

Introduction

Information means power, and economic information means economic power. Information has an economic value, and the capacity to store and process certain kinds of data may earn a country political and technological advantages over other nations.¹²³

As information and communication technologies (ICT) developed, and a series of technological advancements were made in the fields of medicine, computer science and molecular biology, among others, the landscape and context of privacy and the flow of information have changed substantially. This has always been a key factor in decision making and plays an essential role in business.⁴

In the globalized world, Internet and e-commerce transactions have developed, to a great extent, on the basis of information flow and information sharing.⁵ People spend a great amount of their time on the web, exchanging information, profiles and data with other users, either individuals or businesses, by participating in chats, using blogs, making purchases and other transactions, engaging in social networks, using cloud computing services, etcetera.⁶ Technological development has made information exchange much easier.

This significant information traffic has also secured great economic benefits. The analysis of information, as well as the analysis of data and metadata, i.e., data extracted from other information previously collected, have helped reduce credit card frauds, cut costs in genetic therapies and significantly reduce fraudulent claims in the health insurance area.⁷

As the new technologies multiply the opportunities to transfer information, there appear new and potential risks affecting individuals and businesses. Some of those risks are the ones which may injure people's privacy.⁸ This intense information exchange among individuals, and among individuals and businesses, has raised special concerns regarding privacy protection and the transfer of personal information.

While privacy has raised concerns since as early as the 19th century,¹ the protection of privacy and personal information has become a key issue for the State, due to the fear that the information held in the government archives may be misused by means of computerized data processing systems, thus violating citizens' rights. Many countries, especially European nations, started putting in place efforts to raise awareness on the importance of the protection of privacy rights, and study committees were created to deal with these matters.¹¹ Several laws were passed as a result of these governmental efforts to discuss and debate;

* Author may be contacted at lvc@lorenzovillegas.com. All the analyses and opinions included in this article are the author's sole responsibility and do not involve any institution. All translations are free translations.

³ Eger, John, "Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?", in *Law and Policy in International Business*, 10,4 (1978), pages 1065-1066.

⁴ Remolina, Nelson, "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?", in *International Law, Revista Colombiana de Derecho Internacional*, 16 (2010), page 493.

⁵ Friedman, Thomas, *La Tierra es plana*, Madrid, Martínez Roca, 2006, page 162 et seq.

⁶ According to a research study conducted in the United States in 2006, 61% of teenagers disclose their contact information in blogs. The study found that 44% disclose their email; 30% indicate their personal web pages; 55% give their geographic location; 39% disclose their birth date and 20% indicate their name. See Huffaker, David, *Teen Blogs Exposed: The Private Lives of Teens Made Public* (2006), available [online] at:

<http://www.davehuffaker.com/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf>. [Editor's note: accessed on 10/29/11.] Those statistics will probably have increased remarkably with the expansion of the social networks.

⁷ OECD, "Roundtable on Economics of Personal Data and Privacy", DSTI/ICCP/IE/REG (2011) 1, April 21, 2011, page 3.

⁸ OECD, "Report on the Cross-Border Enforcement of Privacy Laws", 2006.

⁹ Warren, Samuel D. and Louis D. Brandeis, "The Right to Privacy", in *Harvard Law Review*, IV, 6 (December 15, 1890).

¹⁰ Bennet, Colin, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992.

¹¹ OECD, "The Evolving Privacy Landscape", DSTI/ICCP/REG (2010) 6/FINAL, page 7.

for instance, the Data Act (1973) of Sweden; the Personal Data and Registration Act (1988) of the Netherlands; the Privacy Act (1974) of the United States and the Information and Information Technology Act (1978) of France, among others. According to OECD, before 1980, more than 8 OECD countries had passed laws relating to personal data protection.¹²

These kinds of regulations are mainly based on the right to privacy that every individual has. However, the notion of privacy and private life, its foundation as a right and the mechanisms to regulate and protect such right vary from region to region and from country to country.

Internet and the phenomena associated with new information technologies have brought about new challenges for countries when it comes to protecting personal information and guaranteeing people's right to privacy. This paper focuses on the challenges imposed by those new technologies, particularly Internet, on the protection of personal data, analyzing different protection systems and establishing comparisons. Our objective is to analyze the legal models in four Latin American countries (Argentina, Chile, Colombia and Mexico) in an effort to understand how our legislations deal with these problems and how they address the issues raised by the Internet in terms of fundamental rights development. In this paper we will look at the standards set forth by the laws of each country regarding data protection, the legal requirements for international transfer of personal data and the way in which the judicial or administrative authorities in Latin America protect privacy in the Internet environment. We will also analyze the regulations that apply to personal data retention in our countries. Last, we will present a series of recommendations and conclusions.¹³

¹² *Id.*

¹³ This paper will not cover the issues of children and adolescents' privacy, as this involves other specific protected interests.

I. Personal data protection models

The right to privacy and private life has been considered as a universal right for every individual. Article 12 of the Universal Declaration of Human Rights provides that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”¹⁴

In this paper we have identified three different conceptions of personal data processing and protection: the United States system, the European system and the Latin American system.

In the first place, the United States system reacts to the privacy issue mainly by means of self-regulation mechanisms. However, privacy is protected to a certain extent by the fourth amendment to the Constitution:

Privacy is only considered “fundamental” when it is threatened by a governmental abuse in the field of personal information processing. Therefore, federal laws apply only in this scenario or in the case of businesses storing sensitive personal information. In all other circumstances, data protection shall be available to citizens.¹⁵

However, privacy as a right is rather limited, particularly, by the protection of freedom of speech enshrined in the first amendment of the Constitution.¹⁶

The United States model in particular was developed based on prior judicial decisions that defined a personal field with which the State could not interfere.¹⁷ This resulted in the passing of the Privacy Act of 1974, the scope of which is limited to data processing by the federal government. However, in the United States there are federal and state sectoral laws that regulate specific fields of privacy right¹⁸ protection.

Second, the European model is based on article 8 of the European Convention on Human Rights of 1950 that guarantees the protection of the right to private and family life as a fundamental right: “1. Everyone has the right to respect for his private and family life, his home and his correspondence.”¹⁹

The European model is believed to accord a high level of personal data protection because it safeguards individual freedoms, besides being stringent and effective.²⁰ Thus, Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 was issued in the first place, followed by Directive 95/46/CE on personal data protection. This rule seeks to establish uniform standards for data protection in order to ensure the flow of information among the European Union countries that was being hindered. Based on this directive, the member states have passed their respective laws.²¹

The third and last model is the Latin American model, mainly based on the fundamental right of *habeas data*. Over time, it turned into a protection model significantly influenced by the one set out by the European Directive of 1995.²² The *habeas data* is a fundamental right as well as a tool to provide legal protection to the owners of personal data. It was created with the aim to secure protection in the face of the undue or illegal processing of personal data by databases or public or private registries. As will be pointed out below, Latin

¹⁴ Available [online] at: <<http://www.un.org/es/documents/udhr>>. [Editor’s note: accessed on 10/29/11.]

¹⁵ Guerrero Picó, María del Carmen, *El impacto del Internet en el derecho fundamental a la protección de datos de carácter personal; sine loco*, Thomson-Civitas, 2006, page 347.

¹⁶ Richard Posner and Lawrence Lessig have criticized privacy protection claiming that it undermines market efficiency by limiting the information available. See Posner, Richard, “The Economics of Privacy”, in *The American Economic Review*, 71(2) (1981), pages 405-409 and Lessig, Lawrence, *Code: Version 2.0*, New York, Basic Books, 2006.

¹⁷ See Supreme Court of Justice of the United States, *Meyer v. Nebraska* (262 U.S. 390 [1923]) and *Pierce v. Society of Sisters* (268 U.S. 510 [1925]). See also *Whalen v. Roe* (429 U.S. 589 [1977]).

¹⁸ See, among others, Cable Communications Policy Act; Video Privacy Protection Act; Omnibus Safe Streets and Crime Control Act; Electronic Communications Privacy Act; Health Insurance Portability and Accountability Act (HIPAA); Children’s Online Privacy Protection Act (COPPA) and Fair and Accurate Credit Transactions Act (FACTA.)

¹⁹ Available [online] at: <http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf>. [Editor’s note: accessed on 10/29/11.]

²⁰ Remolina, *supra* nota 3. However, this stance has been criticized: this European protection has not been very effective because the regulations were poorly enforced and implemented. See Burghardt, Buchmann, Böhm, *et. al.*, “A Study on the Lack of Enforcement of Data Protection Acts Proceedings”, in *3rd int. conference on e-democracy*, 2009.

²¹ See, for example, the Spanish Organic Law on Data Protection (Ley Orgánica de Protección de Datos) of 1998 [online] in: <<http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>>. [Editor’s note: accessed on 10/29/11.]

²² Pucinelli, Oscar, *El habeas data en Indoiberoamérica*, Temis, Bogotá, 1999.

American legislations have moved towards the European model in an effort to be considered, in the eyes of Europe, as legal frameworks with an appropriate level of protection, qualified to engage in business based on international data transfers from Europe.²³

After this preliminary analysis we may summarize the main differences between the European and the United States models: (1) the United States model essentially bases its approach on the concept of freedom as a response to the interference of the State with the life of individuals; the model points at self-regulation and sectoral regulations; (2) the European approach provides a more general and uniform protection, based on the concept of the fundamental right to privacy, in which the State must intervene adopting an active role to protect individuals.²⁴

These important differences—in particular, the fact that there is not a uniform body of laws that may ensure an appropriate level of protection as per the standard of article 25 of the European Directive of 1995—raised controversy on whether European individuals may transfer data to the United States, which poses a significant legal risk. As a response, the Department of Commerce created the *International Safe Harbor Privacy Principles Certification Program*.²⁵ The Safe Harbor program brings a solution to the lack of a uniform law on data protection. It consists in a voluntary system set out by the Department of Commerce in which the organizations that register according to the standards of those principles are deemed qualified for data transfers pursuant to article 25 of the European Directive. The Safe Harbor was approved by the European Commission in Decision 2000/520/CE as a program that provides an adequate level of data protection.²⁶

II. Personal data protection and Internet challenges

The landscape of data utilization has undergone substantial changes over the last two decades. The evolution of information technology—which has brought about the so called Information Society, with Internet being a key component of the process—poses questions about different legal issues associated with the use and collection of personal data. On the one hand, there is a legal system that guarantees (by different means) that citizens are able to control their personal data. At the same time, we are immersed in an environment in which the relationship between users and Internet is based on an interaction in which citizens provide large amounts of information just by surfing the web: browsing as we know it works by collecting data that enables it to function well, quickly and effectively (e.g., cookies used to identify browsing patterns so as to offer users an enhanced customized browsing experience.)

Some authors understand that this development may expose citizens to potential perils.

Internet has served siblylline interests. It is a particularly powerful vehicle through which anyone may infringe four kinds of basic rights, protected interests and legal interests: privacy, image, dignity, honor and sexual freedom [...]²⁷

This perspective, which in our opinion is too focused on the dangers that Internet may pose, overlooks its advantages and underscores the potential risks entailed. It overlooks the fact that the web has provided opportunities to strengthen, rethink and explore new ways to develop other fundamental rights such as freedom of speech, the right to information, the right to education and the right to knowledge, among others. In the view of those who uphold this stance on the risks that the Internet poses to the right to privacy, it is vital that the State regulates Internet use in advance, so as to prevent possible dangers.

The new resources for expression available on the web (Web 2.0), such as Facebook, YouTube, blogs, Twitter, LinkedIn, are based on the information—often classified as private—that the users of those

²³ Remolina, *supra* nota 3.

²⁴ For a deeper analysis of the differences between the European and the United States model, see Gregorio, Carlos, “Protección de datos personales: Europa v. Estados Unidos, todo un dilema para América Latina”, in Concha Cantú, Hugo, Sergio López-Ayllón and Lucy Tacher Epelstein (ed.), *Transparentar al Estado: la experiencia mexicana de acceso a la información; sine nomine et sine loco* 2004.

²⁵ Available [online] at: <<http://export.gov/safeharbor>>. [Editor’s note: accessed on 10/29/11.]

²⁶ Available [online] at: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>>. [Editor’s note: accessed on 10/29/11.]

²⁷ Guerrero Picó, *supra* note 14, page 334.

platforms voluntarily make available to the public. Users freely decide to access those platforms, voluntarily accept the terms of the service and begin interacting with other users and disclosing personal information. Photos, videos, information on their personal and professional life, about their tastes and preferences, etcetera, fill millions and millions of web pages in which people expose their “privacy”, in order to take advantage of the new opportunities brought about by the World Wide Web.²⁸

Moreover, the network has worked, in general, as a “free” service offering, in which the free enjoyment is often associated with online advertising models used to finance content and hosting services, among others. This kind of advertising collects user information in order to display advertisements that are the most appropriate for those particular consumers and the most adequate for cybernauts and their objectives.²⁹

This phenomenon, which is growing rapidly, poses the question of how important personal data are in fact and how valuable they are for each individual. Are they as important to their owners as to require an immediate action by the State to regulate the Internet?

Likewise, ICTs and particularly the globalization strengthened by the Internet, that has enabled global collaboration schemes such as outsourcing, delocalization, e-commerce and off-shoring, have deepened the phenomenon of international processing of personal information, and especially the international transfer and collection of information.³⁰ We will now analyze two aspects involved in Internet and personal data protection.

II.A. Cloud computing and data protection

One of the most relevant trends in Internet service development is cloud computing. This is any internet-based use of computers,³¹ which provides flexible access, regardless of the user’s location, to information technology resources, in a fast, immediate and economic manner. The services provided by means of cloud computing are virtualized, supported by shared technological and automatization resources and available from any access point in the world. These services range from email storage to infrastructure and platforms such as services, among others.

As the Internet develops, cloud computing services are closely linked to international data transfer and collection, and this exerts pressure on the legal systems of the respective countries. The rules that govern international data transfer and international data collection are often a secondary appendix of the regulations on personal data protection. However, the ever growing trend towards the use of virtual services in Internet shall force public policy makers to carry out a careful analysis in order to identify the best standards for protection.

The international transfer of personal data may be defined as the “import or export of such information from a country to another.”³² Thus, data are collected in a country by the individual in charge of personal data processing and transferred to another country where, in turn, they are further processed. Every day, thousands of companies and governments move personal data across the borders: domestic and international security affairs, international judicial cooperation, migration controls, corporate commercial or technical support via call centers, financial transactions, etcetera.

Besides, the international collection of data is a distinct phenomenon which has been particularly intensified by the Internet, since the World Wide Web has instated easy ways of communication among people all over the planet. An individual may collect data from another person located in a different country that has accessed their web page. This event does not imply an international transfer of data, as the information is not collected in a certain country and moved to another, but just collected in another country.

²⁸ For further information on the trends in the use of social networks, see: Instituto Nacional de Tecnologías de la Comunicación (INTECO) and Agencia Española de Protección de Datos (AEPD), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, February 2009.

²⁹ OECD, *supra* nota 6, page 5.

³⁰ Friedman, *supra* note 4.

³¹ Hon, Kuan, Christopher Millard and Ian Walden, “The Problem of “Personal Data” in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, part 1”, in *Legal Studies Research Paper No. 75/2011*, page 6, Queen Mary University of London, School of Law.

³² Remolina, *supra* note 3, page 495.

When users interact on the web, almost all their activities imply an international collection of data. Such collection may be consented or not, for instance, by html, social networks, cookies, web bugs, spyware, phishing, viruses and trojans or Trojan horses.³³

That data processing activity has been transferred to cloud computing providers. Given that this goes beyond national boundaries and jurisdictions where rights may be exercised and guaranteed, it is vital to pose questions about the legal model that should govern this kind of transactions and the protection of personal data. In the current state of affairs regarding personal data regulation, the most appropriate model to regulate their processing in cloud computing is the adoption of contractual stipulations aimed at preserving data integrity, information security and confidentiality, as well as unrestricted access by the owner of such information. This also gives rise to contractual liability, borne by those in charge of data processing, for any damage that the owner may suffer.³⁴ In the following sections we will focus on how the laws of different Latin American countries regulate international data transfers.

II.B. Access to information in Internet: privacy vs. freedom of speech and freedom of information

Internet revolutionized the access to information. As a result of the ever increasing power of Internet browsers, the information existing in the world has become accessible to everyone in a relatively easy manner. A great portion of this information, despite being public —as is the case of court decisions or official gazettes— was not necessarily meant to be spread globally. This has faced law with a new challenge, particularly regarding the scope of freedom of speech and the right to privacy.

Internet has enabled the consultation, in an expedite and broad manner, of governmental information that, being public, may contain personal data (for instance, name, sex, political identity, record of criminal or disciplinary offenses.) Now we should ask ourselves: is this information accessible in Internet regarded as public information or data? How should it be treated? What is the role of Internet and browsers in connection with the information indexed in said data?

These complex questions have not found a satisfactory answer in Latin American legislation.³⁵ On the one hand, access to information must be guaranteed for everyone in a transparent and open way, provided that freedom of speech is not violated.³⁶ On the other hand, the scope of that information and the processing it should receive when it contains personal data must be clearly defined. The Inter-American Commission on Human Rights' Declaration of Principles on Freedom of Expression establishes that "10. Privacy laws should not inhibit or restrict investigation and dissemination of information of public interest [...]"³⁷

This tension has been resolved in different ways by foreign legislations and jurisdictional decisions in the region, as we will explain below. However, we believe that neither court decisions nor legislations are clear when they define the various roles performed by those who participate in the process to access information, particularly the Internet.

Most European countries, especially Spain, have adopted a position in which they do not consider the Internet as a means of communication or as a generally available source of information,³⁸ particularly

³³ Guerrero Picó, *supra* note 14, pages 339-344.

³⁴ Council of Europe, *Protection of privacy and personal data on the Internet and online media report*. Committee on Culture, Science and Education, rapporteur: Andreja Rihter. Document 12021, Reference 3608 from October 2, 2009. Report approved on May 12, 2011.

³⁵ There is a doctrine effort called Heredia Rules or Minimal Rules for the Diffusion of the Judicial Information in Internet. These rules were created to help justice and the institutions responsible for the diffusion of jurisprudence from all Latin American countries in the processing of personal data contained in judicial decisions and court orders in Internet, without infringing the principle of transparency in court decisions or the right to information. Available [online] at: <http://www.cej.org.co/component/docman/doc_view/389-reglas-de-heredia-comentadas>. [Editor's note: accessed on 10/29/11.]

³⁶ See Joint Declaration on Freedom of Expression and the Internet UN, OSCE, OAS and ACHPR of 2004 and 2011, among others.

³⁷ Available [online] at: <<http://www.cidh.oas.org/basicos/basicos13.htm>>. [Editor's note: accessed on 10/29/11.]

³⁸ Agencia de Protección de Datos, *Memoria año 2001*. See also the decision of the Commission Nationale de l'Informatique et des Libertés (CNIL) of May 26, 2004.

regarding search engines.³⁹ In this connection, with respect to the processing of personal data, Europe has considered that search engines, given their role as technological intermediaries, are responsible for the processing of personal information. However, they do not bear the main responsibility in this respect.⁴⁰ Under this interpretation, search engines are related to the European Directive of 1995, pursuant to the principle of proportionality. Therefore, Internet browsers have a series of obligations regarding data processing, such as the obligation to delete obsolete information or remove it from their indexes. In this scenario, the obligation is not borne by the source of the information but by the browser.

This solution—which we deem controversial—results from the fact that laws do not include the concept of intermediary as a party that is clearly differentiated from the agents responsible for or charged with data processing. As will be seen below, different views on this topic coexist in Latin America. However, most countries have adopted the European pattern.

III. Regulation of personal data protection and privacy in Latin America

III.A. The Latin American constitutional system

The data protection system in Latin America shows, as a general rule, a unique feature which differentiates it from the European and the United States models. Compared to the European model, in Latin America there is no international treaty or supranational regional body of rules (in Mercosur or in CAN) to regulate the protection of personal data or their transfer. As to the United States model, the main difference lies in the fact that, in a large number of Latin American countries and legal systems, this protection is enshrined in the Constitution.

According to a research study conducted by Professor Nelson Remolina,⁴¹ 65% of Latin American countries have incorporated, in their Constitutions, explicit regulations on personal data protection, *habeas data* and privacy. This phenomenon—the inclusion of personal data protection in the Constitutions of Latin American countries—appeared with particular intensity in the eighties and consolidated in the nineties and during the first decade of the 21st century. The countries included in our research study, excepting Chile, have incorporated provisions on personal data protection in their Constitutions.

Nevertheless, those constitutional provisions create a framework for such right which is more or less limited.

Of all the countries examined, only the Mexican Constitution sets forth, in section 6, the explicit right to personal data protection (reform of 2009): “Everyone has the right to the protection of their personal data.”

The fact that the rest of the Constitutions do not include provisions as explicit as those enshrined in the Mexican charter does not mean that they do not apply limits on this fundamental right or provide it with content. The aspects of personal data protection contemplated by the Latin American constitutions included in our research study range from the right to access data stored in public and private databases (Argentina, Colombia, Mexico); including the right to access data stored only in public databases (Mexico); the right to know the purported use of data (Argentina); the right to know the actual use of data; the right to require data updating (Argentina, Colombia); the right to request data amendments or corrections (Argentina, Colombia, Mexico); the right to request data removal, deletion, destruction or cancellation (Argentina, Mexico); the right to request confidentiality of data (Argentina); the right to opposition (Mexico); the processing, circulation and collection of data (Colombia); the *habeas data* remedy (Peru) and the right to appeal for legal protection (*amparo* or *tutela*) (Argentina y Colombia).⁴²

TABLE 1. Constitutional provisions

³⁹ Groupe De Travail “Article 29” Sur La Protection Des Données, *Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche*, May 4, 2008. 00737/FR WP 148, available [online] at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_fr.pdf>. [Editor’s note: accessed on 10/29/11.]

⁴⁰ *Id.*, page 15.

⁴¹ Remolina, Nelson, *Retos de la recolección internacional de datos personales para los países latinoamericanos* (March 2011.) Unpublished.

⁴² *Id.*, table 3.

Country	Constitutional provision
<i>Chile</i>	None
<i>Argentina</i>	Section 43
<i>Mexico</i>	Sections 6 and 16
<i>Peru</i>	Section 2
<i>Colombia</i>	Section 15

Another remarkable characteristic of Latin American legal systems is that, in spite of having incorporated these provisions in their constitutions, most countries lack legal rules that build on these constitutional precepts or, at least, most of them have had a delayed legislative development.⁴³

Chile was the first Latin American country that created a general body of regulations on the protection of personal data. Law 19628 was passed in 1999 to regulate the protection of privacy or the protection of personal data.

Later on, Argentina created its legal framework, mainly based on Law 25326 of 2000, that refers to the integral protection of personal data filed in records, registries, data banks or other technical media for data processing, either public or private, aimed at providing information to guarantee the right to honor and privacy for every individual, as well as the access to any information recorded on those individuals [...].

This legal framework was particularly developed by Decree 1558 of 2001.

In July 2010, Mexico passed its law on personal data protection, even though the Federal Act on Transparency and Access to Federal Public Information had been in force since 2002.

In Peru and Colombia, two recent events changed the legal landscape on personal data protection.

In December 2010, the Colombian Congress passed the draft statutory Law 046 of 2010, Chamber of Deputies, and 184 of 2010, Senate, that regulates the fundamental right to personal data protection, which is now undergoing automatic review by the Constitutional Court to determine its constitutionality. Law 1266 of 2008 had been passed previously, with a scope restricted to commercial or financial personal data. On the other hand, after an appeal for legal protection (*tutela*), the constitutional judge had regulated, based on previous court decisions, several aspects of this fundamental right.

In Peru, the Congress passed bill No. 4079/2009-PE on personal data protection on June 7, 2011.

TABLE 2. **Personal data protection laws**

Country	Laws
<i>Chile</i>	Law 19628
<i>Argentina</i>	Law 25326
<i>Mexico</i>	Transparency and Access to Federal Public Information Federal Act
<i>Peru</i>	Bill No. 4079/2009-PE
<i>Colombia</i>	Law 1266 of 2008 and draft Statutory Law 046 of 2010, Chamber of Deputies, and 184 of 2010, Senate

III.B. Regulations on personal data processing in Argentina, Colombia, Mexico and Chile

There are a few subtle differences among the concepts of personal data or personal information in those countries. However, the common factor among them is the broadness of the concept that allows concluding that any kind of information relating to an individual may constitute personal data. That is the definition prevailing in the countries examined in this paper.

In Argentina, personal data is “any kind of information on individuals or entities, identified or identifiable” (section 2, Law 25326.) In the Chilean and Mexican laws, personal data is any kind of information relating to an individual, identified or identifiable (section 2 f of Law 19628 and section 3 v of

⁴³ *Id.* According to Remolina’s study, only 20% of the countries have legal provisions in this respect.

Mexican Federal Law.) In Colombia, Law 1266 of 2008 defines personal data as “any piece of information relating to one or more individuals, identified or identifiable, or that may be related to an individual or entity” (section 2.) This definition was changed in the new statutory law passed in December 2010, where it is defined as “any information relating to one or more individuals, identified or identifiable” (section 3 c.)

This shows that the concept of personal data is broadly defined in the legislations examined. This vital concept determines the scope of protection and the field in which the protection of this right may be applied. In this connection, in the face of a broad definition, the data protection laws currently in force extend their scope and might be interpreted regarding any kind of information or data that “may be related” to an identified or identifiable individual. This means, in a broad interpretation, that a piece of data or information becomes personal (and is therefore protected) not only when it relates to an individual or bears a link with them, but also when such information may be somehow associated with said individual. In this respect, in an interpretation exercise, the reasonable protection of personal data (those that belong to an individual’s private life) may be extended to any data that may be associated with a particular person by any of several means. This kind of interpretation, which raises a number of concerns, may threaten the rule of law and trigger enforcement issues, particularly when rules are to be applied to the Internet environment.

Thus, in our legislations, the concept of personal data does not have clear limitations. As a result, it is hard to achieve an accurate definition of personal data and determine the scope of privacy protection.

Such broad and uncertain definitions lead to complex debates in the Internet sphere. As explained above, in everyday browsing, Internet providers collect pieces of information, for technical or commercial purposes or to make the browsing process easier. Are those pieces of information considered personal data according to the definitions established in our legislations? Should they be considered personal data and thus be accorded a special legal protection?

These questions are not easily answered. There are several aspects that may raise controversy in Internet regarding the broad concept of personal data. However, it is vital to bear in mind that extending the concept of personal data to any information accessed on the network may impair network performance and development. We will clarify this problem with an example: IP addresses.

The IP address is a unique number or numeric label that enables the logical and hierarchical identification of a device (e.g., a computer), so that it connects to a network using the IP protocol. This corresponds to the network level of protocol TCP/IP. The IP address may be static or dynamic. The dynamic IP address enables the identification of the ISP that has been assigned the group of addresses to which it belongs; the static IP address, in turn, enables the identification of which connected device has been assigned to it. A computer or device may be identified by means of an IP address, but can these addresses be considered personal data? In our view, as they do not allow the straightforward identification of an individual, they should not be considered personal data. However, in Europe, the Spanish Agency for Data Protection (Agencia Española de Protección de Datos, APED)⁴⁴ and the Group of section 29⁴⁵ have held that those addresses constitute personal data, since the ISP “may establish a link between the user identity and the IP addresses assigned.”⁴⁶ This stance might extend to Latin American countries (as a result of the notorious influence of the APED) thereby impacting on the Internet development. In order to function, the Internet needs to collect this kind of information while users surf the web. Despite the above, should those addresses be considered personal data, they should be subjected to all the rules on protection of IP address processing, when this information can only be used to identify a computer or device. This would be disproportionate, as no individual could be identified based on such information.

This example may also be applied to other topics, such as cookies, email addresses, social network profiles, etcetera. Therefore, we must ask ourselves about the scope of our rules on personal data protection, what we are really trying to protect and whether an excessive regulation may have negative effects on users or consumers and on markets. These topics must be analyzed in further detail.

⁴⁴ Agencia Española de Protección de Datos, Informe 327/03.

⁴⁵ Decision 2/2002 of May 30, 2002 on the use of unique identification systems in terminal telecommunication devices.

⁴⁶ *Id.*

The comparative analysis shows the deep influence that the European regulations have had on the Latin American legislations examined. Likewise, there is evidence of the guidance set by the OECD⁴⁷ and the APEC⁴⁸ and, more recently, of the Madrid Resolution of 2009.⁴⁹

III.B.I. Argentina

The regulations on personal data protection are developed based on a series of principles established in sections 4 to 12 of Law 25326. It is important to underscore that the regulations developed by Argentina have led the country to be recognized by the European Commission as the only Latin American country with an adequate level of protection. This was stated in Decision 4 of 2002 and later confirmed in decision 6/30/03 of the European Commission. Therefore, Argentina has become the main recipient of personal data transferred from Spain to Latin American countries.⁵⁰

Specifically, in order to protect personal data, Argentina has developed the principles of purpose, data quality and proportionality, transparency in processing, safety, access, modification and opposition and restriction of successive transfers to third party countries.

Data processing and international transfer have been regulated by section 12 of said law, which establishes, as a general rule, the prohibition of transfers to countries or agencies that do not accord an adequate level of protection. This is determined by the National Bureau for Data Protection (Dirección Nacional de Protección de Datos), as provided by Decree 1581 of 2001. It is also understood that an adequate level of protection shall not only rely on the existence of an appropriate legal framework, but it may also be expressed by self-regulation or contractual stipulations.⁵¹

There are a few exceptions to this prohibition: judicial and police collaboration, the fight against terrorism, the exchange of medical information, stock exchange and bank transfers or transfers agreed within the framework of an international treaty. Nevertheless, Decree 1581 of 2001 stipulates that the prohibition to transfer personal data to a country that does not have an adequate protection level shall not apply when the owner of such information has given their consent.

Regarding international collection of personal data, the Argentine law does not contain any special provisions on this matter or any regulations on data processing in Internet.

With respect to international data transfers, Provision No. 2 of 2006 of the National Bureau for Data Protection has determined that those transfers must comply with the following minimum requirements:

- a) complete exporter and importer identification (name, identification number, address, telephone number, fax and email address);
- b) database and representative location;
- c) accurate information on categories and subcategories of personal data transferred;
- d) exporter's affidavit stating that the processing of data to be transferred shall be done in full compliance with Law 25326;
- e) indication of the purpose for which said data shall be used, pursuant to the law;
- f) accurate information on the safety measures that will govern the transfer and processing of personal data;
- g) data processing as a single unit, with no exceptions;
- h) exporter and importer shall bear joint and several liability to data owners;
- i) the assurance that the data owner shall be able to exercise their rights of access, modification, deletion and other rights set forth in chapter III, sections 13 to 20 of Law 25326;

⁴⁷ OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.

⁴⁸ APEC Privacy Framework.

⁴⁹ Joint Proposal for Drafting of International Standards for Privacy Protection, in connection with the personal data processing, accepted by the 31st International Conference on Data Protection and Privacy Authorities, held on November 5, 2009 in Madrid, Spain. The influence of this joint proposal is evident in the case of Colombia, as the reasons for legislative debate in Colombia are based on this text (*Gaceta del Congreso* No. 1023, December 2010).

⁵⁰ Remolina, *supra* note 3, page 504.

⁵¹ Pucinelli, Oscar, *Protección de datos de carácter personal*, Buenos Aires, Astrea, 2004.

- j) the National Bureau of Personal Data Protection shall be allowed to exercise its powers of inspection and sanction;
- k) the obligation to destroy and, if applicable, return to the exporter any personal data involved in the transfer upon contract termination, when it is not possible to comply with the provisions of Law 25326 or when the purpose for which that information was transferred ceases to exist.

From the above provisions we may infer that, in Argentine law, consent is of crucial importance as a key element in personal data processing. In this connection, consent determines the scope of data processing and the purpose of data collection and processing. Therefore, personal data processing is legal provided that there is express, previous, free and informed consent, and that data are used for the purpose for which they were obtained. Such purpose must have been previously informed to the owner.

In Argentine law there are no special rules on the right to privacy in connection with the Internet. In this regard, the Argentine justice courts have held that the treatment accorded to those rights in Internet shall be similar to the treatment they receive in other media, such as television or the press.⁵² They have also determined that Internet and the services provided on the network may be assimilated to “files, databases or other technical media for data processing” set out in the law (section 1 of Law 25326, as well as the definition of file, registry, database or data bank included in section 2), given the broad nature of those concepts.

At this point, it is interesting to analyze how some court decisions in Argentina have held that the scope of the law on personal data protection covers the Internet sphere, particularly regarding the access to information by means of browsers. In a controversial case (*Virginia Da Cunha contra Google y Yahoo*), a model and singer sued two important Internet browsers alleging that searches of her name were linked to pornographic or sexual content websites. She also claimed unauthorized commercial use of her image. The first instance judge sentenced these two companies to “remove the links between the defendants’ browsers and the websites with sexual, erotic or pornographic content that use her name, image and photographs.”⁵³ Therefore, the Internet browsers were held liable for allowing access to those contents.

There is another recent case involving the social networks. In the case *P.O. contra Facebook*, the provincial first instance judge of Rafaela issued a decision against Facebook and sentenced it to withdraw the content that a user had made public, which contained slanderous expressions against an Argentine politician. The judge held that freedom of speech was limited by the right to honor and good name, and that it did not allow for slanderous or libelous treatment.⁵⁴

As regards the first precedent, it is interesting to note that this judicial decision does not affect the source of information, the party that makes it public, but rather the Internet browsers involved in making it available, that are intermediaries in the information chain.

In the second case, the court ruling seeks to place the burden on the social network, which is also an intermediary, and not on the individual that created the content at issue.

These cases, which have emerged in several opportunities, show that the judges have placed a special value on the right to privacy over the right to freedom of speech.⁵⁵ In our view, they set a complex precedent regarding Internet service providers’ liability for their users’ content.⁵⁶ The result of these court decisions is

⁵² National Court of First Instance for Civil Matters No. 75. Judgment in *Da Cunha Virginia c/ Yahoo de Argentina Srl S/Daños y Perjuicios*. Buenos Aires, July 29, 2009.

⁵³ *Id.*

⁵⁴ National Court of First Instance for Civil Matters of Rafaela, Case File No. 1113/2010 *P. O. c/Facebook Inc. s/med. autosatisfactiva*.

⁵⁵ See the following rulings: in the Federal Court of Rosario, *Treviño Susana c/ Google Argentina s/ Daños y Perjuicios*, Case file No. 86,630, Innovative precautionary measures; in the National Court of First Instance for Civil Matters No. 95: *Rodríguez María Belén c/ Google Inc. s /Daños y Perjuicios*, Buenos Aires, March 4, 2010 and Rafaela, September 29, 2010; in the National Court of First Instance for Civil Matters of Rafaela: Case file No. 1113/2010 *P. o. c/Facebook Inc. s/med. autosatisfactiva*; in the National Court for Civil Matters No. 50: *Mazza Valeria Raquel c/ Yahoo* - de Argentina S.R.L. s/Medidas Precautorias*, Buenos Aires, July 2008.

⁵⁶ However, in August 2010, the appeals court rejected the allocation of responsibility to Google and Yahoo in the Virginia Da Cunha case. The decision issued by Chamber D of the National Appeals Court for Civil Matters favored those Internet browsers and found that they are not responsible for the content that third parties may post. National Appeals

not favorable to the development of the Internet, since the burden placed on Internet service providers is disproportionate and may pose restrictions on freedom of speech and on the right to information. Why are restrictions posed on technologic intermediaries and not on those who have created the information and made it public? There is evident confusion of the concepts of third party, intermediary and responsible party, which the laws have not made clear.

III.B.II. Colombia

The Colombian legal system on personal data protection is very special. While there is a constitutional rule (section 15) on the right to privacy, honor and good name, and while the *habeas data* is granted legal protection (*acción de tutela*), no legal regulations to develop this right have been issued for more than 17 years.

During this period, the right to privacy was developed on the basis of previous decisions, focusing on the Constitutional Court rulings that started to define their essential core, so as to set the principles for application and scope, particularly where it clashes with other fundamental rights such as freedom of speech.

This situation prevailed until 2008, when the Statutory Law 1266 of 2008 was passed. This law, which was initially meant to be general, was submitted to the Constitutional Court examination, which considered it sectoral and exclusively targeted at commercial and financial personal data.⁵⁷

In December 2010, the Congress passed Draft Statutory Law No. 146 of 2010, Chamber of Deputies, 184 of 2010, Senate, which incorporates general provisions on personal data protection. Conceived as a rule to regulate and define the scope of a fundamental right, it was treated as a statutory law and submitted to an automatic constitutionality review by the Constitutional Court.⁵⁸ This draft statutory law reflects to a great extent the doctrine of the Constitutional Court on personal data processing.

In general terms, we may state that this draft follows the European pattern. The purpose of the law is to establish a legal framework under which Colombia may be considered, in the eyes of Europe, as a country with an adequate level of personal data protection to receive data and information from Europe, and specifically from Spain.

In contrast with Law 1266 of 2008, this draft has much broader and more general expectations in terms of personal data regulation.

Regarding data processing and international transfer, Colombia has adopted an extremely protectionist model. In the first place, any data processing requires previous, express and informed consent. This is a very high standard which is not even present in European models. In the second place, pursuant to section 26, international data transfers are prohibited, except when done to countries with adequate levels of protection. The level of adequacy shall be determined by the administrative authority of personal data protection (the Superintendency of Industry and Commerce), which shall also issue the relevant certificates.

Constitutional jurisprudence has made a substantial contribution to developing the right to privacy and personal data protection; particularly, as pointed out above, because there are no regulations on this matter. Therefore, the Constitutional Court, by means of orders to grant legal protection (*tutela*), set forth the rules for personal data processing, specially those referring to financial or credit information. However, the principles developed through previous court decisions have been incorporated in Law 1266 as well as in the draft statutory law which is currently being reviewed by the Constitutional Court.

As regards access to personal information via Internet, the draft statutory law contains a remarkable prohibition that establishes that “personal data, except for public information, shall not be available on Internet” (section 4 f.) This rule conceives the Internet only as a means of communication and overlooks the multiple services provided through this network, as well as the rest of the fundamental rights which are developed through the world wide web. Hence, the transfer or storage of data via Internet and using cloud computing systems, and even the disclosure of private information, such as biographies or personal information made available in social networks, would be prohibited. It is evident that the Colombian law has

Court for Civil Matters, Chamber D, *D. C., v. c/ Yahoo de Argentina S.R.L. y otro*, 8/10/10. 2.nd instance, Buenos Aires, August 10, 2010.

⁵⁷ Constitutional Court, decision C-1011 of 2008.

⁵⁸ At present, this draft is being revised by the Constitutional Court.

not been created for a world with Internet: these are obsolete rules. Unfortunately, the question of Internet development does not seem to have any incidence in legislative debate.

However, in terms of information accessible via Internet and protection of privacy, in a case similar to those referenced for Argentina, we may sense the difference in the criterion used by the Colombian constitutional judge to decide on the matter. In ruling 371A/10 of November 30, 2010, the Constitutional Court issued a decision on an action filed by a person that, as victim of violence by paramilitary groups, had been involved in a judicial proceeding in which their rights were recognized. As a result, when this person's name was searched in Google, the entries found referred to court decisions in which she was overtly identified as a victim. Therefore, she filed an appeal for legal protection (*amparo*) so as to preserve her privacy and personal security. The Constitutional Court decided to protect the plaintiff and ordered removal of her name from the judicial decisions posted in Internet. The Court orders to "adopt any measures as are necessary to conceal and protect the plaintiff's identity [...]. Thus, any indication of Ms. XXXXX's identity must be removed from the copies of the relevant court rulings and from any other public reference."

Through this interesting example we may note that the judge does not restrict the actions taken on the Internet (we might understand that the Internet service provider acts as a third party intermediary and not as the party responsible for data processing), but goes to the original source of the information (the court of justice that made the judicial decision public), and that is where action is taken to protect privacy. In our opinion, the standard used by the Colombian judge is more favorable to Internet development, as it does not subject Internet service providers (in this case, browsers) to disproportionate limitations.

III.B.III. Chile

Law 19628 on the Protection of Private Life, or protection of personal data, is the rule in force in Chile that governs processing of personal data in registries or databases maintained by public or private bodies. This law establishes rules for data processing that comprise personal information collection, processing, transfer and storage. There being no specific rule in this connection, this law regulates the collection and processing of data collected in Internet.

We might state, in general terms, that this law follows the same development pattern as the European directive, as it is comprised in the opt-in system. Thus, section 4 stipulates that personal data processing shall only be permitted when authorized by the law or with the express authorization by the owner of the information in question (the individual.)

The Chilean law requires that notice be given when personal data are collected. Section 5 states that "Whenever personal data are requested by means of an electronic network, the following information shall be provided: a) identification of the party requesting the information; b) reason and purpose for collection and c) kind of data transmitted."

Likewise, the owner of the information in question must give their prior consent, being duly informed on the "purpose for which their personal data are stored and acknowledging that they might be publicly disclosed" (section 4.) The law also recognizes the rights of opposition, access and modification (sections 6, 12 et seq.)

As to the international transfer of personal data, the law does not establish a specific pattern, as observed in other countries under study. However, we might infer that the international transfer of data, being included in the concept of processing, is allowed to the extent it complies with the provisions of the law for data processing. It is worth pointing out that the original text submitted before the Chamber of Deputies prohibited transfers to countries or third parties unless they had protection levels similar to those prevailing in Chile. This text was not approved by the law makers.

The Chilean law has raised controversy because it does not incorporate the principle of purpose in personal data processing. Therefore, some authors understand that this rule lacks legal effect. At present, the Legislative branch is working on a bill to incorporate the principle of purpose in Law 19628.⁵⁹ However, in section 1, the law provides that "anyone may process personal data, provided they do so [...] for the purposes authorized by the law." To this respect, the purpose is a broad concept and guarantees that personal data processing may be done in compliance with the legal standards. Pursuant to section 4, purpose must be

⁵⁹ *Boletín* 7392-03.

comprised in the conditions accepted by the owner of the information upon giving consent (section 9) and in accordance with the privacy notice.

In terms of access to information posted in Internet and privacy, it is interesting to analyze the case *NN contra la Corporación Administrativa del Poder Judicial* submitted before the Appeals Court in Santiago,⁶⁰ regarding personal data which may be accessed via Internet. In this case, NN requested protection for her good name and privacy because when she typed her name in the search tool of the website of the Chilean Judicial Branch, the system returned her personal data identifying her as plaintiff in a filiation proceeding. Said information included her name and ID number, and information on her daughter's claim for not being recognized as such by her father. The court held that there is no violation of the rights invoked by the plaintiff to the extent that there is no disclosure of private information. The information disclosed, in accordance with the Civil Code, is public because it pertains to a judicial proceeding. When appealed, this decision was sustained by the Supreme Court.

III.B.IV. Mexico

The federal law on personal data protection is also a late-coming law. It was passed in 2010 as a consequence of the amendment of the Mexican Constitution that—as seen above—incorporated personal data protection as a fundamental right.

Just as other laws, the Mexican law is based on the principles of purpose and consent. In this connection, the Mexican law establishes that any processing of personal data (except for the exceptions contemplated therein) is subject to the owner's consent. However, it recognizes that there are different ways of expressing consent and accepts that, in section 8, the consent for data processing may be implicit. Nevertheless, the person responsible for managing such information shall inform, by means of a privacy notice, what kind of information shall be collected and for what purpose (section 12 et seq.)

In our opinion, those provisions are favorable to personal data processing in Internet. To serve its usual purpose, Internet needs to collect a great deal of information, so that browsing and other activities are optimally performed. Provided that those responsible include a privacy notice, the cybernaut's behavior implies that they have accepted the conditions set forth by such notice (implicit consent.) This opt-out system contributes to developing the Internet.

The same protection standard is reflected in international data transfers. Section 36 authorizes international data transfers and therefore they are carried out in accordance with the privacy notice. Nevertheless, the law foresees a series of scenarios in which international data transfers are authorized even when the owner of the information has not given their consent. These events cover a broader scope than that covered by the legislations of other countries in the region.

In this regard, the Mexican law seems to be flexible and capable of adapting to the Internet trends in a reasonable manner.

In terms of access to personal information on the Internet, there is a recent case that is worth analyzing. An individual filed a labor suit before the competent authorities. From the very moment said lawsuit was filed, the information on this individual was publicly accessible, as it was included in the Labor Bulletin (*Boletín Laboral*.) However, when such process came to an end, the plaintiff requested that their information was withdrawn from the Bulletin and that it may not be found by Internet search tools. The labor authority held that the information included in the Labor Bulletin is public and that it is not appropriate to modify documents in any manner whatsoever seeking to remove data that, pursuant to the legal provisions in force, must be published. It proposed modifying the Bulletin files so that they could not be found by a search tool and requesting Google to withdraw the information in question from browsers. The Federal Institute of Access to Information and Data Protection (*Instituto Federal de Acceso a la Información y Protección de Datos*, IFAI), the Mexican authority for data protection, reviewed the appeal and ratified the stance adopted by

⁶⁰ Available [online] at:

<<http://www.ijilac.org/jurisprudencia/components.php?name=Articulos&artid=103&idioma=spanish>>. [Editor's note: accessed on 10/29/11.]

the labor authority. It held that, although the information could not be removed from the Labor Bulletin, the personal information of the appellant could not be found in Internet browsers.⁶¹

This decision by the IFAI marks an intermediate position between the judicial decision standards examined above. On the one hand, it recognizes that the information of a public nature that is found in official bulletins may not be altered. However, the file where it is contained may be modified by the source entity of said information, so that the name of the person involved may not be found in the browser. Besides that, the decision issued by the Institute requests the Internet browser to update the indexed information so that it may not be found in the browser.

IV. Data retention: conflicts regarding the right to privacy

Personal data retention (or conservation) may be defined as the storage of personal information, telephone call records and Internet traffic information, including communication content, by either public entities or business companies. According to the provisions of several rules on this matter, the protection of personal information may be considered a form of data processing.

Most legal systems prohibit communication violations, under a principle that is associated to the very origins of the liberal State in the 18th century. Nevertheless, a series of recent events have provided the grounds for the nations to set restrictions on this principle that prohibits communication violations and protects the right to privacy. After the terrorist attacks that hit New York on September 11, 2001, and then those that took place in Madrid on March 11, 2004 and in London on July 7, 2005, the European and United States authorities have established that data retention is necessary to avoid terrorist attacks and to cooperate with the fight against organized crime.

Those legal developments have been harshly criticized: in the first place, it has been argued that those are exaggerated measures that endanger the right to privacy; in the second place, they have been deemed disproportionate, since the damage and limitation sustained by the right to privacy are not compensated by the effectiveness of such measures. That is to say that the results achieved by those measures do not justify a high level of privacy limitation. Therefore, a modification in the scope of such measures has been proposed in order to arrive at a more balanced scenario.⁶²

IV.A European Directives 2002/58/ CE, 2006/24/CE and 2009/136/ CE

The Council of Europe urged the European Union authorities to issue rules that contribute with the fight against terrorism. In this connection, Directive 2002/58/CE of the European Parliament and the Council of Europe was issued in the first place on July 12, 2002. It dealt with personal data processing and the protection of privacy in the electronic communications sector. This rule replaced and repealed Directive 97/66/ CE.

Directive 2002/58/CE provides a broad definition of traffic data: “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof” (article 2 b.) Therefore, traffic data may refer, among other considerations, to the routing, duration, time or volume of a communication; the protocol used; the location of the terminal equipment of the sender or recipient; the network where the transmission begins or ends; to the beginning, end or duration of a connection. It may also refer to the format used by the network for the conveyance of a communication.⁶³

Article 5 paragraph 1 sets forth the guarantee of confidentiality of traffic data and prohibits their storage, interception or surveillance, except for the technical storage which is necessary for the conveyance of a communication or when an authorization has been issued under paragraph 1, article 15, which refers to the eventual retention of traffic data, provided that guarantees are in place and with the sole purpose of

⁶¹ Instituto Federal de Acceso a la Información y Protección de Datos. Federal Board of Settlement and Arbitration (Junta Federal de Conciliación y Arbitraje) case. Case file: 4198/09, March 22, 2011. Reporting Commissioner: María Marván Laborde.

⁶² Breyer, Patrick, “Telecommunications Data Retention and Human Rights”, in *European Law Journal*, 11, 3, May 2005, pages 365-37.

⁶³ Recital 15 of European Directive 2002/58/CE.

safeguarding national security.⁶⁴ At the same time, article 6.1 establishes the obligation to erase those data or make them anonymous when they are no longer necessary for the purpose of the transmission of a communication. However, those data may be processed for subscriber billing purposes (article 6 paragraph 2); for marketing of services, provided that the user has given their consent (article 6 paragraph 3) and for fraud detection (section 6 subsection 5.)

After the attacks perpetrated in Madrid and London, the European Union authorities acknowledged the need to strengthen the measures identified in the 2002 Directive, and determined that data retention was necessary to fight against crime. To such effect, Directive 2006/24/CE was issued by the European Parliament and the Council on March 15, 2006 on retention of data generated or processed as a consequence of the provision of electronic communications services for public access or of public communication networks, in order to introduce changes in Directive 2002/58/CE. Later on, said directive was partially modified by Directive 2009/136/CE.

The objective of this directive is to have telecommunications service providers maintain certain data in order to ensure their availability for investigation, detection and prosecution of serious crimes (section 1.) The field of application of this directive comprises data on traffic and location of individuals and entities as well as the related data as are necessary to identify the registered subscriber or user; however, it does not include the content of communications (section 2.2.) The data referred to herein, in accordance with section 5, are those necessary to: 1) track and identify the point of origin of a communication; 2) identify the destination of a communication; 3) identify the date, time and duration of a communication; 4) identify the type of communication; 5) identify the users' communication device or what is considered to be the communication device; 6) identify the location of the mobile communication equipment.

Nevertheless, the directive stipulates a retention period for such data which may not be less than six months or more than two years from the date of the communication.

This European model has been widely criticized. The European Data Protection Supervisor pointed out that the European directive does not comply with the fundamental rights to privacy and personal data protection, as it establishes measures which are extremely intrusive. Moreover, the need for such data retention has not been sufficiently proven.⁶⁵

IV.B. The United States of America

In the United States, data retention is governed by several federal laws. In the first place, there is the *Electronic Communication Privacy Act* (ECPA) of 1986. This law protects wired and wireless communications by imposing conditions for communication interception. To this respect, it requires a court order to access information maintained or retained by electronic communication operators. The *USA PATRIOT Act* was passed later on and introduced changes in several aspects of the ECPA, which authorized the FBI to use *National Security Letters* (NSL) to request ISP information on their users without any kind of judicial control. This section of ECPA (section 2709) was considered unconstitutional under the first and the fourth amendments of the Constitution in the decision of the case *ACLU v. Ashcroft* of 2004 issued by the Federal Court of the New York district.⁶⁶

⁶⁴ One of the restrictions set forth by the directive, among others, is that the limitation of communication confidentiality must constitute a necessary, appropriate and proportionate measure, within a democratic society to safeguard national security, defense, public security or the prevention, investigation, detection and prosecution of criminal offences or of the unauthorized use of the electronic communication system.

⁶⁵ Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), May 31, 2011, available [online] at: <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf>. [Editor's note: accessed on 10/29/11.]

⁶⁶ *American Civil Liberties Union v. Ashcroft*, 2004. Available [online] at: <http://www.aclu.org/FilesPDFs/nsl_decision.pdf>. [Editor's note: accessed on 10/29/11.]

The *Telephone Records and Privacy Protection Act* of 2006 also prohibits deception in order to sale, buy or obtain personal telephonic records, except when this is done by police or intelligence authorities. This act imposes penalties of up to ten years on those who deliver confidential information about users.

On the other hand, the SAFETY Act (*Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act*) of 2009 requires electronic communications or remote computing service providers to retain, for a maximum of two years, all the records and any relevant information to identify the user of a temporary network address that the service provider may have assigned them.

Last, the CALEA law (*Under the Communications Assistance for Law Enforcement Act*) of 1995 requires that Internet service and telecommunications providers allow the police authorities to intercept and retain information on their users.

IV.C. Latin America

Regarding retention or conservation of personal information in Latin America, we have not found rules which may be assimilated to the European directive on personal data withholding. We may point out that, as a general rule, Latin American legislations have legal frameworks regulating the intervention in communications (especially telephone communications) when there is a previous judicial order.

However, every nation has their own rules that impose a series of obligations in terms of information conservation, particularly with respect to credit and financial information and to the obligations of the data banks that store this kind of information and their reports. This is due, to a great extent, to the fact that most Latin American countries have not faced massive terrorist attacks which might have forced them to set special limits on the conservation of telephonic records and Internet traffic information so as to allow the police authorities to access such information.

Despite this, it is worth analyzing a series of concrete topics about the experiences in our region.

Even though Colombia does not have a law that specifically regulates data retention, the constitutional jurisprudence has established, in terms of personal data conservation, the concept of right to oblivion or expiration of personal information. In this regard, the Constitutional Court has stated:

limits (...) have been established for the time that a piece of information may be maintained in the archives [...] In our view, commercial misconduct incurred in the past must not be perpetually kept in the archives. However, any time limitation set on data must be harmonized with the need for information on commercial conduct which may allow financial institutions to assess their risks.⁶⁷

Nevertheless, the Constitutional Court has acknowledged that law makers have the power to set limitations on the period during which personal data may be maintained in databases and files. This point has only been developed by Law 1266 of 2008, on financial, credit, commercial and service personal information.

Section 13 of the law at issue provides that:

Positive information shall be indefinitely maintained in information operators' data banks. Data whose content refers to delinquency period, type of collection, portfolio status and, in general, data referring to the breach of obligations shall be subject to a maximum conservation term. After expiry of such term, the operator shall remove said information from data banks, so that it may not be accessed or checked by users. That information shall be retained for four (4) years as from the date on which the overdue installments are paid or the overdue obligation is settled.

The Constitutional Court held this rule conditionally enforceable "understanding that the expiry of financial information, in case of delinquency periods of less than two years, shall not exceed twice the

⁶⁷ Constitutional Court, Sentence T-176 of 1995, Reporting Judge: Nelson Cifuentes Muñoz.

delinquency period and that the four-year retention term shall also be counted as from the moment in which the obligation ceases to exist in whatever manner.”⁶⁸

The draft statutory law that is currently being reviewed by the Constitutional Court does not contain provisions on data retention apart from the provision that such retention must comply with the principles of purpose and freedom.

Another interesting case in Colombia is the one referred to Law 633 of 2000, which in section 91 provides that

Any Colombian web pages and sites operating in Internet which carry out commercial or financial activities, or provide services, shall register before the Companies Registry and provide the Colombian Tax and Customs Bureau (Dirección de Impuestos y Aduanas Nacionales, DIAN) with the information on business transaction as requested by this entity.

This rule was challenged before the Constitutional Court, which decided to declare it conditionally enforceable, stating that the information that the DIAN may request is directly relevant and strictly necessary to comply with its duties upon exercising its legal competences.⁶⁹

In Argentina, there is an interesting case to analyze: Law 25873 that established the obligation of telecommunications service providers to retain certain personal data for a specific term. This law introduced modifications in Law 19798 in order to incorporate the obligations of telecommunications operators, including Internet providers: (1) telecommunications operators must have, and pay for, the human and technologic resources as are necessary to capture and deviate the communications they transmit, so that they may be remotely monitored by the competent authorities upon request; (2) telecommunications operators must record and systematize users’ filiation data and addresses, as well as the records of their communications traffic, for consultation by the competent authorities and (3) telecommunications operators must retain the personal information collected for ten years.

This law was intensely challenged, as it was considered to damage certain fundamental rights. These objections were submitted before the relevant judicial authorities and in the case *Halabi, Ernesto c/ Poder Ejecutivo Nacional*, the Supreme Court of Justice held sections 1 and 2 of said law and regulatory decree 1563/04 unconstitutional, as

the communications referred to by Law 25873 and all the data transmitted by users through the relevant mechanisms belong to the personal privacy sphere and are covered by the provisions of sections 18 and 19 of the Constitution. The right to privacy and the resulting protection against violations oppose to any “arbitrary” or “abusive” “intervention” or “intromission” in the “private life” of the affected parties [...] It is evident that the rules challenged have established a restriction that affects one of the facets of individual autonomy— the right to privacy. Its provisions do not differentiate or identify with the necessary accuracy the scenarios in which the interceptions shall be applicable, as they do not specify how the Internet information traffic must be processed. In this context, it is unquestionable that browsing data are associated with content. This is compounded by the fact that the regulations do not provide a specific system for communications protection regarding the storage and the automatic processing of personal data.⁷⁰

In terms of personal data retention, in Mexico, in addition to the regulations on personal data protection, we found the National Security Act.⁷¹ This law stipulates that, in the case of an imminent threat to national security, the Government shall be entitled to use the legally available resources, including anonymous information (section 33), and to intercept all sorts of private communication based on a previous judicial authorization (section 34.) The law specifies that communications interception comprises recording and registering information. Section 42 specifies that the data obtained by means of communications interception

⁶⁸ Constitutional Court, Sentence C-1011 of 2008, Reporting Judge: Jaime Córdoba Triviño.

⁶⁹ Constitutional Court, sentence C-1147/01 of October 31, 2001.

⁷⁰ Judgment of *Halabi c/ PEN*. Argentine Supreme Court, June 26, 2007.

⁷¹ National Security Act, published on January 31, 2005.

must be considered sensitive information. The law does not include provisions on the maximum term for retention of the information collected.

Another interesting case of personal data collection and retention in Mexico is the National Registry of Mobile Telephony Users (Registro Nacional de Usuarios de Telefonía Móvil, RENAUT.) This is a directory of mobile telephony users that links the number of their mobile line to their Single Personal Code (Clave Única de Registro de Población, CURP.) This mechanism was established by a decree dated February 9, 2009. Under this rule, an accurate record of mobile telephone users may be maintained, with due protection of data privacy. To fulfill its purpose of keeping data on telephone call traffic and location, the directory saves the following information:⁷² 1) type of communication, complementary, messaging or multimedia services used; 2) data required to track communication origin and destination; 3) data required to determine the date, time and duration of the communication; 4) date and time of first service activation and location from where service was activated and 5) digital identification of telephone line geographic location.

V. Conclusions and recommendations

Latin American legislation has been strongly influenced by the European rules on personal data protection, particularly seeking to adjust its rules to the European standards and thus be considered to provide an adequate protection level. As a result, over the last eleven years, most Latin American countries have undergone a transition from the *habeas data* model to general legislations with very stringent data protection (especially in the case of Colombia and Peru.)

At the regional level, we have not found specific projects to standardize regulations in Latin American countries. However, the Committee on Juridical and Political Affairs of the Organization of American States⁷³ has issued a recommendation that is worth mentioning here. This document aims to serve as guidance for the Member States of the OAS to develop their national legislations. It is based on a study of the current legislative trends aimed at adjusting the personal data protection regulations to the rest of the new technologies and adopts an intermediate stance between the European and the United States models. This recommendation is based on a series of principles devised to regulate personal data processing (purpose, consent, quality, legitimacy, etcetera), as well as on rules for international data transfers. The OAS' concern for setting clear and consistent rules for transborder flows of data that enable developing Internet businesses is particularly evident. At the same time, the recommendation guarantees minimum standards of personal data protection. However, these are mere recommendations that lack a concrete juridical value for Member States.

Therefore, apart from this initiative led by the OAS, we have not seen, in the short or medium term, regional efforts to harmonize data protection.

As a general rule, we have observed that Latin American legislations tend to adopt rather stringent protection standards (Argentina, Colombia, Peru) based on the European pattern. However, it would be very advantageous that, taking into account the dynamics and challenges posed by the Internet, Latin American nations adopted more flexible laws, so as to acknowledge this phenomenon and be prepared for the challenges they will face in the future. As pointed out above, personal data protection is a fundamental right that must be protected, but in a reasonable, flexible and proportionate manner. For instance, the new Colombian law provides that data may only be transferred to countries with similar protection levels. But the protection standards set forth in the Colombian regulations are even more stringent than those prevailing in Europe and the United States. This will hinder the enforcement of the laws on data protection.

⁷² Del Conde Ugarte, Alejandro. *La seguridad y privacidad en el marco de las telecomunicaciones*. Seminario Iberoamericano de Protección de Datos “Nuevas Tecnologías, Seguridad y Privacidad”. 2010. Available [online] at: <http://www.redipd.org/reuniones/seminario_2010_cartagena/common/Alejandro_CondeADCU_Proteccion_Datos_telecomunicaciones_Cartagena_julio_2010.pdf>. [Editor's note: accessed on 10/29/11.]

⁷³ Organization of American States. Committee on Juridical and Political Affairs. “Draft preliminary principles and recommendations on data protection”, November 19, 2010. CP/CAJP-2921/10.

Nevertheless, the challenges that the Internet has posed on people's privacy must be incorporated in the Latin American debate. The discussions on privacy still deal with the usual topics, especially those relating to credit and financial information. It is curious to note that the problems brought about by the Internet were not discussed during the legislative procedures that took place in Latin America over the last six months. The legislative debates carried out in Peru and in Colombia have not analyzed the impact that the Internet has had on privacy or how the Latin American legislations should address personal data protection in the globalized world of our days. We could state that our laws follow a local trend that is not fully compatible with the challenges posed by the Internet or by globalization.

In this scenario, judges will probably be the protagonists, as they will have to apply the rules on data protection to concrete situations involving Internet, based on the exercise of the *habeas data* rights (as a special legal action or as an appeal for legal protection [*tutela* or *amparo*]) enshrined in Latin American constitutions. In this connection, we have seen how a series of judicial proceedings in Argentina have sought to impose standards for the protection of privacy in Internet, particularly by applying restrictions on browsers and on the exercise of freedom of speech in social networks. This sensitive issue, in which the exercise of the right to privacy is assessed with other rights exercised on the network (right to information, freedom of speech, etcetera), together with other technical and commercial considerations, is not always subjected to a deep analysis by judges. It is interesting to note the perspective from which the Colombian constitutional judge addresses the restriction on access to information in Internet: he places the burden of protecting the right to privacy on the source of information, and not on the Internet intermediary that indexes the information available on the web.

In spite of that, there is a tendency to strengthen the role of special authorities for personal data protection as part of the local policies, following the European pattern. At this point, those protection systems (judicial and administrative) shall operate simultaneously, so decisions on Internet privacy shall be made based on the legal framework in force. This model of administrative entities for data protection is still scarcely developed in Latin America, so it will be vital to track its evolution.

In our view, it would thus be advisable that Latin American countries could work on a joint policy to establish reasonable protection standards, appropriate to the contemporary privacy issues, which could ensure the adoption of a flexible regulatory framework to respond to the challenges posed by the Internet.

On the other hand, we see the need, in our countries, to carry out a thorough analysis of the scope of the privacy protection that must be granted, and how such right must be assessed in connection with the exercise of other fundamental rights, such as the right to information and freedom of speech. It is essential to have the State really question itself about the value that people place on their "personal data" and whether the level of protection should extend uniformly to anything that may be considered "personal information." As the regional laws provide a broad and unspecific definition of personal information, this concept might end up including information which has little connection with people's privacy and private life. To this respect, we must recover a definition of right that protects what is genuinely associated to people's private life; for example, certain sensitive or private information. However, extending the constitutional safeguards to any kind of information that may be associated or related to an individual is inadequate and may restrict the exercise of other rights without justification.

As pointed out above, not all the people place the same value on their personal information. Many of them are willing to disclose their information, tastes, beliefs, photographs,⁷⁴ and the State should not restrict people's exercise of their rights. In this connection, a model for personal data processing should be subject to the individual's tacit consent implemented by a privacy notice (as in the case of Mexico) and not to their express consent (as is the case of Colombia, Argentina and Chile) regarding any personal information.

⁷⁴ Facebook has more than 14 million users in Colombia (as of June 2011); 26 million in Mexico; 20 million in Brazil and 15.3 million in Argentina. Available [online] at: <www.facebookcolombia.com>. [Editor's note: accessed on 10/29/11.]

With respect to transborder data flows, which have a significant impact on the development of cloud computing and other Internet services, two models can be identified in the region: a model that authorizes international data transfers (with a few exceptions) and another model that does not authorize this kind of transfers (with a few exceptions.) Mexico and Chile are comprised in the first model; Colombia and Argentina belong to the second. In the first model, data transfer is a positive event that should occur under certain conditions; in the second, there is a negative approach (“data transfers of any kind shall be prohibited...”.) In our opinion, taking into account the ever growing impact of cloud computing processes, as well as other phenomena associated with globalization (such as service outsourcing or off-shoring), the legislations of the region should be open to international data transfers, establishing minimum protection conditions (and not restricting them exclusively to nations with a level of protection that is similar to or higher than the protection granted), which may even be contractually stipulated. Notwithstanding the above, we must bear in mind that, as the phenomenon goes beyond frontiers and national jurisdictions, it cannot be exclusively controlled by national laws. In this connection, it would be advisable that the countries in the region started multilateral proceedings to set out common standards for data protection based on the accountability principle, following the draft recommendations document issued by the OAS. This is contained in principle 5 and reads as follow: *“The data controller is responsible for taking all the necessary steps to follow personal data processing measures imposed by national legislation and other applicable authority.”*

All in all, technology poses challenges, but it also provides solutions. At present there are technologic tools to reduce the unwanted data collection, as well as mechanisms to ensure privacy (software to *anonymize* personal information, that limits data tracking and controls spyware, antivirus software, communication encryption mechanisms, etcetera.) Thus, people may set the protection levels they wish to get using these tools and decide how they wish to have their information used by third parties.

This also implies the possibility of opening spaces and scenarios for industry self-regulation, where private actors may set protection standards instead of just waiting to get the restrictive protection of the State (e.g., privacy by design.)

It is evident that Internet and the new technologies bring about a large number of challenges that the law must face. But this requires modern, innovative solutions which help develop these new technologies, so as to ensure innovation without damaging fundamental rights such as freedom of speech, freedom of information or the right to privacy and private life. This study does not purport to cover all the legal issues posed by the Internet in terms of personal data protection or claim to have the solutions to those problems: it seeks to open paths, pose questions and analyze, from a critical perspective, the response provided by some legal systems.