Department of International Law
Secretariat for Legal Affairs

WEBINAR
"PROTECTION OF PERSONAL DATA: INNOVATION AND MANAGEMENT DURING AND AFTER THE PANDEMIC"

JUNE 1ST, 2020

SUMMARY OF CONCLUSIONS

I. PROTECTION OF PERSONAL DATA AND COVID-19: WHERE ARE WE?

DR. JONATHAN MENDOZA ISERTE
SECRETARY FOR PROTECTION OF PERSONAL DATA
NATIONAL INSTITUTE FOR TRANSPARENCY, ACCESS TO INFORMATION AND PROTECTION OF PERSONAL DATA (INAI), MEXICO

- It is false that we have to choose between enjoying our privacy and enjoying health; both rights are fundamental and are not mutually exclusive.

- The technology that enables the collection and processing of personal data offers valuable opportunities to strengthen efforts aimed at social development, but in the absence of effective controls and limitations, this capacity may end up eroding respect for human rights.

- In addition to the rights highlighted by the Inter-American Commission on Human Rights (IACHR) in its resolution 01/2020 "Pandemic and Human Rights in the Americas" (consent, limited purpose, and the right to the cancellation of personal data), the rights of access to and rectification of the sensitive information that is obtained when applying COVID-19 tests or undergoing medical care must also be protected.

- Our migration to digital life confronts us with the enormous digital divide that exists in the region. That is why, within their authority, the public institutions that are in charge of promoting human rights in a democratic system must become and serve as a differentiating element.

- INAI has created the COVID 19 Secure Personal Data microsite, which, in addition to putting a large volume of information in the hands of citizens, offers them practical recommendations to take care of their personal data and informs them about their rights and resources to report an improper treatment of their data. It also includes good practices for those responsible for health services and recommendations to avoid causing harm or discrimination in the provision of these services based on the personal data that people may or may not provide when interacting with these services.

DR. LUIS DE SALVADOR CARRASCO
COORDINATOR
UNIT FOR EVALUATION AND TECHNOLOGICAL STUDIES (UEET),
SPANISH AGENCY FOR DATA PROTECTION (AEPD)

- The management of a health crisis should not be based on fear of the political and media impact of adopting a series of harsh measures, nor on ignorance-based decisions. To prevent this health

crisis from becoming a privacy crisis, it is necessary that the decisions made right now are based on scientific evidence, and that the treatment of data is understood as a whole, recognizing the inherent human rights implications and avoids using technology as a stand-alone remedy for everything.

- The principle of fairness of the General Data Protection Regulation (GDPR) implies that the treatment of personal data must actually be consistent with the purpose and function for which it was collected. This must be determined using organizational and scientific criteria; for example, it is not enough to conduct COVID-19 tests if the results are not obtained and communicated to the patient in a reasonable period, together with the corresponding instructions and medical resources. Otherwise, such data processing does not satisfy the fairness requirements.

- The purposes of processing personal data in the context of the pandemic may be classified as: i) quarantine and social distancing control; ii) pandemic expansion controls; iii) controls on the use of facemasks and gatherings; and iv) the epidemiological study. None of them requires the level of intrusion that is being inflicted by many of the newly developed applications.

- It is important to determine what will happen to the personal data that has been collected in this context and to have measures in place to prevent this information from leaking, guarantee the quality of the data, prevent abuse and discrimination, and reduce the risk of re-identification. These measures should not imply a relaxation of the security and privacy guarantees; they must be transparent and temporary.

II. Looking Ahead: What happens next?

Dr. Eduardo Bertoni
Director
Agency for Access to Public Information, Argentina

- Privacy protection has been constantly evolving over the years. The way in which we protect or fail to protect our data changes over time due to sporadic public explosions that draw our attention to the importance of protecting our personal data and gradually change our behavior, followed by regulatory issues, as was the case with the Edward Snowden and Facebook \ Cambridge Analytica scandals. But this does not necessarily mean that the current pandemic is going to trigger a cultural shift in our relationship with our personal data, it is just another call for attention.
- The obligation to destroy personal data once the purpose for which it was collected has been satisfied will represent the greatest challenge for the authorities in charge of monitoring this destruction. The enormous collection of personal data carried out during the pandemic includes sensitive data and must be conducted in a way that also satisfies the different international instruments that include the principle of purpose of said collection.
- Data protection authorities should ask specific questions to governments and companies that operate data collection applications to manage the pandemic, ensuring that they are complying with, at a minimum, the general recommendations on the treatment of personal data collected in this context.

III. TOWARDS A REGIONAL MODEL

DR. MARIANA SALAZAR ALBORNOZ
MEMBER
INTER-AMERICAN JURIDICAL COMMITTEE (CJI)

- A pandemic can trigger human rights violations, due to the state of emergency in which certain rights are suspended, including the right to privacy. That is why it is important to guarantee the protection of personal data through clear and updated standards. However, the frequency and ease with which personal data and people flow across borders makes the protection of personal data an international issue, which merits a homogeneous approach that protects it at the regional level.

- At the international level there are very important regional standards in the OECD, the Council of Europe, and the African Union, among others. In our region there are the Ibero-American Standards adopted in 2017 by the Ibero-American Network of Personal Data, made up of various government agencies from some OAS Member States. These Standards manage to establish a minimum common denominator among the members of the Network. In this sense, the CJI seeks to extend this standardization to the 35 Member States of the Organization.

- The CJI has studied the subject of personal data protection since 1996. This work has translated into the adoption of Principles for Privacy and Protection of Personal Data (2012), a Legislative Guide to implement those Principles (2015) and it now seeks to incorporate to the Principles the most important and recent developments to achieve a cutting-edge regional standard, in accordance with a mandate conferred in 2018 by the OAS General Assembly.

- In its review of the 12 Principles of 2012, the CJI proposes to incorporate the different approaches that the OAS Member States have on each Principle, which will give added value to this work, although in most cases these approaches are quite similar. This review will also attempt to strengthen the provisions related to: i) consent for the processing of personal data, ii) confidentiality, iii) rectification, cancellation and portability of personal data, and iv) cross-border flow of personal data, among others.

NOTE: The Department of International Law will be periodically reporting on the development of this proposal both in the Inter-American Juridical Committee and, at the appropriate time, in the OAS political bodies.