**CJI/doc. 597/19**

# THIRD REPORT: UPDATE ON THE PRINCIPLES ON PRIVACY AND PERSONAL DATA PROTECTION

(Presented by Dr. Carlos Mata Prates)

In the *Second Report on the Updating of the Principles on Privacy and Personal Data Protection,* delivered on February 21, 2019, I provided a review on the work of the Inter-American Juridical Committee (CJI), pursuant to the resolution of the General Assembly of the Organization of American States AG/RES. 2811 (XLIII-O/13), which culminated in the Committee resolution (CJI/RES. 212 (LXXXVI-O/15) dated March 27, 2015 through which the entity decided to *"Approve the report of the Inter-American Juridical Committee on Privacy and Personal Data Protection*, document *CJI/doc. 474/15 rev.2, attached to this resolution. 3. To convey this resolution to the Permanent Council of the Organization of American States. 4. To conclude the work of the Inter-American Juridical Committee on this topic"*.

It is convenient to note that the Second Report also included a description of the philosophy and of the technique used and developed by the Committee for the drafting of the *Declaration of Principles on Privacy and Personal Data Protection.*

Subsequently, the resolution of the General Assembly of June 5, 2018 - AG/RES. 2926 (XLVIII-O/18) - International Law, item *"i. Remarks and recommendations to the CJI Annual Report"* established a mandate for the CJI to *"Start updating the Principles on the Protection of Personal Data, taking into consideration the progress of same"*.

We should mention here that, as mentioned in the Second Report on the topic, the Committee, taking into account – among other aspects – the Standards for the Protection of Personal Data for the Ibero-American States drafted by the Ibero-American Network of Protection of Personal Data (RIPD) and the new norms of the European Union on the issue, decided, during its 92nd Regular Session – which was held from February 26 to March 2, 2018 in Mexico City – to include this topic on its agenda again.

The concept of privacy, as mentioned before, is

> "*clearly established in Article V of the American Declaration of Rights and Duties of Man (1948) and on articles 11 and 13 of the American Convention on Human Rights ("San José Pact") (1969) (Appendix A). The Inter-American Court of Human Rights has confirmed the right to privacy. In addition, the constitutions and the fundamental laws of many OAS Member States guarantee the respect and the protection of privacy, personal dignity and family honor, the inviolability of the home and of private communications, personal data and related concepts … In addition, the fundamental principles of freedom of expression and of association and the free flow of information, are enshrined in the main systems of human rights worldwide, among them in the OAS system".*

In turn, the area of enforcement comprises also the public and private organizations as regards the data they themselves create, comply or manage.

As regards the *Principles on Privacy and Personal Data Protection*, they are specified as follows:

**Lawful and Fair Purposes**: Personal data must be compiled solely for lawful purposes and through fair and lawful means;

**Clarity and Consent**: The aims for which personal data are compiled must be specified at the time of compiling them. As a general rule, personal data must only be compiled with the consent of the person they refer to;

**Pertinence and Necessity**: Data must be veridical, pertinent and necessary for the purposes mentioned in the compilation;

**Restricted Use and Withholding of Data**: Personal data must be maintained and used solely in a lawful manner compatible with the aim or aims for which they were compiled. They should not be withheld longer than necessary for their purpose or purposes and in conformity with the related domestic legislation;

**Duty of Confidentiality**: Personal data must not be disclosed, or made available to third parties nor be used for purposes other than those for which they were secured, except with the knowledge or consent of the person in question, or in case of legal authorization;

**Protection and Security**: Personal data must be protected by means of reasonable and adequate safeguards against unauthorized access, loss, destruction, use, modification or disclosure;

**Data Accuracy**: Personal data must be accurate and updated as required for the purposes of their use;

**Access and Correction**: Reasonable methods must be established for allowing persons whose personal data has been complied to request the controller thereof to modify, correct or delete them. Should there be any constraint on such access or correction, justification must be given for the reasons behind any of such constraints, in compliance with national legislation.

**Sensitive Personal Data**: In view of their sensitivity in certain contexts, some types of personal data are particularly likely to cause considerable harm to people if misused. Data controllers must take steps that ensure the privacy and security thereof, aligned with the sensitivity of the data and their capacity to harm individuals addressed by this information;

**Responsibility**: Data controllers shall adopt and implement the corresponding steps as red to comply with these principles.

**Transborder Data Flow and Responsibility**: The Member States shall cooperate among themselves in order to create mechanisms and procedures ensuring the data controllers operating in more than one jurisdiction may be effectively held liable for any failure to comply with these principles.

**Disclosure of Exceptions**: When national authorities establish exceptions to these principles for reasons related to national sovereignty, internal or external security, fighting crime, compliance with regulations or other public prerogatives, they must publicly disclose such exceptions.

As mentioned in the Second Report on Updating these Principles, I beg to reiterate that the work of the CJI on the *OAS Principles on Privacy and Personal Data Protection* remains fully effective, although requiring efforts in greater depth, and if the Committee shares the Report, the remarks should include the following points:

a) so-called ***Anonymization,*** taken as being roughly *"the application of steps of any type intended to prevent the identification or reidentification of a natural person without disproportionate efforts"*;

b) the links with and effects of the Principles with Internal Rights, on the understanding that the Principles establish a threshold, which does not prevent Internal Rights from establishing systems with stronger guarantees for individuals than those established in the former;

c) the treatment of personal data when related to children and adolescents;

d) the right to portability for personal data;

e) expansion of the legitimation of natural persons related to deceased personas or designated thereby in the established terms, for exercising the right of access, correction, cancelation, opposition, and portability;

f) adopting a broader concept, the so-called *Right to be Forgotten* may be included;

g) the inclusion of pro-active responsibility as a principle; and

h) the establishment of *security as a substantive principle*.

Finally, should the views set forth in this Report be shared, steps must be taken to include the principles mentioned in the text prepared by the Committee, with the necessary structural harmonization and development, thus ensuring compliance with the mandate assigned by the General Assembly.

I am available to the Committee for any clarification or expansion of this rapportership.