CJI/doc.541/17 corr.1

PRIVACY AND PROTECTION OF PERSONAL DATA

(Presented by Dr. Ana Elizabeth Villalta Vizcarra)

I MANDATE

The Inter-American Juridical Committee (CJI) chose the undersigned to represent it in various meetings of the Ibero-American Data Protection Network (RIPD) during which the participants discussed the protection of personal data and went on to develop Standards for Personal Data Protection to promote the adoption of uniform rules across the region.

In that connection, I hereby submit the following report to the Inter-American Juridical Committee at its 91st Regular Session, to be held in Rio de Janeiro, Brazil, from August 7 to 16, 2017.

II. BACKGROUND

The Inter-American Juridical Committee (CJI) proposed a set of principles on privacy and personal data protection in the Americas aimed at encouraging OAS Member States to institute measures ensuring respect for people's privacy, reputations, and dignity and, in particular, to consider formulating and enacting legislation to protect the personal information and privacy interests of individuals.

At its forty-fourth regular session (Asunción, Paraguay, June 2014), the OAS General Assembly instructed the Inter-American Juridical Committee "to prepare proposals for the [Committee on Juridical and Political Affairs] on the different ways in which the protection of personal data can be regulated, including a model law on personal data protection, taking into account international standards in that area" AG/RES. 2842 (XLIV-O/14).

The CJI rapporteur for this topic concluded that the most effective approach would be to develop a legislative guide based on the 12 principles adopted by the Committee, with a few changes taking account of the various sets of guidance prepared within the European Union, the OECD, APEC, etc., and providing additional guidance to states. The purpose of the guide would be to assist Member States in the preparation of national legislation, drawing on the achievements in other regions while taking into account developments in our own region and technological advances.

These principles are based on internationally recognized standards. They are intended to protect individuals from wrongful collection, use, retention, and disclosure of personal data. National rules for the protection of personal data must

have a legitimate purpose and ensure that the data is processed in a fair, legal, and nondiscriminatory manner. They must ensure that those who collect, process, use, and disseminate personal data do so appropriately and with due regard for the rights of the individual.

Member States must seek a balance between the right to access data and the right to the protection of personal data. In other words, they must balance the right of individuals to control how their personal data is collected, stored, and used against the right of individuals and organizations to use personal data for reasonable and legitimate business purposes in a secure and protected manner.

The principles on personal data protection apply equally to the public and private sectors—that is, to personal data generated, collected, or administered by either government or private entities. They do not apply to personal data used by an individual exclusively in the context of his or her private life.

The concept of privacy rests on the fundamental rights of honor, dignity, intimacy, and image as well as freedom of speech, thought, opinion, and association. Many of these rights are recognized in the international human rights instruments and the constitutions and fundamental laws of the OAS Member States.

Within the Inter-American system, these rights are clearly established in Article V of the American Declaration of the Rights and Duties of Man (April 30, 1948) as well as Articles 11 and 13 of the American Convention on Human Rights ("Pact of San José") (November 22, 1969). The Inter-American Court of Human Rights has also cited them in various judgments, including *Case of the Ituango Massacres v. Colombia* and *Case of Atala Riffo and daughters v. Chile*.

With respect to national secondary legislation, a number of OAS Member States have adopted rules guaranteeing respect and protection for privacy and personal data.

At the same time, most of these laws establish that the right to privacy is not absolute and may have reasonable limitations. Similarly, the fundamental principles of freedom of expression and association and free flow of information are also recognized in the international human rights instruments. Within the Inter-American system, they are guaranteed under Article IV of the American Declaration of the Rights and Duties of Man (April 30, 1948) and Article 13 of the American Convention on Human Rights, ("Pact of San José") (November 22, 1969).

"Personal data" is any information specific to an individual that can be used to identify that individual. It is information that identifies or can reasonably be used to identify an individual, whether directly or indirectly. It is information about an identified or identifiable individual such as his or her name, email address, marital status, occupation, or identification number.

"Sensitive personal data" is data whose disclosure would affect the most intimate aspects of a person's life or place him or her at serious risk. This category includes, for example, racial or ethnic origin; present and future state of health; genetic information; religious, philosophical, or moral beliefs; union membership; political opinions; and sexual preference or orientation.

The "data controller" is the natural or legal person, private entity, public authority, or other body or organization which, alone or jointly with others, is responsible for storing, processing, using, protecting, and disseminating the data. In some circumstances, it is also responsible for collecting the data.

The "data processor" is the natural or legal person, private entity, public authority, or other body or organization that processes the data in question, alone or jointly with others. "Data processing" includes any operation or set of operations performed on personal data, such as collection, recording, storage, retrieval, disclosure, or transfer.

The "data protection authority" is the body responsible for setting and enforcing the laws, regulations, and requirements relating to the protection of personal data in order to ensure consistency. Data protection authorities may differ from one member state to another, depending on the state's legislation.

The "data subject" is the individual whose personal data is being collected, processed, stored, used, or disseminated; in other words, the individual whom the personal data is about.

The principles on privacy and personal data protection presented by the Inter-American Juridical Committee rapporteur are briefly explained below:

OAS Principles on Privacy and Personal Data Protection

First Principle: Lawful and Fair Purposes

"Personal data should be collected only for lawful purposes and by fair and lawful means."

This principle must be respected throughout the process of gathering, compiling, storing, using, disclosing, and disposing of personal data.

The requirement of lawfulness embraces the notion of legitimacy and excludes the arbitrary and capricious collection of personal data. It implies transparency and a legal structure that is accessible to the person whose data is being collected. The purposes for which the data is collected must be stated clearly so that the individual is able to understand how the data will be collected, used, or disclosed.

Use of fair and lawful means excludes obtaining personal data by fraud or deception or under false pretenses. Collection must be consistent with not only the applicable legal requirements, but also the reasonable expectations of individuals

based on their relationship with the data controller collecting the data and the notice(s) provided to individuals at the time their data is collected.

Second Principle: Clarity and Consent

"The purposes for which personal data is collected should be specified at the time the data is collected. As a general rule, personal data should only be collected with the consent of the individual concerned."

This principle is based on transparency and consent. This means that the purposes for which personal data is collected should be specified clearly at the time the data is collected. In addition, individuals should be informed about the practices and policies of the entities or persons collecting the personal data so they can make an informed decision about providing that data.

The individual will thus be able to consent freely to the collection of personal data in the manner and for the purposes intended. The individual's consent should be based on clear and sufficient information; it should leave no doubt or ambiguity. For consent to be valid, the individual should have adequate information about the specific details of the data to be collected, how it is to be collected, the purposes of the processing, and any disclosures that may be made. The individual must have the ability to exercise a real choice.

There must be no risk of deception, intimidation, coercion, or negative consequences for an individual who refuses to consent. The data subject's consent to the processing of his or her personal data must be freely given, specific, and informed.

Third Principle: Relevant and Necessary

"The data should be accurate, relevant, and necessary to the stated purposes for which it is collected."

Personal data should be correct, accurate, complete, and as up to date as necessary for the purposes for which it was collected. Data quality is important to the protection of privacy interests. The data collector or processor should therefore adopt mechanisms to ensure that personal data is correct, accurate, complete, and up to date.

The data must be relevant, that is, reasonably related to the purposes for which it was collected. It should not be used for unrelated purposes.

Fourth Principle: Limited Use and Retention

"Personal data should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law."

Personal data should not be used for purposes incompatible with those for which it was collected, except with the consent of the data subject or by the authority of law.

Personal data should be kept only as long as required by the purpose for which it was collected and as prescribed by relevant domestic law, since unnecessary and excessive retention of personal data clearly has privacy implications. Therefore, data must be disposed of when it is no longer needed for its original purpose or as otherwise required by national law.

However, in some instances (patient, employee, and student records, for example), a data controller may have legitimate reasons to retain data for a certain period of time.

Fifth Principle: Duty of Confidentiality

"Personal data should not be disclosed, made available, or used for purposes other than those for which it was collected, except with the knowledge or consent of the concerned individual or under the authority of law."

The data controller has a basic duty to maintain the confidentiality of personal data in a safe and controlled environment and to ensure that such data is not used for purposes which are incompatible with the original purpose. Protecting privacy means not only keeping personal data secure, but also allowing this data to be used and disclosed for other purposes. Trust must be established and maintained between data subject and data controller.

Sixth Principle: Protection and Security

"Personal data should be protected by reasonable and appropriate security safeguards against unauthorized access, loss, destruction, use, modification, or disclosure."

Data controllers have a duty to take necessary practical and technical steps to protect personal data in their possession or custody and to ensure that such personal data is not accessed, lost, destroyed, used, modified, or disclosed.

Personal data should be protected by safeguards that are reasonably designed to prevent material harm to individuals from the unauthorized access to or loss or destruction of the data. Sensitive personal data requires a higher level of protection.

These safeguards must be "reasonable and adequate" against cyber threats and respond to their evolution. The challenge is to provide meaningful guidance to data controllers while ensuring that the standards remain technologically neutral and are not rendered obsolete by rapid changes in technology.

In the event of personal data breaches, data controllers should have a legal obligation to notify the individuals whose data has been compromised so that they can take stronger protective measures and obtain access and seek correction of any

inaccurate data or misuse resulting from the breaches. They should also review their data retention policies and improve their security practices. For example, data controllers might be required to cooperate with criminal law enforcement agencies and other authorities.

Data controllers should be subject to penalties proportionate to the harm or risk incurred for noncompliance with the duty to safeguard and protect data. All of this should be provided for in national law.

Seventh Principle: Accuracy of Data

"Personal data should be kept accurate and up to date to the extent necessary for the purposes of use."

When personal data is collected and retained for continuing use, the data controller has an obligation to take steps to ensure that the data remains as up to date, complete, and accurate as necessary for the purposes for which it was collected and is being used, so that the rights of the data subject are not impaired.

Eighth Principle: Access and Correction

"Reasonable methods should be available to permit individuals whose personal data has been collected to seek access to that data and to request that the data controller amend, correct, or delete that data. If such access or correction needs to be restricted, the specific grounds for any such restrictions should be specified in accordance with domestic law."

Data subjects must have the right to access the data, so that they may challenge its accuracy. They must also be able to ask the data controller to amend, revise, correct, or delete the data in question, thereby exercising their right of rectification.

These rights of access and rectification are among the most important safeguards in the field of privacy protection. The right of access to personal data held by a data controller should be simple to exercise, although it may sometimes be subject to exceptions and limitations. If an individual's request for access is denied, the individual must receive an explanation of the reasons for the denial so that denials do not become arbitrary.

The national legal systems of some OAS Member States recognize a right of *habeas data*, by virtue of which data subjects may file a judicial proceeding to prevent or terminate an alleged abuse of their personal data. The specifics of this right vary from state to state. In some it is even a constitutional right.

Ninth Principle: Sensitive Personal Data

"Some types of personal data, given its sensitivity in particular contexts, are especially likely to cause material harm to individuals if misused. Data controllers should adopt privacy and security measures that are commensurate with the sensitivity of the data and its capacity to harm individual data subjects."

The term “sensitive personal data” refers to data affecting the most intimate aspects of individuals. Depending on the specific cultural, social, and political context, it might include data related to an individual’s personal health, sexual preferences, religious beliefs, political ideology, or racial or ethnic origins, sex, etc.

Improper processing or disclosure of such data would intrude deeply upon the personal dignity and honor of the individual concerned and could trigger unlawful or arbitrary discrimination or result in risk of serious harm to the individual. The nature of the sensitivity may vary from country to country.

Data controllers should be able to assess the greatest risks to data subjects if data is disclosed and should therefore be held accountable for the disclosure of sensitive data.

Tenth Principle: Accountability

"Data controllers should adopt and implement appropriate procedures to demonstrate their accountability for compliance with these principles."

The effective protection of rights of privacy and data protection rests on responsible conduct by the data controllers in both the public and private sectors. Privacy protection schemes must reflect an appropriate balance between government regulation and effective implementation by those with direct responsibility for the collection, use, retention, and dissemination of personal data.

Proper application of this set of principles depends on the ability of those who collect, process, and retain personal data to make responsible, ethical, and disciplined decisions about that data and its use throughout the data's lifecycle. These data managers must act as good stewards of the data provided or entrusted to them.

Data controllers should ensure that employees who handle personal data are appropriately trained about the purposes and procedures for the protection of that data through effective privacy management training programs.

Eleventh Principle: Transborder Flow of Data and Accountability

"Member States should cooperate with one another in developing mechanisms and procedures to ensure that data controllers operating in more than one jurisdiction can be effectively held accountable for their adherence to these principles."

In the modern world of rapid data flows and cross-border commerce, personal data is increasingly likely to be transferred across national boundaries. However, the rules and regulations in various national jurisdictions today differ in substance and procedure. In consequence, the possibility exists for confusion, conflict, and contradictions.

The central challenge for effective data protection policy and practice is to reconcile (i) the differences in national approaches to privacy protection with the modern realities of global data flow; (ii) the rights of individuals to access data in a transnational context; and (iii) the fundamental fact that data and data processing drive development and innovation. Any international data protection instrument should strive to achieve the proper balance between these goals.

Cross-border transfers should be permitted when data controllers take appropriate measures to ensure that transferred data is effectively protected in accordance with all of the principles. Member States should take the necessary measures to ensure that data controllers are held accountable for providing such protection.

Member States should work towards mutual recognition of accountability rules and practices, in order to avoid and resolve conflicts. They should promote the

cross-border transfer of data (subject to appropriate safeguards), and they should not impose burdens that limit the free flow of information or economic activity between jurisdictions.

Data controllers must take reasonable measures to ensure personal data is effectively protected in accordance with these principles, whether the data is transferred to third parties domestically or across international boundaries.

Twelfth Principle: Disclosing Exceptions

"When national authorities make exceptions to these principles for reasons relating to national sovereignty, internal or external security, the fight against criminality, regulatory compliance, or other public order policies, they should make those exceptions known to the public."

Given the increasing importance of protecting privacy, Member States should provide individuals with the basic rights needed to safeguard their interests by adhering to all of the principles on privacy and personal data protection. However, in some situations, they may be required to make exceptions for reasons related to overriding concerns of national security and public safety, the administration of justice, regulatory compliance, etc. Such exceptions should be the exception, not the rule.

III. IBERO-AMERICAN DATA PROTECTION NETWORK (RIPD)

The Ibero-American Data Protection Network (RIPD) is a product of the June 2003 Ibero-American Meeting on Data Protection in La Antigua, Guatemala. The CJI and the OAS Department of International Law have participated in a number of its meetings, including the meetings in Cartagena de Indias, Colombia, and La Antigua; Guatemala. At one of the most important of these meetings, the November 2016 seminar in Montevideo, Uruguay, the preliminary draft of the Ibero-American Standards was presented to the RIPD for comments and observations (development of the Standards had been agreed at the June 2016 meeting in Santa Marta, Colombia). The Standards were revised from the technical standpoint and finalized during the May 2017 RIPD workshop in Cartagena de Indias. They were approved by unanimous vote and formally proclaimed in open session at the June 2017 Ibero-American Meeting on Data Protection in Santiago, Chile.

These Standards give the region an essential tool with which to establish a set of common data protection principles and rights that the states can adopt and develop in their national laws. The resulting uniform rules will ensure effective exercise and protection of the right to the protection of personal data and facilitate personal data flows in the region and beyond, thereby strengthening economic and social growth and encouraging international cooperation in this connection among supervisory authorities in and outside the region, as well as international authorities and organizations.

The Standards can be summarized as follows:

The preamble notes that, in a number of states in the region, the protection of personal data is a fundamental right recognized in the constitution, in the form of *habeas data* (right to personal data protection) provisions, and even has a body of case law. The lack of harmonization in this area (not all states have legislation) makes it difficult to meet new challenges for the protection of this right created by constant, rapid technological progress and globalization in various fields. We need regulatory instruments that protect personal data, including the free flow of such data among states in the region, and a harmonized legal framework that provides adequate protection, with uniform rules that give all data subjects the same protection guarantees.

As stated in the General Provisions, the purpose of the Standards is to establish a set of personal data protection principles and rights that the states can adopt and develop in their national legislation, thereby guaranteeing appropriate processing of personal data, facilitating personal data flow among the states and beyond their borders, promoting regional social and economic growth, and encouraging international cooperation in this connection among supervisory authorities in and outside the region as well as with international authorities and entities.

The Standards define a series of terms to facilitate comprehension. Their subjective scope is private natural or legal persons and public authorities or bodies processing personal data in the course of their activities and functions. Their objective scope is personal data found on partially and/or fully automated physical media, regardless of the form or method of data generation or the type of media, processing, storage, or organization. Their territorial scope is the processing of personal data by controllers or processors established primarily within the territory of the states of the region or, when not established in this territory, as provided in the Standards.

The Standards also address general exceptions to the right to the protection of personal data. Limitations are permitted for reasons of national security, public security, public health, protection of the rights and freedoms of third parties, and public interest.

A very important provision involves the processing of sensitive personal data. Data controllers may process this data only when strictly necessary for the discharge of the powers and duties expressly established in the norms governing their activities; when complying with a legal mandate; when they have obtained the express, written consent of the data subject; or by reason of national security, public security, public order, public health, or protection of the rights and freedoms of third parties.

The Standards also spell out the principles of personal data protection—legitimacy, lawfulness, fairness, transparency, purpose, proportionality, quality, accountability, security, and confidentiality—and discuss each one.

In addition, the Standards discuss the rights of data subjects, which are the rights of access, the right of rectification, the right to erasure, the right to object to processing, and the right of portability. Under the right of access, data subjects are entitled to request access their own personal data in a data controller's possession and to be fully informed of the general and specific terms of its processing. Under the right of rectification, data subjects are entitled to require a controller to rectify their personal data when it is inaccurate, incomplete, or out of date.

Data subjects also have the right to request erasure or removal of their personal data from a controller's archives, records, files, and systems, so that it is no longer held or processed by the controller. Data subjects may also object to the processing of their personal data on grounds relating to their particular situation or when the purpose of processing their personal data is direct marketing, including creating profiles, to the extent that such activity is involved. This is known as the right to object to processing. Lastly, the right of portability of personal data means that, when personal data is processed electronically or by automated means, data subjects have the right to obtain and, if necessary, transfer to another controller a copy of any personal data they have provided to a controller or that is subject to processing. The copy must be provided in a structured, commonly used and machine-readable form that ensures continued usability.

The right of access (*derecho de acceso*) is the right of any individual to request and obtain, free of charge, a report showing his or her personal data subject to processing, its source (how it was obtained), and with whom it has been shared.

The right of rectification (*derecho de rectificación*) is the individual's right to rectify any inaccurate or incomplete personal data. It means that the authorities involved have a duty to maintain up-to-date files.

The right to erasure (*derecho de cancelación*) is the individual's right to erasure of his or her inaccurate or excessive data. The data is blocked and may only be accessed by the authorities, who will erase it unless there are legitimate reasons not to.

The right to object to processing (*derecho de oposición*) is the individual's right to not to have his or her personal data processed where there are legitimate grounds.

The right of portability (*derecho de portabilidad*) allows data holders to request a copy of personal data they have provided to the controller or that is subject to processing.

These rights of access, rectification, erasure, and objection, sometimes referred to [by their Spanish acronym] as ARCO rights, are well defined in the Standards, as is the right of portability.

The Standards also discuss the data processor and its activities, as well as all aspects of international transfers of personal data. International transfers of categories of personal data may be expressly limited by the national legislation of the region's states for reasons of national security, public security, public health, or public interest or to protect the rights and liberties of third parties.

With respect to the supervisory authorities, the Standards require each State to have one or more fully autonomous supervisory authority for personal data protection, as established by its national legislation. These authorities may be single- or multiple-person bodies. They must exercise their powers impartially and independently and be free from all direct or indirect outside influences. They may not solicit orders or instructions of any kind.

These Standards also address complaints, penalties, and the associated right to compensation of data subjects who have been harmed by a violation of their right to the protection of personal data.

In addition, the Standards encourage states to establish international cooperation mechanisms for strengthening international judicial assistance between states, as well as mechanisms for promoting and exchanging best practices and experiences in the field of personal data protection, including with regard to jurisdictional conflicts with third countries.

IV. RELEVANT INTERNATIONAL LEGISLATION

Within the international human rights system, the right to privacy is protected by the American Declaration of the Rights and Duties of Man (April 30, 1948). Article V of the Declaration reads: "Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life."

Article IX of the Declaration establishes "[t]hat every person has the right to the inviolability of his home."

And Article X States "[t]hat every person has the right to the inviolability and transmission of his correspondence."

Article 11 of the American Convention on Human Rights ("Pact of San José") (November 22, 1969) provides as follows:

1. Everyone has the right to have his honor respected and his dignity recognized.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

3. Everyone has the right to the protection of the law against such interference or attacks.

Within the universal framework, the right to privacy is governed by Article 12 of the Universal Declaration of Human Rights (December 10, 1948), which reads as follows:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 18 of the Declaration provides as follows:

Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19 establishes the following:

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20 of the Declaration reads as follows:

1. Everyone has the right to freedom of peaceful assembly and association.

2. No one may be compelled to belong to an association.

This right is also guaranteed in Article 17 of the International Covenant on Civil and Political Rights (1966), which reads as follows:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Article 18 of the Covenant provides as follows:

1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.

2. No one shall be subject to coercion which would impair his freedom to have or to adopt a religion or belief of his choice.

3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others.

4. The States Parties to the present Covenant undertake to have respect for the liberty of parents and, when applicable, legal guardians to ensure the religious and moral education of their children in conformity with their own convictions.

Article 19 reads as follows:

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

a) For respect of the rights or reputations of others;

b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

The Charter of Fundamental Rights of the European Union (2000) addresses the right to privacy in its Articles 1, 7,8, 10, 11, and 12, which read as follows:

Article 1. “Human dignity is inviolable. It must be respected and protected.”

Article 7. “Everyone has the right to respect for his or her private and family life, home and communications.”

Article 8.

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Article 10.

1. Everyone has the right to freedom of thought, conscience and religion. This right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance.
2. The right to conscientious objection is recognised, in accordance with the national laws governing the exercise of this right.

Article 11.

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
2. The freedom and pluralism of the media shall be respected.

Article 12.

1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.
2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.

The Charter of Fundamental Rights of the European Union therefore makes a distinction among all of these rights

With respect to the right to the free flow of information, in the Inter-American system it is established in Article IV of the American Declaration of the Rights and Duties of Man (April 30, 1948), as follows:

“Every person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever.”

The American Convention on Human Rights (November 22, 1969) addresses this right in its Article 13, which provides as follows:

1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure (a) respect for the rights or reputations of others or (b) the protection of national security, public order, or public health or morals.

3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
5. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar illegal action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

At the universal level, Article 19 of the Universal Declaration of Human Rights (December 10, 1948, provides as follows:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) establishes the following:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Article 14 of the American Convention on Human Rights (“Pact of San José) (November 22, 1969) establishes the right of rectification or reply, as follows:

1. Anyone injured by inaccurate or offensive statements or ideas disseminated to the public in general by a legally regulated medium of communication has the right to reply or to make a correction using the same communications outlet, under such conditions as the law may establish.
2. The correction or reply shall not in any case remit other legal liabilities that may have been incurred.
3. For the effective protection of honor and reputation, every publisher, and every newspaper, motion picture, radio, and television company shall have a person responsible who is not protected by immunities or special privileges.

V. CONCLUSION

The Inter-American system should have a model law on the protection of personal data that would give the states in the region that do not have data protection legislation a tool box of provisions to incorporate in their domestic legislation. For the region to have uniform rules, we need a set of common principles and rights that the states of the Americas can adopt and develop in their individual legal systems.

In modern society, information and knowledge technologies are increasingly vital to every aspect of daily life, and globalization has a similar impact. In recent years, states have emphasized the right to access public information in order to make the handling of public information more transparent. Today, countries have freedom of information laws, which are unquestionably necessary for citizens to exercise their right to take part in public affairs and for the authorities to fulfil their obligation of accountability in governance. They are also ideal tools for preventing, detecting, penalizing, and rooting out corruption. For these reasons, they strengthen democracy and the rule of law and foster a culture of transparency.

However, this right to access public information must be balanced by the right to the protection of personal data and privacy. While there should indeed be a right to access information, the law should also recognize a right to privacy and the protection of personal data.

Yet not all countries in the Americas have data protection laws or recognize the right of *habeas data*, which is necessary for the protection of fundamental human rights.

This is why the region needs a regionally appropriate model law on personal data protection that countries lacking domestic data protection legislation could adopt.

The model law could be based on the data protection laws of other countries in the region, including Mexico, Uruguay, Argentina, Colombia, Peru, and Nicaragua, or on the Standards for Protection of Personal Data recently approved by the Ibero-

American Data Protection Network (RIPD) and unanimously adopted at the 15th Ibero-American Meeting on Data Protection (20 to 22 June, 2017, Santiago, Chile). These Standards are also based on Ibero-American data protection laws.

We need to seek a balance between the right to access information and the right to the protection of personal data. In other words, we must balance the right of individuals to control how their personal data is collected, stored, and used against their right to access data and the right of individuals and organizations to use personal data for reasonable and legitimate business purposes in a secure and protected manner.

Thus, with a law on protection of personal data, we would achieve an equitable pairing: a law on access to public information alongside a law on protection of personal data.

* * *