtain from a data controller, or his representative, the confirmation that he has data related to him;
- b) be informed by the data controller of any individual's personal data item in his possession, as follows:
  - I. Within a reasonable period of time;
  - II. At a reasonable cost, if any;
  - III. In a reasonable way;
  - IV. In a manner clearly intelligible for the individual;
- c) be informed of the reasons why any of the requests made under paragraphs a) and b) is rejected and be able to dispute it;
- d) dispute data related to him, and if such dispute is successful, erase, correct, complete or modify such data.

Individuals' right to access and dispute personal data is one of the most important steps toward privacy protection. Data disputes may be settled with the data collector or brought before a court, an administrative or professional organization or any other institution, pursuant to national regulations.

## **2. Identifying Purposes**

The purpose for which personal data are collected must be specified at or before the time the information is assembled and the subsequent use must be limited to achieve such purpose or any other that is not inconsistent with the former one, and every change in the purpose must also be specified. Furthermore, data must only include information required for the purposes for which the data will be used. No new purposes must be arbitrarily introduced; freedom to make changes must involve consistency with the original purposes.

## **3. Limiting Collection**

Limits must be imposed on personal data collection; any data item must be obtained by lawful and fair means and, when appropriate, with the previous knowledge or consent of the data subject.

Personal data disclosing the individual's racial origin, political or religious opinions or other beliefs, as well as personal data on his health or sexual life may not be automatically processed, unless the national law provides for the appropriate security measures.

## **4. Limiting Use And Transfer**

Personal data must not be disclosed, made available or used for purposes other than those specified, excluding:

- a) upon previous consent of the data subject; or
- b) by operation of law.

## **5. Limiting Data Withholding**

It may be required to erase data in order to protect the consumer or when the data are not suitable any more for the purposes for which they were collected.

## **6. Data Quality; Accurate And Up-to-date**

Personal data must be accurate, complete, and up-to-date.

## **7. Security Measures**

Reasonable security measures must be used to protect personal data against risks like loss, non-authorized access, destruction, use, data modification or disclosure. Safety measures may be physical (identification cards), organizational (different level access to data), or computational.

## **8. Sanctions and Remedies**

*Each country shall cause the appropriate sanctions and remedies to be established against any breach of the laws, so that the basic data protection principles established herein are complied with.*

## **9. Data Controller's Accountability**

The data controller is accountable for the personal information he possesses and for the compliance with these principles and laws as well as decisions made for privacy protection. The data controller is not released from this responsibility upon transferring his information for processing to a third party.

Outstanding among Canadian standards are:

- a) The data controller must designate one or more individuals to supervise the compliance with the principles within that organization.
- b) Upon express request, the identity of individuals appointed to supervise the compliance with the principles must be made publicly known.

## **10. Openness**

The data controller must pursue a transparent policy by making specific information on the developments, policies, and practices relative to personal data management readily available to individuals. Besides, devices for an individual to be aware of the existence and nature of the individual's personal data and the main purposes for which they will be used as well as the data controller's identity and address must be set up.

## **11. Exceptions**

Exceptions to the implementation of these principles are authorized provided they are required to protect national security, public order, the morale, or public health.

\* \* \*

The description of the main international guidelines on personal data protection and the Code of the Canadian Standard Association (CSA) make evident the remarkable similarities between the principles and objectives required to succeed in protecting privacy and promoting personal data flow. In addition, the joint recommendation to enact laws nationwide to attain such objectives must be stressed.

## ***III.2.- Database Protection in the United States, the European Union And Latin America***

Following is a detailed description of personal data protection regulation objectives, scope, and other characteristics in different Latin American countries (Argentina, Brazil, Chile,

Colombia, Mexico, and Peru). This description incorporates as a reference the United States and the European Union.

### **III.2.1 Rights Established in the Constitutions**

At a constitutional level there are three main individuals' fundamental guarantees closely related to personal data protection (See Table 4).

#### ***1.- Right to Privacy***

This right includes an individual's right not to be disturbed in his private life and the right of respect of his honor, image or good name, as well as of confidentiality and inviolability of his communications and private documents. Constitutions of all the analyzed countries guarantee this right on a general basis. Additionally, constitutions in some countries explicitly set forth that the right to privacy involves personal data. Thus, in the Colombian and Peruvian constitutions, the fact that data treatment must respect a person's privacy is explicitly established.

#### ***2.- Individual's Right to Access and Correct his Information held by any Data Controller***

In some countries, the constitution explicitly sets forth people's right to know, update, and correct personal information collected by any public or private data bank. Such is the case in Brazil and Colombia. The Constitution of Argentina provides for this right in relation to public data banks, and certain private data banks, namely those furnishers of reports. The Constitutions of Chile and Peru set forth that any and all persons affected by inaccurate statements in any social communication media has the right to a free correction. The Peruvian constitution further establishes the individual's right to access the information required from any public institution without specifying any reason. The Constitutions of Mexico and the United States do not explicitly refer to this subject.

#### ***3.- Individual's Entitlement to bring a Claim for the Protection of his Rights relative to Personal Data Treatment before a Court. (Habeas Data)***

In order to guarantee the observance of constitutional rights relative to personal data treatment, the Argentinean, Brazilian, Chilean, and Peruvian constitutions provide for an expedite judicial action. Such action may be brought by a natural person to defend his right to privacy and to access and correct his personal data. It is worth to mention that even though the Colombian constitution does not explicitly set forth the Habeas Data, the Article 86 provides for the "guardianship", which is a preferential and summary proceeding (the "guardianship" must be resolved within 10 days following the date on which is was claimed), used extensively by Colombians to request the modification or elimination of their personal data reported in credit bureaus.

**Table 4**  
**Constitutional Grounds**

	Argentina	Brazil	Chile	Colombia	Mexico	Peru	United States
<b>1) Right to Privacy</b>							
General Principle of Intimacy or Privacy	YES Art. 19	YES Art. 5, X	YES Art. 19 paragraph 4 and 5	YES Art. 15 and 21	YES Art. 7	YES Art. 2 paragraph 5 and 7	YES 1st amendment
Specific reference to individuals' data treatment and information	NO	NO	NO	YES Art. 15	NO	YES Art.2 paragraph 6	NO
<b>2) Individual's right to access and correct information in the possession of any data controller</b>	In any public data bank, and in private reporting banks. Art. 43	YES Art. 5 XIV and XXXIII	NO	YES Art. 15	NO	Only in public data banks Art. 2 paragraph 5	NO
<b>3) Right to a Judicial Hearing on personal data (Habeas Data)</b>	YES Art. 43	YES Art. 5, LXXII	YES Art. 20	YES Art. 15	NO	YES Art. 200	NO

### III.2.2 Data Protection Enactment and Objectives in the Analyzed Countries

Data protection enactment levels vary greatly in the analyzed countries. Countries with a general personal data protection law are the European Union nations and Argentina and Chile in Latin America .

The European Union Directive is built on the principles adopted by multinational organizations discussed above. This directive establishes a general law framework comprising databases held both by the public and the private sector. A large number of private sector institutions have to comply with these provisions because they govern personal data treatment by any database controller<sup>6</sup>, excluding activities beyond the scope of the Community Law, such as national security and criminal law, and data treatment by a natural person exercising personal or household activities. Nevertheless, it does not specifically regulate the RAs functioning and operation, which may reflect the fact that credit bureaus are relatively recent in Europe

The United States lacks a general data protection law but it has issued several acts related to these issues like the Freedom of Information Act, the Fair Credit Reporting Act<sup>7</sup> of 1971

<sup>6</sup> In the European Union, personal data treatment is defined as: “any operation or set of operations whether or not conducted through automated procedures and applied to personal data, such as collection, registration, organization, conservation, preparing or modification, extraction, consultation, use, communication through transfer, diffusion or any other form facilitating access to them, comparison or interconnection, as well as the blocking, suppression or destruction thereof.”

<sup>7</sup> Outstanding among the myriad statutes in the United States relative to personal data protection are the Fair Credit Reporting Act (FCRA) of 1971, whose main objectives are: i) Protect privacy of consumer report information; ii) Guarantee that information offered by the RAs (referred to in the FCRA as

and acts regarding privacy in the financial system, mainly Title V of the Gramm-Leach-Bliley Act of 1999 and the Financial Information Privacy Protection Act of 2000 that amends the Gramm-Leach-Bliley Act. The objectives of privacy regulation in the United States and data protection regulation in the European Union<sup>8</sup> are focused not only on privacy protection, but also on supporting trade and on improving the functioning of markets, through the promotion of the flow of information. In the European Union the latter basically operates by eliminating barriers to the flow of information among the Union countries and the nations that are willing to protect data at a level similar to the Union's. In the United States, people's rights to information privacy has not been as meaningful as in Europe, while RAs development has been far greater.

It is worth stressing that the FCRA — which has been amended many times — regulates the consumer reporting private industry, which makes all kinds of reports on individuals. This industry includes credit bureaus. It is worth to stress that in the United States the term consumer information comprises besides financial information, data on employment, health, leasing, etc. The consumer reporting agency concept used in the FCRA includes basically any firm selling consumer information services.<sup>9</sup>

Regardless of the above, with the lack of a general data protection law that may apply to any data controller there is no universal right in the United States for a natural person to access and correct his information in the possession of any private database controller.

Argentina and Chile, the Latin American countries that have made an effort to enact on the subject through a general law like in the European Union, have focused on the protection of individual freedom and people's fundamental rights (privacy). The Chilean Natural Person Data Protection Law<sup>10</sup> of 1999 and the Argentinean law of October 2000<sup>11</sup> do not explicitly pursue the objective of supporting businesses. Like the European Union Directive, the Chilean law includes all data controllers in the public and private sector, while the Argentinean law includes the public and private sector only in respect to RAs databases.

---

*“consumer reporting agencies”) is as truthful and accurate as possible and iii) Encourage the RAs to adopt reasonable procedures to support business by enabling credit flow, personal hiring decisions, insurance and other information needs, so that information furnished by the RAs is fair for the consumer and the confidentiality, truthfulness, relevance and appropriate use thereof are respected.*

<sup>8</sup> *The European Union Directive (1995) goals are: i) protection of individuals' freedom and fundamental rights and, particularly, the right to privacy, relative to personal data treatment and; ii) member states may not restrain or forbid free personal data flow among member states owing to reasons related with people's and privacy protection, because it is guaranteed by this directive.*

<sup>9</sup> The concept of Reporting Agencies (RAs) used in this paper is similar to consumer reporting agencies in the FCRA.

<sup>10</sup> In Chile the Natural Person Data Protection Law (1999) proposes to adequately protect individuals in relation to the right to privacy, by preventing eventual unlawful intromission that may affect them through the regulation of the use by third parties of their personal data. In the Preliminary Title, Article 1 sets forth that “Any person may treat personal data... But in any case the full exercise of data owners fundamental rights must be respected.”

<sup>11</sup> The purpose of the law is the full protection of personal data recorded in files, records, data banks or other data treatment technical media, both public or private, aimed at giving information to guarantee the right to peoples' honor and privacy, as well as access to personal information, in accordance with Article 43, Paragraph three of the National Constitution (which refers to Habeas Data).

Additionally, Chile and Argentina have particular provisions for the financial sector, in both countries authorities (Banking Superintendent's Office in the case of Chile, Central Bank in the case of Argentina) keep a debtor record. The rest of the analyzed Latin American countries – Brazil, Colombia, Mexico, and Peru – do not have a personal data protection law, but they have some sectorial standards on the subject. Following is a description of the general characteristics of legal provisions in the United States, the European Union, and the six analyzed Latin American countries.

### **III.2.3 Legal and Regulatory Scope**

The regulation may include the private sector, the public sector or both. Also, when the regulation includes the private sector it may be general if it is applied to all the sectors and industries or it may be focused on a particular sector.

Regulation in the United States has been evolving from judicial decisions and disputes arising from RAs operation. Therefore, the laws have been assimilating these experiences in two ways: access to public sector personal databases through the Freedom of Information Act (FOIA) and personal data processing by consumer reporting agencies through the Fair Credit Reporting Act (FCRA).

The United State has several sectorial provisions on personal data protection as well. The Gramm-Leach-Bliley and Financial Information Privacy Protection Acts regulate individuals' data protection in their transactions with financial institutions, banks, insurance companies, etc. These acts contain various provisions that are worth to stress. They give the financial system users the right to access and correct their personal information, establish the consumer right to oppose, in certain circumstances, the disclosing of their non-public personal data by financial institutions, and restrict information on individuals' consumer patterns. These acts considerably stress financial institutions self-regulation by allowing them to define their policy on non-public customer information transfer, and may be penalized when they do not submit to said policy. In addition, they direct the conduction of research on the impact of information exchange between affiliates on privacy, and create a stringent regime for fraudulent access to financial information.

The Social Security Act with a chapter on privacy of medical information is among the other various sectorial laws on privacy in the United States. Despite lacking a general law, the United States is the country with the most developed RAs market resulting in a flow of information in the economy and the conduction of all kind of transaction turning them into a significant factor in the economic progress.

The scope of the regulation in the rest of the analyzed Latin American countries varies considerably. Besides the constitutional provision, Brazil's 9.507 Common Law (published on 11/12/97) regulates the right to access information as well as the Habeas Data proceeding providing for the terms to access and correct data as well as judicial proceedings. Additionally, its Consumer Protection and Defense Code, Articles 43 and 44, provide for certain rules and rights regarding information found in databanks or consumer

records.<sup>12</sup> Furthermore, Brazil has a Credit Risk Central Office operated by the Central Bank.

Peru has a constitutional provision governing the Habeas Data applied to the private and public sectors. Additionally, this country has statutes on the financial sector<sup>13</sup> governing the Risk Central Office of the Banking Superintendent's Office and authorizing the creation of private risk central offices. Such laws force financial institutions and insurance companies to periodically and timely furnish the relevant information.

In Colombia, there is jurisprudence from the Constitutional Court regarding the Habeas Data constitutional right. This country has a law similar to the U.S. Freedom of Information Act, the 57 Law of 1985, which aims at enabling the public to know and learn about the handling of public affairs and exercising an efficient control on authorities' behavior, provides for access to official acts and documents information.

The kind of banking information that may be recorded and released by credit bureaus in Colombia are data deemed relevant for the evaluation of the creditworthiness of data owners, pursuant to the Banking Superintendent's Office and in accordance with Article 15 of the Constitution. The Superintendent's Office supplies credit bureaus with information related to people's indebtedness assessment and ranking at financial sector institutions. In turn, the Superintendent's Office receives from banks additional information on the behavior of the financial system users; for example, real-estate information on lessees' payment habits, etc.

Mexico lacks Habeas Data laws as well as access to information controlled by the public sector. It has a few provisions on data protection. The financial sector provisions govern credit bureau transactions and the credit information they obtain, both from individuals and corporations. Additionally, sectorial provisions on personal data have started to be

---

<sup>12</sup> The DISPOE SOBRE A PROTECAO DO CONSUMIDOR E DA OUTRAS PROVIDENCIAS of September 1990, Article 43, sets forth:

- (1) Consumer right to access to information of real-estate official records, records, personal and consumer data filed on him as well as on the respective sources thereof;
- (2) Real-estate official records, records, personal and consumer data filed on him must be objective, clear and truthful and expressed in an easily comprehensible language, and no negative information may be withheld beyond five years;
- (3) When real-estate official records, records or personal or consumer data are released without the consumer's request, he must be notified in writing of the release;
- (4) Whenever the consumer finds any inaccuracy on his personal data and real-estate records, he may demand the immediate correction thereof, and the person in charge of the database (file clerk) must notify of the changes within 5 business days to the receivers of inaccurate data;
- (5) Whenever the consumer finds any inaccuracy in his data or real-estate records, may demand the immediate correction thereof, the person in charge of the database (file clerk) must notify of the changes within 5 business days to the receivers of inaccurate data, and;
- (6) Data banks and consumer real-estate records or credit protection services are considered public entities; after consumer debt collection is outlawed, no information hampering or making new access to credit difficult will be furnished to the relevant Credit Protection Systems.

<sup>13</sup>General Financial and Insurance System Law and Organic Law of the Banking and Insurance Superintendent's Office 12/06/96, Art. 158-160.

published, for instance, in the telecommunications sector. These provisions aim at encouraging a fair competition in the sector, although consumer rights are not considered<sup>14</sup>.

### **III.2.4 Kind of Information Handled by Reporting Agencies**

Reporting agencies have generally focused on information services tending to facilitate decisions on credit granting. In order to enhance credit decision-making, RAs gain access to banking information related to asset transactions, both negative and positive and, in some instances, to information on the compliance with tax obligations. In addition, the RAs have started to process personal data for various purposes like employment, medical, real estate leasing, etc. Following is a brief description of the kind of information processed by the RAs in analyzed countries.

---

<sup>14</sup> The Federal Consumer Protection Law partially regulates some aspects of personal data handled by firms for marketing purposes. In practice, the significance of this provision is not clear. Credit bureaus are governed by the financial system laws.

**Table 5**  
**Kind of Information Treated by Reporting Agencies\***

	Argentina <sup>1</sup>	Brazil <sup>2</sup>	Chile <sup>3</sup>	Colombia <sup>4</sup>	Mexico	Peru <sup>5</sup>	United States <sup>6</sup>	European Union <sup>7</sup>
<b>Banking and Insurance**</b>	---							
Credit and other asset-related								
Positive Information	x	x	--	x	x	x	x	x
Negative Information	x	x	x	x	x	x	x	x
Banking liability -related	--	--	--	--	--	--	--	--
<b>Tax</b>								
Positive Information	--	--	--	--	--	--	--	--
Negative Information	x	--	x	x	x	x	x	--
<b>For employment purposes</b>	x	--	x	n.a.	--	x	x	x
<b>For leasing purposes</b>	x	--	x	x	--	--	x	x
<b>Special categories</b>								
Medical	x	--	x	--	--	--	x	x
Sensitive	--	--	x	--	--	--	x	x

\*The meaning of the term Reporting Agencies (RAs) varies with the country. The regulation on private RAs in Argentina includes private reporting data banks; in Brazil, consumer data banks or records; in Colombia and Mexico, only credit bureaus; in Peru, private risk central offices; in the United States, consumer reporting agencies; and in Chile and Europe, personal data banks.

\*\* It includes credit granted by non-banking institutions (for instance, commercial non-banking institutions).

x means that private information is treated by the RAs; na means that information was not available to prepare this work.

1. In Argentina personal data on health may be released without authorization provided it is required for public health or emergency reasons or for the conduction of epidemiological research. According to the recently enacted people's data protection law, sensitive data may be assembled and subject to treatment only for general interest reasons authorized by the law or for statistical or scientific purposes if data subjects cannot be identified. Files, banks or records storing information that may directly or indirectly reveal sensitive data are forbidden.
2. In Brazil, the main private RA, SERASA, includes information on Tax Administration (Secretaria da Receita Federal).
3. Article 18 of the Personal-nature Data Protection Law in Chile (enacted on August 18, 1999) establishes that only negative information may be shared, as it sets forth that: *"Persons accountable for the records or personal data banks may only report information on economic, financial, bank or business obligations provided they consist of bills of exchange and protested promissory notes; protested checks for lack of funds, for having been drafted against a closed current account or due to any other reason; as well as on the failure to comply with obligations arising from collateral mortgages and loans or bank credits, financial associations, collateral mortgage administrators, savings and loans associations, public organizations, and state companies subject to common laws, and from administrators of credit granted to purchase at business firms"*. Sensitive data including medical information may be treated provided it is authorized by law or by the data subject, or they are required for the sake of the data subject's health.
4. In Colombia only data deemed relevant by the Banking Superintendent's Office standards and pursuant to Article 15 of the Constitution to evaluate the data subject's creditworthiness may be released.

5. In Peru there is an agreement between the National Tax Superintendent's Office (SUNAT) and private credit bureaus under which the SUNAT transfers information on tax debtors as well as lists of defaulting taxpayers to credit bureaus.
  6. In the United States a report may not contain consumer medical information unless the consumer so agrees and provided the report is for purposes of employment or credit or insurance transactions. It may include information on the character, reputation, life style and personal characteristics of the consumer only if he is clearly informed that such information is to be obtained and of the scope of such report and the consumer authorizes it, and the consumer must be furnished with a copy of a summary of his rights. The sensitive information includes information on arrests or criminal judgments for the last seven years.
  7. The European Union Directive sets forth that member states will forbid treatment of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, as well as the treatment of health or sexual life data, except upon the concerned party's explicit consent.
- 

## **1.- The Banking Secret**

The purpose of the banking secret is to protect the financial system users by preventing undue disclosing of their information. The discussion of this subject should begin with the description of the nature of the banking secret in the United States and Spain.

### The Banking Secret in the United States

Title V of the Gramm-Leach-Bliley Act of 1999 and the resulting strengthening with the Financial Information Privacy Protection Act of 2000, bind financial institutions to respect customer privacy and protect the confidentiality and security of non-public personal information. This Title also regulates the use of non-public personal information by financial institutions and its transfer to third parties.

Non-public personal information is defined as the information that identifies the individual, whether it is furnished by the consumer to the financial institution at the time he requests a product or financial service, originates from a transaction between the financial institution and the consumer or is obtained by the financial institution as a result of the financial product or service provided to the consumer.

The general obligation to respect customer privacy does not prevent a financial institution from transferring other institutions non-public customer personal information, provided that it meets the following requirements: 1.- Provide the consumer with a clear and conspicuous note of the information categories that may be revealed to third parties; 2.- give the consumer the opportunity to oppose this transfer before such information is revealed for the first time and at least on a yearly basis in the case of its current customers; 3.- inform consumers of its privacy policy upon request or the demand of a product or service from the financial institution. Before revealing for the first time information on a customer to other institutions, it must give the consumer the opportunity to instruct through simple means that such information is not divulged, mainly through the same method used by the financial institution to notify him of the personal data items it intends to reveal to third parties.

The law identifies several circumstances in which financial institutions may divulge non-public consumer personal information to third parties. Among them:

- 1.- when it is required to conduct, manage or enforce any transaction requested or authorized by the consumer or related to the provision or processing of a financial product or service requested by the consumer;
- 2.- upon the consumer's direction or consent;
- 3.- the financial institution reveals the non-public personal information to consumer reporting agencies pursuant to the Fair Credit Reporting Act, despite the consumer's opposition.

### The Banking Secret in Spain

In Spain like in other European countries, there are no general and explicit legal provisions forcing financial intermediaries to keep their operations secret (except in the Canary Islands zone).<sup>15</sup> Despite the above, there are provisions presupposing secret on banks operations with customers and the respect to banking information, besides the tradition to protect bank customers information implicit in national and international banking relationships.

In Spain tax authorities have access to bank information. Banking or credit institutions are forced to cooperate with the Tax Administration and furnish all kind of tax-related data, reports, or records, and such institutions may not get protection to fail to collaborate.<sup>16</sup> All the data obtained by Tax Authorities in performing its duties are confidential.

### The Banking Secret in Latin American Countries

In the analyzed Latin American countries, the banking secret is generally explicitly enacted in the financial system laws. There is no distinction between public or non-public information like in the United States, but regulations rather tend to differentiate between liability-related and asset-related bank information. Liability-related bank information is protected by the banking secret in all the countries, while asset-related information has a lower protection level to enable the development of credit markets. Public credit bureaus managed by financial authorities and private credit bureaus process credit information in all the countries. These bodies are liable for keeping bank secret and thereby for preventing third parties from having undue access to information in their databases.

In Argentina, Chile<sup>17</sup> and Peru<sup>18</sup>, the banking secret includes only liability-related operations (any kind of deposits received by banks). In Chile, credit operations are subject

---

<sup>15</sup> Such is the case, too, in other European countries including Switzerland. The lack of a formal regulation has not prevented these countries from protecting the privacy of individuals' bank transactions.

<sup>16</sup> General Tax Law (Law 50/1977), Articles 111 and 112 and General Tax Inspection Law.

<sup>17</sup> The General Banks Law (Dec. 1997 - Art. 154) sets forth that the banking secret includes deposits of any nature received by banks, which may only furnish records on said operations to the data subject or his legal representative; i.e., the RAs may not receive this kind of information from banks although they have the subject's authorization.

<sup>18</sup> Banking Secret is governed by the General Financial System and the Insurance System and the Organic Law of the Banking and Insurance Superintendent's Office No. 26702 (06/12/96, modified in 05/06/99 - Arts.

to confidentiality and banks may only make them known to a person proving a legitimate interest. Personal Data Protection Law in Argentina<sup>19</sup> — whose Article 26 provides for the regulation of credit reporting services — sets forth that credit reporting will not require the previous consent of the data subject for the transfer of his personal data nor the eventual notification of the transfer if the information is related to the reporting agencies business or credit activities.

In Brazil<sup>20</sup> and Mexico<sup>21</sup>, on the other hand, the banking secret includes both asset- and liability-related operations. Like in Spain, no financial law has been published in Colombia which expressly refers to the banking secret. The Constitutional Court in this country has established that the banking secret must not prevent information from flowing to credit grantors.

“The activity carried out by credit institutions is of a general interest because they handle the public’s savings (...). It would be foolish to believe that they provide services and, mainly, grant credits to individuals on which they have no information. On the contrary, for a prudent management information must be obtained to anticipate the fate of funds lent. The debtor, in turn, does not have the right, in the analyzed case, to hamper the furnishing of information, due mainly to three reasons: The first, they are facts in which not only him is involved; the second, he may not oppose the credit institution from exercising a right; and the third, it is not related to issues relative to his privacy (...)”<sup>22</sup>.

Like in Spain, the banking secret in Colombia does not oppose authorities. Law 57 of 1985 sets forth that authorities may know confidential documents (including those held by financial institutions). “A confidential document will not be denied to authorities requesting it for the due exercise of their functions. Such authorities must assure the confidentiality of documents disclosed to them as provided for in this article”. (Article 20)

### The Banking Secret Regulation Models for Latin America

Although the banking secret may become regulated by a general data protection law, Argentina and Chile have not followed suit. In these countries like in those lacking a data protection law, the banking secret has been regulated by dispositions on privacy in the

---

140-143). Banking secret includes liability-related operations of the financial system firms, which are forbidden to furnish customer information unless they are authorize in writing by the customer.

<sup>19</sup> Personal Data Protection Law 25.326 enacted on October 30, 2000.

<sup>20</sup> Law No.4.595 of 1964 Article 38 sets forth that financial institutions must keep their liability- and asset-related operations as well as services provided confidential.

<sup>21</sup> The Credit Institutions Law, Article 117, sets forth that credit institutions may only furnish news or information on deposits, services or any kind of operation to the relevant consumer or beneficiary. Despite the above, the Financial Groups Law (Article 33) allows credit bureaus (credit reporting company) to receive and furnish information on asset-related operations.

<sup>22</sup> The Constitutional Court pointed out in Judgment T-82/95.

financial system laws. This reflects the fact that a general personal data protection law is consistent with the existence of sectorial laws that incorporate more specific regulations like the banking secret. Despite the above, rather than seeking to regulate by kind of operation, either asset- or liability-related, the financial system laws should establish a general framework for bank secret. The United States model that stems from the definition of non-public information and defines the conditions for the transfer to third parties of such information by financial institutions, could be the starting point for a reform of the banking secret in Latin America.

## 2.- Tax Secret

As already mentioned, RAs access to tax information is considerably important because this kind of information is useful to evaluate individuals' creditworthiness as well as to foster compliance with tax obligations. In the United States, tax debtors information on which courts have passed judgment is public and is collected by the RAs. Several Latin American countries have lately amended or are in the process of reforming their tax laws to lessen tax secret and enable the exchange of information on defaulting taxpayers with the RAs. Such is the case for Chile, Peru and Argentina.

The Mexican Tax Code<sup>23</sup> was amended in December, 2000 as to enable information on tax obligations past due from taxpayers to be furnished to credit bureaus. The credit bureau that operates in this country will start to assemble negative tax information in its database the latest in 2002.

In Chile the Internal Tax Service currently publishes information on taxpayers who are included in the list of persons hard to audit, who have not appeared to summons for differences found on their tax return, have not been located during personal requisitions or have not attended requisitions notified by the authority. Chilean RAs incorporate this information into their databases<sup>24</sup>.

---

<sup>23</sup> Article 69 sets forth that the official personnel participating in the various processes relative to the application of tax provisions is forced to keep the confidentiality of:

- Tax returns and data furnished by taxpayers or related third parties, as well as those obtained during the checking process.

Such confidentiality shall not include *information on tax credits payable to taxpayers furnished by tax authorities to credit reporting agencies authorized by the Secretariat of Finance and Public Credit in accordance with the Financial Associations Law (added in December, 2000)* and cases established by tax laws and those cases in which data must be furnished to:

- Officials in charge of the management and defense of national fiscal interests;
- Judicial authorities in criminal proceedings;
- Competent courts that hear board allowance cases.

<sup>24</sup>Included among services furnished by Dicom Chile, is a report on the tax situation of individuals or corporations that may not stamp slips for any reason whatsoever. Tax information is released as well through a database containing information on state organizations with records of taxes for collection, real estate for collection, debts, defaulting persons (Form 21), tax credit debtors, and other.

The Chilean Internal Tax Service has developed a system through which it may consult certain information on the tax situation of taxpayers:

- who are included in lists of persons hard to audit.
- who did not attend summons for differences found in their tax returns.
- who were not found during personal requisitions.

In Peru banking and tax secret may be released upon the judge's demand during civil or criminal proceedings or upon request of the Investigation Commission or the Congress Investigation Commissions, provided it refers to the case under investigation<sup>25</sup>. Furthermore, the Tax Administration diffuses the amount of tax debt receivable (which gives rise to coercive actions for collection). The National Tax Administration Superintendent's Office (SUNAT), entered into a cooperation agreement with credit bureaus to disclose the lists of defaulting taxpayers, specific data from the Sole Taxpayer Record and lists of persons failing to file the tax return and, at the same time, give the SUNAT access to its database on defaults by the financial system customers and business institutions.<sup>26</sup>

In Brazil and Colombia credit bureaus do not have any kind of taxpayer information yet and there are still no agreements between tax authorities and RAs. An agreement of this kind may likely be reached soon in Colombia, since the Tax Administration is interested in tax information being processed by credit bureaus. Nevertheless, the scope of the tax secret in this country is still under discussion.

### **3.- Employment Information**

As far as employment information in the possession of RAs is concerned, it is worth mentioning that in the United States the FCRA sets forth strict rules for the issuance of consumer reports for employment purposes. The bureau user must notify the consumer that he will request a report, for which he must obtain the authorization in writing by the subject. The RA must verify the compliance of the above and obtain from the user a certification that the information will not be used in contravention of labor laws. Before bringing an action against the consumer, the user must deliver him a copy of the report and a description of his rights in accordance with the FCRA. When the RA uses information on public records and this information is likely to have an adverse effect on the subject's ability to obtain employment, the RA shall notify the consumer of the fact that it will prepare a report together with the name of the person to whom the report will be furnished.

There are no laws regulating the management of personal databases for employment purposes in Latin America.

### **4.- Sensitive Information**

---

- who did not attend a requisition after being notified by the authority.

<sup>25</sup>Constitution of Peru, Article. 2, section 5 and Tax Code (Decreto Legis 816) 20/04/96 Title III, Article 85.

<sup>26</sup>Only tax debt found in the coercive collection stage whose enforcement is not questioned is to be reported.

The information to be furnished by the SUNAT to Risk Central Offices is:

- 1) Sole Taxpayer Registration List (RUC).
- 2) Last name, first name, firm name, registration, address, etc.
- 3) Legal Representatives.
- 4) Tax Debt.
  - a) Amount of debt, debt tax period, date in which the coercive collection process begins, date of the last information processed.
  - b) Persons failing to appear.
  - c) Undeclared item(s), defaulting period(s), date of process.

There is a consensus among countries on the treatment and definition of sensitive information, which means data revealing the racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, union membership and health or sexual life information. Pursuant to the aforementioned international principles, in most countries this information may be collected and transferred only upon the authorization of the concerned party or under any particular legal instance.

An example of the above is the Spanish Constitution and data protection law.<sup>27</sup> In accordance with this law, personal data as to the racial origin, health or sexual life may only be collected, treated and transferred for general interest purposes as provided by a Law or upon the data subject's express consent. For personal data revealing the ideology, union membership, religion, and beliefs, paragraph 2, Article 16 of the Constitution sets forth that nobody may be forced to make declarations on them and that the authorization must be express and in writing, and the data subject will be warned of his right to withhold his authorization. The law forbids, too, personal databases created with the sole purpose of storing personal data revealing the ideology, union membership, religion, beliefs, racial or ethnic origin, or sexual life.

Regardless of the above, sensitive personal data may be subject to treatment if it is required for prevention or medical diagnosis, health assistance or medical treatment or the arrangement of sanitary services, provided such data treatment is made by a health professional subject to professional secret or by any other individual subject to an equivalent secret obligation. Data treatment is also lawful when it is required to safeguard the vital interest of the data subject or of any other person if the data subject is physically or judicially disabled to give his consent.

The data protection law in Chile considers medical information may not be subject to treatment, except upon the consent of the data subject or when the information is required to determine or give health benefits to data subjects. Prescriptions and laboratory analyses or examinations and health-related services are confidential (Article 127 of the Health Code). Its contents may be disclosed or a copy furnished only upon the patient's express consent in writing. The undue disclosing of its contents or breach of its provisions shall be penalized and sanctioned.

### **III.2.5 Consumer Rights in respect to Personal Information**

Although there is an international consensus on the consumer right to know and correct his personal information in the possession of RAs, the levels of development and coverage vary in the analyzed countries. In some countries, the consumer has the right to know his personal information from any data controller, either public or private; in others, however, not even from credit bureaus. Similarly, there are additional rights that have not been established by all the countries, like not being included in consumer lists or knowing the

---

<sup>27</sup> Article 7 of the Personal Data Protection Organic Law 15/91999, of December 13, 1999.

personal data recipient. The particular characteristics of each of the analyzed countries are discussed below.

**Table 6**  
**Consumer Rights relative to Personal Data**

	Argentina <sup>1</sup>	Brazil <sup>2</sup>	Chile	Colom- bia <sup>3</sup>	Mexico <sup>4</sup>	Peru <sup>5</sup>	United States <sup>6</sup>	European Union
<b>Access to Information</b>								
From credit bureaus	<b>x</b>	<b>x</b>	<b>x</b>	<b>x</b>	--	<b>x</b>	<b>x</b>	<b>x</b>
From any public or private data controller	--	<b>x</b>	<b>x</b>	<b>x</b>	--	<b>x</b>	<b>x</b>	<b>x</b>
The cost and time of delivery is regulated	<b>x</b>	<b>x</b>	<b>x</b>	--	--	--	<b>x</b>	<b>x</b>
<b>Know recipients of reports with his personal data</b>	<b>x</b>	--	<b>x</b>	<b>x</b>	--	--	<b>x</b>	<b>x</b>
<b>Correct his information</b>								
Held by credit bureaus	<b>x</b>	<b>x</b>	<b>x</b>	<b>x</b>	--	<b>x</b>	<b>x</b>	<b>x</b>
Held by recipients of information or creditors	<b>x</b>	--	<b>x</b>	--	<b>x</b>	--	<b>x</b>	<b>x</b>
Held by any data controller	--	<b>x</b>	<b>x</b>	<b>x</b>	--	<b>x</b>	<b>x</b>	<b>x</b>
<b>To be excluded from the offer list</b>	<b>x</b>	--	<b>x</b>	--	<b>x</b>	--	<b>x</b>	<b>x</b>
<b>Protection against an adverse action</b>	--	--	--	--	--	--	<b>x</b>	<b>x</b>

1. Article . 43 of the Argentinean Constitution grants every person the right to protection to know his personal data and the purpose thereof included in records or reporting public files or private data banks; in other words, the right to access and correct personal information held in the private sector databases is limited to reporting databases (including credit bureaus). Consequently, such right may not be exercised with any private data controller.
2. The Brazilian Constitution sets forth that the Habeas Data is a free right and the 9.507 Law governing the right to access to information and the Habeas Data proceeding provides for terms.
3. The Colombia Constitution sets forth in Article 15 people's right to know, up date and correct their personal information.
4. In Mexico the consumer does not have the right to access his personal information in the possession of credit bureaus. The Federal Consumer Protection Law grants the right to access and correct data with firms compiling information for marketing purposes, excluding credit bureaus. Pursuant to the July 1993 Reform of Article 33A of the Law for Financial Institutions Regulation, corrections are made only with creditors. This Article sets forth that: "*Data clarifications (of credit reports) will be made by the concerned parties with the creditors involved who, if any, will carry out the relevant arrangements with the Credit Information Company involved.*".
5. In Peru, the consumer may exercise such right through the Habeas Data, the procedure of which is set forth in the 26301 Law. The Bill for the 3903 Law relative to the access to information in the possession of the public administration specifies the periods in which the authority must satisfy the requirements.
6. In the United States, the Financial Information Privacy Protection Act sets forth that upon the consumer request, every financial institution must make available to the consumer any personal data held by it and reasonable available to the financial institution. By means of the Fair Credit Reporting Act , access to

information includes RAs as well. Individuals have also access to the public sector database as established by the Freedom of Information Act.

---

The broadest consumer rights to access and to correction of personal data in the analyzed countries are found in Brazil, Chile, Colombia, Peru, and the European Union. The consumer has the right to access and correct data from any data controller in these countries. Mainly the Personal-nature Data Protection Law in Chile, as well as the European Union Directive set forth that every individual has the right to demand anyone dealing either publicly or privately with personal data treatment, information on his personal data, the origin and recipient thereof, the purpose of storing them and the individualization of persons or organizations to whom data are regularly transferred. If the personal data are in a data bank to which several organizations have lawful access, the data subject may request information to any of them. In the event personal data are mistaken, inaccurate, incorrect or incomplete, and it is so proved, the consumer will have the right to modify them.

Although the United States Constitution does not contain provisions on the subject and lacks a general personal data protection law, the consumer, through provisions in various laws, has the right to access and correct his personal information held by RAs, public sector databases, and financial institutions, among other. The Constitution of Argentina sets forth that the consumer has the right to access and correct his personal information held by RAs as well as by the public sector. The consumer may not exercise such right with any private data controller. In Mexico the right to access and correct consumer information is too limited. The consumer does not have the right to directly access personal information in the possession of a credit bureau. He has only right to access and clarify his personal data through creditors.

### **III.2.6 Regulation of Reporting Agencies**

In this section we describe the regulation governing RAs in the analyzed countries. The main ones are: a) requirements to operate; b) principles to be observed for data treatment (collection, objectives, etc.); c) operation requirements; d) information transfer; e) information quality; f) security standards, and g) transparency. Following is the experience of the countries and regions analyzed in respect to these issues.

**Table 7**  
**Reporting Agencies Regulation**

	Argentina <sup>1</sup>	Brazil	Chile <sup>2</sup>	Colom— bia <sup>3</sup>	Mexico <sup>4</sup>	Peru	United States	European Union <sup>5</sup>
<b>Start of Operations</b>								
No registration or authorization is needed to start		X	X	X		X	X	
A registration is required	X							X
Authorization is required					X			
<b>Principles established in international instruments<sup>6</sup></b>								
◆ Purpose identification	X	--	X	X	X	--	X	X
◆ Limiting data collection								
a) Obtained through lawful media	X	--	X	X	--	--	X	X
b) Consumer awareness	--	X	--	--	--	--	--	--
◆ Transfer authorization								
a) Express and in writing	X	--	X	--	X	--	X	X
b) Implied in transactions initiated by the consumer	--	--	--	--	--	--	X	X
c) Authorized purposes or lawful interest of the recipient of information	X	--	X	--	--	--	X	X
◆ Limiting data withholding period	X	X	X	--	--	--	X	X
◆ Data quality	X	X	X	X	--	--	X	X
◆ Security regulation	X	--	X	--	X	--	--	X
◆ Controller's accountability	X	--	X	--	X	--	X	X
◆ Sanctions	X	--	X	--	X	--	X	X

\*Because the term Reporting Agencies (RAs) has been used extensively in this paper, the institutions which the analysis refers to in each country must be specified. In Argentina we refer to public or private banks aimed at furnishing reports; in Brazil, to consumer data banks or records, both public and private; in Chile and Europe, personal data banks; in Colombia, Mexico and Peru, we refer only to credit bureaus; in the United States, to consumer reporting agencies.

1. In Argentina the Individuals' Data Protection Law (Article 5) sets forth that the data subject shall give his consent in writing or by any other similar means, Article 26 exempts credit bureaus from requiring the consent to transfer or release data related to the transferees' business or credit activities. The Argentinean Individuals' Data Protection Law sets forth that only personal data relevant for the evaluation of the economic and financial standing of the parties involved for the last five years may be filed, recorded or released. This period will be reduced to two years when the debtor cancels or otherwise extinguishes the obligation upon proof thereof.
2. In Chile public organizations must register with the Civil Registry Service. It is worth to mention that "***The treatment of personal data arising out of or assembled from sources available to the public does not require any authorization provided they are of an economic, financial, banking or business nature, ... or they are required for direct-reply business communications or direct marketing or sale of goods or services***" We conclude that in Chile no express or written authorization is required for data transfer from credit bureaus to users.

3. Judgment No. SU-089/95 of the Colombian Constitutional Court sets forth that *“the habeas data relates to the manner in which data are handled, ... data obtained from unlawful means may neither become part of data banks nor flow”*. There is no regulation thereon; nevertheless, the Constitutional Court has pointed out that the debtor has the right to oblivion. *“A reasonable limit must also be set on the past, since it would not be fair or logic that a good performance in recent years would not suppress past bad performance. A term that avoids the abuse of reporting power and preserves sound credit practices is reasonable.”*
4. In Mexico, a Credit Reporting Company requires the authorization of the Federal Government, which must be granted discretionally by the Secretariat of Finance based on the opinion of Banco de Mexico and the National Banking and Securities Commission. Any person or group of persons acquiring the control of a Company requires also the authorization of the Secretariat of Finance. Sanctions are applied for violations of the banking secret by credit bureaus.
5. In accordance with the European Directive, when data have not been collected by the concerned party, the person accountable for the treatment shall, at the time of the registration or no later than at the time of the first data release, notify the concerned party of: \_ a) the identity of the person accountable for the treatment and, if any, his representative; b) the purposes of the data treatment; c) any other information similar to the above

## **1.- Requirements for the Starting of Operations of RAs**

Most of the analyzed countries lack established requirements. In the European Union, registration is a requirement<sup>28</sup>. Mexico is on the opposite side, where credit bureaus are discretionally authorized.

In order to eliminate potential regulatory barriers to RAs entrance to the market, a registration requirement rather than an authorization process must be established. A suitable data protection law eliminates the need to set up a discretionary authorization process to guarantee consumer right or verify that RAs observe the law.

## **2.- Principles on Data Treatment**

### **a) Data Collection by the RAs**

As mentioned in the international data protection principles (chapter IV.1.1), limits must be set to personal data collection; every data item must be obtained through legal and fair means and, when appropriate, with the knowledge of the data subject. The analyzed countries consider that it is not suitable to require the debtor's consent for the RAs to collect credit information.

### **b) Transfer Authorization**

According to the discussed international guidelines, the basic principle to disclose, make available or use consumer data for purposes other than those specified is the consumer's consent.

<sup>28</sup> In Argentina, the data file record must have at least the following information: a) Name and address of the accountable person; b) Characteristics and purpose of the file; c) Nature of the personal data contained in every file; d) Manner of compiling and updating data; e) Destination of data and individuals to which they may be transferred; f) Manner of interrelating recorded information; g) Means used to guarantee data security and specification of the category of persons that have access to information treatment; h) Data withholding period, and; i) Manner and conditions in which persons may access their personal data and procedures used to correct or update data.

In the United States the Fair Credit Reporting Act uses the generic concept of authorized purposes. Besides the consumer consent in writing, RAs data transfer to third parties is allowed provided that: i) the RA has reasons to believe that the third party intends to use the information in relation to a credit transaction, for purposes of employment, to contract an insurance or to evaluate the right of a consumer to receive a license or a government benefit; ii) there is a lawful business need of information, like mercantile transactions initiated by the consumer; iii) the request for information comes from a judicial authority; and iv) the State requires it to evaluate the individual's capacity to pay child support or an allowance for board. The transfer of sensitive information to third parties always requires of the previous consumer explicit consent. There is the possibility, too, that RAs transfer information to resellers. They are required to declare the final user's identity and the purpose for which he will use the information.

In Argentina and Chile the authorization as a general rule must be in writing and does not require authorization. Nevertheless, there are significant exceptions such as economic, financial, banking or business data in Chile<sup>29</sup>, or asset-related banking information in Argentina. Besides, the system adopted in Mexico for credit bureaus regulated by financial authorities is substantially more restrictive than in the aforementioned countries, since the regulation of asset-related bank operations forces bureaus to have the consumer express authorization in writing.

### **c) Limits to the Data Withholding Period or the “Right to Oblivion”**

Most analyzed countries regulate the time during which data may be withheld in the RAs databases. In the United States information on enforcement is withheld as a general rule for 7 years in the RAs databases. Such is the case for trials and judgments, noncompliance with tax obligations, accounts receivable, arrest records, denunciations and crime convictions, while bankruptcies are reported for 10 years. Credit information on RAs for 150 thousand dollars or more may not be erased, as well as life insurance data with coverage equal to or higher than 150 thousand dollars, or employment data with annual wages of 75 thousand dollars or higher.

Analyzed Latin American countries maintain a lower data-withholding period. For example, in Brazil a 5-year period has been established.

In Chile information on economic, financial, banking or business obligations is kept for seven years in RAs databases from the date on which the obligation became due; if the debtor settles his obligation, however, this period is lowered to three years. This device to encourage payment of obligations was incorporated into the Argentinean law. Pursuant to this law, only significant personal data to evaluate the economic and financial standing of the concerned parties may be filed, recorded or transferred during the last five years and such period is reduced to two years when the debtor either cancels or pays off the obligation. This differentiation is a strong incentive for the payment of due debts, succeeds in freeing some debtors from an old stigma and restore them as worthy of credit and business and, in addition, allows to pick individuals who had occasional

---

<sup>29</sup> The data protection law recently passed in Chile sets forth that the consumer authorization in writing is not needed to transfer economic and financial information. This is partly due to the fact that only negative information is shared in that country. Additionally, the user is accountable for the lawfulness of every service application to a credit bureau in Chile.

payment problems from individuals who acted fraudulently and who do not deserve the application of the shortened period.

It is too important not to mistake this reduction in the withholding period resulting from the compliance with a due obligation for a reduction in the withholding period or amnesty resulting from the enactment of a law. This kind of laws must avoid amnesties like the law approved by the Argentinean Legislative Power (October 2000) that was subsequently vetoed by the Presidency of the Republic. The vetoed article set forth that “data banks reporting credit information must suppress, or if any, not enter, any data on the failure to comply with or defaulting payment of an obligation if it had been cancelled at the time this law came into force.” This kind of amnesty produces an unfair treatment between consumers, a strong decapitalization of information essential for credit granting and makes domestic market transactions more risky.

The risk for the establishment of this kind of amnesties is not limited to Argentina. Recently Article 76 of the Colombian 550 Law of 1999 “On Economic Intervention” established that persons who within ten (10) months following the effectiveness of the law 114/99 settled the obligations due that had been reported to data banks would be released by the immediate expiration of their negative personal information. Financial institutions customers that settled their defaulting obligations between August 4, 1999 and June 4, 2000, had the right to the immediate expiry of negative information reported to Risk Central Offices.<sup>30</sup>

#### **d) Database Security-related Provisions**

Provisions generally only set forth that data must be protected against the risk of loss, destruction or undue transfer. Such is the case in the United States where regulations do not specify explicit RAs security obligations. Security measures adopted by this country’s industry stem from standards developed by the industry, which are required to build consumer confidence on services rendered by RAs. In this regard, it is worth to mention that various companies compete by promoting their security policies and privacy practices. Additionally, several organizations provide for privacy protection standards and help consumers that have been adversely affected by the reported information. Industrial associations have adopted guidelines and principles that have become widespread in the industry. For example, part of the service industry has agreed to follow the ISRG principles, which set forth protection standards like annual audits to verify them. Furthermore, firms and organizations have spread out on the Internet aimed at protecting privacy, like the “Truste”, a firm rating Internet pages based on their protection and privacy level.

#### **e) Sanctions to Data Controllers**

The regulation must recognize that the consumer has the right to be redressed of damage suffered, which requires a penalty system. In the United States, sanctions include both the redressing of damage and loss and payment of judicial costs.

---

<sup>30</sup> Another example of this kind of amnesty is Article 52, Law 546 of 1.999 “On the regulation of the housing financing system”. This article sets forth that long-term individual housing credit debtors who restructure their mortgage loans or repay with their house after January 1<sup>st</sup>, 1997, will have the right to have their loans declared paid –up and their names withdrawn from risk central offices. In practice, the benefit is obtained after the first three restructured credit installments have been cancelled and the obligation to withdraw information from defaulting debtors falls on the financial institution rather than on the credit bureau.

**f) Provisions Related to RAs Transparency**

These provisions may refer both to facilitating a consumer the existence, nature, and purposes of his personal data treatment as well as the identity and address of the data controller (the public registry, like the one set up by the European Union satisfies this principle); and b) the disclosure of their policies and practices related to personal data administration. This is a significant aspect in the United States' Fair Credit Reporting Act.

## **IV.- The Institutional Framework in Analyzed Countries**

This chapter describes: (a) the authorities in charge of watching, supervising and regulating matters related to natural persons' information protection in each country; (b) functions entrusted to such authorities; and (c) the role played by the judicial power in enforcing the laws.

We will begin the discussion of this subject with a description of the institutional frameworks in the United States and the European Union countries, which vary greatly from one country to another, but are highly developed. This situation considerably contrasts with analyzed Latin American countries, some of which have serious institutional lacks.

### ***IV.1.- International Comparison of the Personal Data Protection Institutional Framework***

Because there are many laws regulating personal data protection in the United States, there are several competent authorities, like in the financial system regulation where various authorities have jurisdiction depending on the financial institution involved. In the European Union, each country has a control authority nationwide with competence on public and private databases. They are liable for enforcing the national personal data protection law. In addition, at the community level, a counseling body exists and the European Commission may propose community provisions on personal data protection backed by a committee composed of member countries' representatives.

#### Administrative Authorities in the United States

In the United States there is no data protection authority for databases held by the private sector nor an authority related to databases held by the public sector. The enforcement of laws related to databases in the possession of the public sector has been traditionally entrusted to courts. Thus, in accordance with the Freedom of Information Act (FOIA), any complaint or conflict arising out of access to information controlled by any authority shall be settled by the District Court. Regardless of the above, laws regulating databases in the possession of the private sector show a clear trend to strengthen the role played by administrative authorities as inferred from amendments to the Fair Credit Reporting Act (FCRA) of 1997 and 1999, and the issuance of the Gramm-Leach-Bliley Act (1999) and the Financial Information Privacy Protection Act (2000). These legal reforms have conferred on the Executive Power authorities greater faculties and obligations relative to: (i) the enforcement of these laws; (ii) the issuance of supplementary regulations; (iii) the evaluation of law enforcement; and (iv) the duty to conduct research that will improve legal provisions in the future. Furthermore, law makers have strengthened provisions to facilitate the industry's self-regulation.

As far as federal administrative authorities are concerned, the role played by the Federal Trade Commission (FTC) in the enforcement of the FCRA, whose goals are on the one hand regulate RAs aimed at their sound development, and on the other protect consumer use of information is outstanding. The FTC provides for violations by RAs, RAs users, and

information furnishers. It has the power to settle complaints, ask for the submittal of reports and documents, bring a lawsuit before a district court, as well as significant diffusion and education functions. The FTC must prescribe regulations required to comply with such faculties<sup>31</sup>.

Federal financial authorities are liable, too, for enforcing the FCRA, the Gramm-Leach-Bliley Act and the Financial Information Privacy Protection Act, pursuant to the jurisdiction they have under the various financial system laws. The aforementioned financial authorities have to issue the necessary supplementary regulations to comply with these laws. They must have consultations and coordinate among them so as to assure that, as practicable, the secondary provisions they create are consistent and comparable. Additionally, the Gramm-Leach-Bliley Act sets forth that the Secretary of the Treasury must submit to Congress a report on the sharing of information between financial institutions no later than on January 1st, 2002.

Furthermore, the FCRA, the Gramm-Leach-Bliley Act and the Financial Information Privacy Protection Act, confer on state governments the power to apply the laws on those matters through the attorney general or through an official authorized by the state. Such powers consist of filing denunciations in favor of state residents before a district court to forbid the violation of provisions and obtain payment for damage and loss to the state residents. The state shall notify the FTC in advance of the actions it will take and the FTC has the faculty to intervene, be heard in all matters, remove actions to a district court and file remedies of appeal.

#### Control Authorities in the European Union

Three bodies are in charge of the enforcement of the European Directive of 1995. First, the Group Protecting Individuals relative to Personal Data Treatment, which is an advisory group at the European Community level whose duties are, among other, study the application of the directive in each Member State and the protection level offered by third countries. The second one is the Secretary of the Protection Group that carries on the tasks entrusted by the Group. The Secretary falls on the European Community Commission and is aided by a Committee of Representatives of Member States. The third body is National Control Authorities, who are in charge of supervising the enforcement of national laws within their territory. These national authorities carry on their duties independently, which is an essential component of the European model since they have extensive faculties in relation to public databases, too. National control authorities' decisions may be disputed before a court.

#### Authorities in the Analyzed Latin American Countries

---

<sup>31</sup> Specifically, pursuant to the Federal Trade Commission Act, the FTC's mission is to: (a) avoid unfair competition methods and unfair or fraudulent acts or practices in trade or affecting trade; (b) seek to obtain monetary compensation or any other repair for any offensive behavior toward consumers; (c) prescribe rules specifically defining unfair or fraudulent acts or practices; (d) conduct investigations related to the organization, business, practices, and administration of establishments engaged in trade; (e) prepare reports and legislative recommendations for Congress.

In Chile, law makers decided neither to create a national control authority nor entrust any existing administrative authority with responsibilities relative to law enforcement<sup>32</sup>. Unlike the model adopted in the United States or the European Union model, the Chilean law entrusts the full responsibility of the enforcement of the data protection law of 1999 to judicial instances. Judges are liable for taking measures to enforce the protection of rights under the law. Civil action tending to exercise rights under the law, including indemnifying material or moral damage caused are brought before courts under the summary procedure. Criminal action is governed by general rules.

Unlike Chile, the design of the institutional model in Argentina stemmed from the model adopted in the European Union. The Personal Data Protection Law of 2000 created a governing body in charge of taking all necessary action to comply with the law, which confers on the governing body significant powers relative to data protection and credit bureaus, but it is not clear if it has available all the means necessary to effectively perform such duties.

The Argentinean governing body functions are: (i) Aid and advise people as needed about the scope of the law and the legal means available to protect the rights it safeguards; (ii) establish standards and regulations; (iii) take a census of files, records or data banks and keep a permanent registration thereof; (iv) control the observance of rules on data integrity and security; (v) request information to public and private institutions, which shall furnish the required records, documents or programs or other items relative to personal data treatment; (vi) impose sanctions; (vii) become plaintiff in criminal action brought for violations of this law and; (viii) control compliance with requirements and guarantees that private files or data banks aimed at furnishing reports (i.e., credit bureaus) must meet to be entered on the Registry created by the law.

The Argentinean law is also advanced in terms of self-regulation. Under it, associations or organizations representing users or persons responsible for private databanks may create professional practice codes of conduct with standards for personal data treatment tending to assure and improve operation conditions of information systems in accordance with the principles provided for by the law. Said codes must be entered on the registry administered by the governing body, which may deny registration if it deems they do not satisfy legal and regulatory provisions on the matter.

Upon the law enactment, the Presidency of the Republic vetoed the text under which the governing body was conferred functional autonomy as a decentralized body within the scope of the Justice and Human Rights Ministry of the Nation, which set forth that the body would be headed and managed by a director appointed for a four-year period by the Executive Power upon the agreement of the Senate of the Nation. The presidential veto together with the fact that the Director may be removed by the Executive Power when it

---

<sup>32</sup> Pursuant to the Constitution of Chile, individuals may resort to the relevant Court of Appeals, which will promptly adopt the necessary measures to reestablish law and assure due protection of the affected party from any breach of his fundamental rights and guarantees (Article 20). Such is the case of the right of respect and protection of private and public life and the individual and his family's honor (Article 19, 4°), the grounds of the Personal-nature Data Protection Law of 1999.

deems that the director's performance has been wrong weaken the governing body. In addition, the law does not provide for the evaluation of the governing body or its accountability for its performance. Consequently, the actual capacities of the governing body are questionable.

It must be borne in mind that the banking secret in Argentina does not apply to credit granted by financial institutions. Consequently, the Financial System Debtors Central Office managed by the Central Bank of the Republic of Argentina may make available such information to the public in general with no restraints through its Internet page ([www.bcra.gov.ar](http://www.bcra.gov.ar)). The access to information on non-defaulting debtors; i.e., those ranked 1 and 2, may be obtained on a one-by-one basis, while access to the database on defaulting debtors, those ranked 3 and 6, and to the database of individuals forbidden to operate current bank accounts for having drawn checks refused for lack of funds is available on a monthly basis in a CD for \$10. Financial institutions are forced to report on a monthly basis all debtors with a debt higher than \$50, thus this is a very large database. The central bank uses this information, too, for purposes of risk concentration analysis, supervision of the detailed performance of the institutions' credit portfolios, as well as to evaluate compliance with prudential and credit ranking laws thereof. Besides this debtor central office, there are over 100 regional chamber of commerce bureaus and three national private credit bureaus associated with US credit bureaus.

In Brazil, the Consumer Protection and Defense Department (DPDC) of the Ministry of Justice Economic Law Secretariat has several powers on the matter, like keeping up-to-date records of grounded claims against RAs, which must be made public on a yearly basis. The disclosing shall specify if the claim actually was or was not attended by the provider. Additionally, since 1997<sup>33</sup>, administrative penalties are applied to persons: i) hampering or obstructing consumer free access to the consumer's personal data in individuals' databases, as well as to the relevant sources; ii) compiling consumer databases with false or inaccurate data; iii) maintaining databases with negative information for a period longer than the established one; and iv) ceasing to promptly and freely correct inaccurate data items in databases upon the consumer's request.

Additionally, since 1997 the Central Bank of Brazil is accountable for administrating the Credit Risk Central Office, on which loans higher than \$25,900 granted by financial institutions<sup>34</sup> to consumers and corporations are recorded on a monthly basis. Owing to the large amount of loans entered, only a small percentage of consumer credits is recorded on the database. Financial institutions upon the customer's specific authorization may consult consolidated information by customer. This central office is also used by the Central Bank as an instrumentality to supervise financial institutions.

Four different authorities participate in the regulation and supervision of credit bureaus in Mexico. The Secretariat of Finance and Public Credit is responsible for: (i) discretionally

---

<sup>33</sup> Decree No. 2.181 of March 20, 1997 confers these powers on the Consumer Protection and Defense Department.

<sup>34</sup> It includes both positive and negative information of multiple banks, commercial banks, savings banks, investment and development banks, real-estate loan associations, loan, financing, and investment associations, mortgage firms, promotion agencies, and mercantile leasing firms.

authorizing the setting up of credit bureaus; (ii) authorizing users of credit bureau information services; and (iii) fixing inspection and supervision fees to be paid by credit bureaus to the National Banking and Securities Commission. The Banco de Mexico has the power to issue general provisions to regulate credit bureaus activities and determine service fees. The National Banking and Securities Commission supervises credit bureaus and has the power to sanction financial users who are not authorized by the consumer before consulting the bureau. The National Commission for the Protection and Defense of Financial Services Users is in charge of attending and, if any, settling people's complaints against credit bureaus.

Banco de Mexico is liable, too, since 1954, for managing the risk central office called Servicio Nacional de Información de Crédito Bancario (Senicreb) (National Banking Credit Information Service). The Senicreb processes information on outstanding and due loans from corporations and individuals with entrepreneurial activity higher than 20 thousand dollars. Unlike the Argentinean or German Central Bank's Risk Central Office, the Senicreb was not created as an instrument to supervise banks' loan practices with the purpose of evaluating if banks had adopted prudent credit practices. At most, the Senicreb was used in the 70's and 80's to evaluate if these institutions complied with granting loans to the industrial and commerce sectors in the required percentages. As of today, Senicreb's operation is marginal since banks are not forced any more to consult this database, so they prefer to consult the database held in the bureau in which they have a share.

In Colombia, owing to the lack of a data protection law, the Constitutional Court has played a key role in settling disputes and construing and developing the main regulations on this matter by pronouncing judgments that have created jurisprudence. Like in Chile, in the event of a breach of the right of *habeas data* by any public authority or individual, a person may bring the guardianship action through a preferential and summary proceeding before a court.

Table 8 shows institutional frameworks in the various analyzed countries.

**Table 8**  
**Institutional Framework**

	<b>Independent Data Protection Authority</b>	<b>Non-skilled Authorities with Competence on Data Protection and RAs Matters</b>	<b>Judicial Power Habeas Data Proceeding</b>
<b>Argentina</b>	Governing Body	--	Local or federal court depending on the case <sup>1</sup>
<b>Brazil</b>	--	Consumer Protection and Defense Department Central Bank	Civil Court depending on the defendant
<b>Chile</b>	--	--	Civil Court
<b>Colombia</b>	--	Banking Superintendent's Office	Civil Court
<b>Mexico</b>	--	Secretariat of Finance and Public Credit, Banco de Mexico, Banking and Securities Commission, National Commission for the Defense of Financial Services Users, Federal Consumer Attorney General's Office.	Criminal or Civil Court
<b>Peru</b>	--	Banking and Insurance Superintendent's Office	Civil Court
<b>United States <sup>2</sup></b>	--	Federal Trade Commission, Financial and other Sectorial Authorities	District Court <sup>3</sup>
<b>European Union</b>	National Control Authorities		Judicial Authority <sup>4</sup>

1. In Argentina, the Habeas Data proceeding is brought before a judge in the domicile of the plaintiff or defendant. Nevertheless, the federal jurisdiction shall govern records or public data files of national organizations or data banks interconnected to inter-jurisdictional networks.
2. For the United States we refer to authorities set forth in the Fair Credit Reporting Act (Section 621).
3. The U.S. District Court has jurisdiction over its district concerning federal laws.
4. Without prejudice of the administrative recourse that may be brought before the control authority, any person has a judicial remedy available in the event his rights are violated.

In the following table we summarize the main advantages and disadvantages of data protection authorities.

**Table 9**  
**Is it convenient to have Control Authorities?**

Advantages	Disadvantages
<ul style="list-style-type: none"> <li>◆ The courts' role is diminished. This is especially significant for countries with a judicial system lacking either experience in the matter or expedite proceedings.</li> <li>◆ When the market is not yet developed, the authority may set the guidelines for its development looking for a balance among the different targets (Privacy, Security, Economic Efficiency, Freedom of Speech, Flow of Information, and Government Supervision).</li> <li>◆ Self-regulation does not apply to public databases and is limited for incipient or over concentrated markets.</li> <li>◆ An homogeneous regulation with a central control authority may better encourage the RAs market development, by reducing barriers to information access and enabling them to offer a wide range of services.</li> </ul>	<ul style="list-style-type: none"> <li>◆ The existence of several sectorial authorities involved results in the overlapping of duties and confusion, which undermine their effectiveness.</li> <li>◆ If authorities are not accountable, their administration could be driven off the goals set forth in the law.</li> </ul>

#### ***IV. 2.- Analysis of Administrative Authorities' Responsibilities***

We deem it convenient to divide administrative authorities' responsibilities into three categories; the responsibility to supervise the application of data protection legal provisions; regulatory powers; and the duty to submit reports and be accountable.

##### **1.- Supervise the Application of the Law**

The liability of supervising the application of the law includes receiving and settling complaints; obtaining access to data or reports from data controllers; being able to conduct or cause audits to be conducted to data controllers; having the power to bring a lawsuit against data controllers failing to comply with data protection provisions; having the power to sanction and impose remedies in the event data controllers fail to comply with

provisions; and diffuse and make known to the public in general legal provisions on data protection.

a) Settlement of Complaints

Settling complaints is a core component of personal data protection, but may become an expensive process in terms of time and money for authorities. Therefore, a policy designed to process complaints is important. Under the principles of the Standard Canadian Association, data controllers must appoint one or more individuals responsible for the compliance of guidelines, who must receive people's complaints. It is worth to mention that although Canadian standards apply only to the private sector, it would be suitable to apply them to databases controlled by the public sector as well, so these authorities should appoint one or more individuals accountable for attending this kind of complaints.

b) Access to data or reports

With this faculty control authorities may conduct investigations when there is no formal complaint. In addition, authorities may attain other goals, like supervising the financial sector or combating tax evasion.

c) Conducting or Causing Audits to be Conducted

Audits to database controllers may be an efficient mechanism to encourage them to comply with the established regulation. Audits are more systematic and have a greater scope than the investigation of a specific complaint.

d) Bringing Actions

Consumers and control authorities should trigger the bringing of summary proceedings before courts for alleged noncompliance of data controllers.

e) Sanctions and Remedies

The need to include fines in the laws to enforce rules will prevail. Besides fines, the market should be encouraged to penalize firms that do not adequately protect consumer data, as for example by creating the obligation for certain firms to obtain a certification from third parties of their compliance with the established provisions or rules. The fact that the authority publishes information on the firms complying with the above certification may be an incentive to observe regulations. It would also be required that authorities had the power to impose remedies for data controllers, like directing them to change their practices.

f) Consumer diffusion and education

Consumer diffusion and education are important factors contributing to a better compliance with legal provisions. The consumer needs to know his rights and the manner in which he can correct mistakes in databases, add information, etc. Thus, authorities should pursue a diffusion policy that would make RAs' goals and functions more understandable and combat notions like bureaus are just black lists or responsible for the denial of loans and, besides, make known how consumers may exercise their rights in a simple manner. Educating the public in relation to privacy may anticipate many conflicts and drive consumers to get protection. Additionally, authorities should keep the public informed on the impact that new practices or technologies may have on the public's privacy.

## **2.- Administrative Authority's Regulatory Powers**

We divide regulatory powers into control authorities' power to issue data protection secondary regulations and the power to examine and approve protection codes or standards developed by the industry.

### a) Power to Construe and Issue Secondary Regulations Facilitating the Enforcement of the Law

Conferring control authorities with the power to issue secondary provisions enable them to construe legal provisions based on each particular condition. This is specially significant for Latin American countries analyzed because they have relatively little experience on data protection and it is hard to believe that regulations as detailed as those contained in the US laws may be established from the beginning. Despite these advantages, conferring authorities with excessive discretionary regulatory powers on data protection could result in excessive regulations and/ or the establishment of regulations driven off the spirit of the law.

### b) Examine and Approve the Industry's Codes or Standards

It is likely that operating codes or standards developed by industries for the handling of databases will become important constituents of privacy protection policies. Control authorities should approve them since the codes or standards may contain provisions not related to the law. Despite this fact, delay and red tape of formal approval processes must be avoided. Regulation must be conceived as a minimum consumer protection standard, which must be fully complied with anytime, allowing industrial standards to offer consumers greater protection and benefits.

## **3.- Accountability**

An independent data protection authority must be obliged to account for its acts, so that the society may evaluate its performance. Even though this obligation may imply some costs, it entails significant benefits. In explaining its duty, the authority gains the society's confidence and support thereby increasing the efficiency of its actions.

## ***IV.3.- Comparing Responsibilities of Administrative Authorities in Analyzed Countries***

As may be inferred from the table below, the largest backwardness in Latin American countries is seen in the institutional framework. Control authorities both in the United States and in the European Union have responsibilities and powers significantly greater than authorities in Latin American countries, with the exception of Argentina's governing body. This may probably be due to the little experience in data protection in the region, as well as the structural lack of resources that characterizes Latin American governments and prevent them from creating and maintaining sound institutions. It should be remembered that these countries give preeminence to courts through which individuals carry out the Habeas Data.

**Table 10**  
**Administrative Authorities' Responsibilities and Powers Relative to**  
**Credit Bureaus**

	Argentina <sup>1</sup>	Brazil <sup>2</sup>	Chile	Colombia <sup>3</sup>	Mexico	Peru	United States	European Union
<b>Supervise regulation enforcement</b>								
Receive and settle complaints	--	X	--	--	--	--	X	X
Access to data to verify compliance with data protection provisions	X	--	--	--	--	--	X	X
Conduct or cause audits to be conducted to data controllers	X	--	--	--	--	--	--	X
Bringing lawsuits	X	X	--	--	--	--	X	X
Sanctions and remedies	X	X	--	--	X	--	--	X
Diffusion, education	--	--	--	--	--	--	X	X
<b>Regulatory powers</b>								
Regulatory or advisory body	X	--	--	X	X	X	X	X
Examination or approval of codes or standards	X	--	--	--	--	--	X	X
<b>Bound to submit an activity report</b>	--	--	--	--	--	--	X	X

1. The governing body advises people on the legal means to defend their rights. Complaints may be settled through the Habeas Data before courts. The governing body may request information on public and private institutions that shall furnish the records, documents, programs or any other items relative to personal data treatment. The governing body may request judicial authorization to access data treatment premises, equipment, or programs in order to check for breaches of the relevant law. The Argentinean governing body may apply sanctions ranging from warning, suspension, a fine amounting from one thousand (\$ 1.000) to one hundred thousand dollars (\$ 100.000) to the closing or cancellation of the file, record or data bank.
2. In Brazil, the Consumer Protection and Defense Department of the Ministry of Justice Economic Law Secretariat is the authority in charge of settling complaints.
3. In Colombia there is no administrative authority liable for data protection. Individuals' complaints or actions against credit bureaus are brought through the Habeas Data before a court.

\* \* \*

In the event control authorities are established, they should be independent to regulate private and public sector databases so as to prevent the government from unduly accessing individuals' data. They should settle disputes and impose sanctions on public sector institutions as well. The functions of this specialized authority should be: i) supervise the application of the law (receive and settle complaints, conduct investigations, bring lawsuits, impose remedies and sanctions, pursue diffusion and education policies for consumers, data controllers; users, etc.); ii) regulatory powers (construe the regulation, issue secondary provisions, examine and approve codes developed by the industry, etc.); and iii) be accountable and submit periodical activity reports.

## V.- Recommendations

A series of recommendations to protect personal data, promote the flow of information, and develop the RAs market in Latin American countries have stemmed from this work.

### General Recommendations

- Latin American countries should have a general framework for data protection and RAs development that considers international principles regulating personal data protection (OECD, UN, European Council, etc.). It is recommended that the regulation govern personal data treatment by any data controller (including RAs), both in the private and the public sector. The purposes of this legal framework must be personal data protection, trade support, and better market performance through the promotion of the flow of information. A major function of this legal framework is avoiding discrimination among individuals by restraining collection and transfer of people's sensitive data.
- Outstanding among personal data protection principles are: (i) the various individual's rights, including the right to know, obtain, and dispute information on his personal data in the possession of data controllers; (ii) restrains on data collection, use, and withholding; and (iii) data controllers' obligation to specify the purpose of the treatment, keep information quality (accurate and up-to-date), adopt the relevant security measures and be accountable for the data they control.
- The banking secret that in some Latin American countries protects depositor's information (Brazil, Colombia, Mexico) and bank debtor's information as well, has occasionally unnecessarily slowed down the flow of information in the economy. To avoid this situation the banking secret could be regulated under the general data protection law proposed. This, however, has not occurred in Argentina and Chile, which are the only Latin-American countries with a general law in the region, because of the reduced scope of the banking secret in these countries which does not include credit information.
- Tax authorities will be a significant prospective beneficiary if credit bureaus include information on defaulting taxpayers (those taxpayers with a debt payable), since it encourages the compliance of tax obligations. In Argentina, Brazil, and Colombia, RAs do not process any tax information yet. To further strengthen the government's tax collection capacity, tax authorities should be able to make consultations to credit bureaus. As is the case for the banking secret, the tax secret could be regulated under a general data protection law.
- Because of lack of experience on the subject, in the beginning the regulation of personal data protection and RAs is likely to be general. The private sector should be allowed to promote the development of additional standards adopted by the industry to bring greater security to consumers and drive the industry's sound growth. In the initial stage, minimum protection standards play an essential role in fitting and homologating several protection criteria, which are frequently scattered. Nevertheless, it may be anticipated

that operating codes or standards developed by the private sector for database management will be significant items contributing to the development of the legal framework.

- The institutional design should consider the administrative and legal tools for individuals to exercise their rights and have access to their personal data in a simple, prompt, and cost-efficient manner, which is not unduly expensive for consumers and data controllers. In this regard we noted that there has been considerable progress in the development of judicial instruments. Individuals in the analyzed Latin American countries, excluding Mexico, have the right to the *Habeas Data* proceeding, in other words, to a brief judicial proceeding to settle disputes on their personal data.
- There is a wide range of prospective administrative models for the effective application of the personal data protection and RAs encouragement provisions. We consider it would be desirable to create a specialized administrative authority in the countries that do not have experience in this matter, despite huge tax restraints faced by Latin American countries that hamper public funds appropriation for these purposes. In countries with the greatest experience, an administrative authority is advantageous, too: it reduces the load on courts, facilitates the homogeneous application of the law to different sectors, builds society's confidence in the enforcement of rules, and is the vehicle for the carrying out of the major diffusion and education functions, mainly to guide consumers and make known that RAs and credit bureaus are not black lists, but they rather play a useful role in backing non-defaulting consumers.
- Such authority must be conferred high independence and be subject to a strict accountability. Independence is desirable to prevent the government from unduly accessing personal data, as well as to enable the control authority to *de facto* settle disputes and impose sanctions to public sector institutions.
- Control authorities functions would be: i) supervise law enforcement (receive and settle complaints, conduct investigations, bring lawsuits, impose remedies and sanctions, pursue diffusion and education policies for consumers, data controllers and users); ii) regulatory powers (construe the regulation, issue secondary provisions, examine and approve codes developed by the industry, etc.); and iii) be accountable and submit periodical activity reports.

### **Facilitating the Development of Reporting Agencies**

In virtue of the obstacles faced by some Latin American countries (Mexico, Colombia, Brazil and Peru) to develop private credit bureaus, measures required to facilitate their development have to be evaluated.

- Grant RAs access to the greatest universe of personal information possible. In order to offer higher value and a wider range of services, they must have access to individuals'

information in the possession of the public and private sector. RAs should be able to process all types of personal information.

- Not require consumer authorization to compile information on financial institutions asset-related operations, since it would unduly limit RAs capacity to set up databases and offer credit information reporting services. The fact that credit information compiled by RAs will not be misused is assured by compelling RAs to send reports only to persons having “permissible purpose” as the term is used in the United States.
- Avoid that the financial system laws regulate credit bureaus. Such situation leads to an unnecessarily restrictive operation of RAs, thus reducing the quality of services rendered and private agents interest in investing to set up RAs<sup>35</sup>.
- In some countries in the region (particularly Brazil and Mexico) financial sector user groups (e.g. banks) have set up their own bureaus. This is in part due to the lack of a general regulatory framework protecting the integrity of databases and banks unwillingness to “loose control” of the credit information. Vertical integration of the major banks into a credit bureau allows them to keep some control on the bureau.
- This vertical integration hampers the development of the personal information market for several reasons: i) it creates a monopoly in the credit information market niche, since banks owning the bureau discriminate against other bureaus by not sharing their databases with them thus hampering bureaus from setting up competitive databases; ii) raises doubts on the impartial handling of information which discourages prospective customers to transfer their databases and thus demand services of the monopolist; and iii) prevents information services from being provided to sectors where the establishment of a sectorial bureau is not profitable. As a result, vertically integrated bureaus generally have no competition and are characterized by having little information available and provide limited and low-quality services. To counteract these distortions the cleanest and most effective measure, though perhaps the most difficult politically is to force banks to sell their equity shares in the bureau.
- Establishing the right of resale among RAs, that is to say, allow a RA to make consultations to another RA may facilitate entry into the market to new and efficient RAs. Resale reduces barriers for new RAs to enter the market, which is very significant in low developed or monopolized markets. For consultations between RAs to be economically feasible, consultation fees between RAs must be lower (or at least not higher) than the lowest fees offered by RAs to their best users.
- It is convenient to eliminate regulatory entry barriers to the RAs market. A registration requirement should be enough rather than a discretionary authorization process which is significantly more expensive for interested RAs. The data protection and RAs development promotion law would create effective and prompt institutional devices for the supervision, looking after, settling and sanctioning of complaints and for the proper

---

<sup>35</sup> The US Fair Credit Reporting Act is a Law that regulates credit bureaus and all kinds of RAs in a uniform legal framework.

protection of consumer rights, thus making an expensive authorization process unnecessary.

## **VI. Use of Definitions**

### **Data Controller**

General term referring to any person, either an individual or corporation, public or private, dealing with personal data treatment.

### **Data Treatment**

Data treatment is broadly defined and refers to any kind of operation or set of operations performed through automated procedures or otherwise and applied to personal data, such as the collection, registration, organization, maintenance, modification, extraction, consultation, use, communication through transmission, diffusion or any other way facilitating access to, comparison of, or interconnection to personal data, as well as the blocking, suppression or destruction thereof.

### **Personal Data**

Personal data are defined as any information on an individual identified or identifiable with the characteristics of his physical, physiological, psychical, economical, cultural or social identity (For example, credit, insurance, leasing, employment, health information, etc.).

### **Report Agencies (RAs)**

Data controllers, public or private firms, selling reports of individuals' personal data.

#### Private RAs

Reporting Agencies operated by the private sector. Includes specialized RAs like **Credit Bureaus**, Private Risk Central Offices, sectorial RAs, Financial Institution Rating Companies and firms that evaluate the industry for compliance with standards. This paper focuses on the regulation of private reporting agencies.

#### Public RAs

Reporting agencies operated by the government like Public Registries (Commerce, Property, etc.), and Public Risk Central Offices (traditionally operated by central banks or bank superintendent's offices).