Tomás Arankowsky-Tamés Partner
tomas@avafirm.com
AVA, Mexico City

Image: Thomas Kelley / Unsplash.com

Mexico: Trends and developments in data protection

Mexico's Federal Law on the Protection of Personal Data Held by Private Parties was passed in 2010, creating a regime that the Mexican data protection authority, the National Institute for Transparency Access to Information and Data Protection ('INAI'), has since been interpreting, developing and enforcing. Tomás Arankowsky-Tamés, Partner at AVA, provides a breakdown of INAI's work and the main data protection challenges facing Mexico today.

In previous contributions, I outlined that the issue of data protection in Mexico is not just a recent one, but a very fast evolving topic on the public agenda. It is not a secret that, in Mexico, the existence of legislation on the matter is quite recent in comparison with other jurisdictions with more robust and lengthy traditions of protecting personal data.

Since its creation, INAI has been the authority in charge of enforcing data protection at the federal level. INAI has made great efforts towards raising awareness about the relevance of data protection, with good results despite having suffered an important increase in its obligations, which now also include enforcing and supervising the freshly enacted public transparency requirements.

Data protection, INAI's original institutional obligation and the reason for its conception, remains an issue that keeps the authority on its toes. INAI received over 2,000 complaints from data subjects between 2011 and 2017, of which 1,600 developed into preliminary investigations. Around 95% were concluded and more than 180 of them led to the launch of sanctioning proceedings against private companies that violated their obligation to protect personal data, resulting in fines (in over 150 cases) amounting to over MXN 350 million (approx. $20 million). This, at least by Mexican standards, is a significant amount of money, especially for small and medium-sized enterprises. Among the most sanctioned industries, continuing with the trend observed in prior years, are banks and financial institutions (including insurance companies), retail stores, mass communication companies and hospitals and health service providers.

In this very same period, INAI processed over 900 complaints regarding the exercise of individuals' rights to access, rectify, delete and oppose data processing ('ARCO rights'), which were not correctly handled by private entities. Non-compliance with the right to access personal data amounted to around 30% of such requests, and in a recent decision, INAI fined a hospital over MXN 4.5 million (approx. $230,000) for denying a patient access to their medical records.

In a study carried out with another governmental entity examining data practices in Mexico, INAI identified that 44.4 out of 46.3 million people over 18, living in communities of at least 100,000 inhabitants, have shared some kind of personal information with public entities. The personal data includes names (42.9 million), addresses (42.1 million), telephone numbers (39.8 million), health statuses (23.7 million), emails (22.5 million), wages or income (17.7 million) and credit card information (10.8 million). INAI also determined that 36.6 million people have shared this kind of information (in similar proportions) with companies in the private sector.

It is also worth mentioning that, according to INAI, 84% of the Mexican population is worried or in some way worried about the misuse of their personal information. But INAI highlighted that around 50% of those over 18 living in urban locations own some kind of social network (for professional or leisure purposes) and that, of these, almost 90% have shared at least one form of personal data in addition to their name. What also seems to be a trend regarding

INAI has made great efforts towards raising awareness about the relevance of data protection, with good results despite having suffered an important increase in its obligations.

Mexican data protection is the existence of more sophisticated schemes dealing with the use and transfer of personal data. In the same measure that people are becoming more and more aware of the relevance of protecting their information, the schemes for using, storing and transferring it are becoming more complex.

Nowadays, companies are more inclined to invest in robust and complex security measures to ensure that any and all personal data in their possession is being processed lawfully. Companies are now far more careful about, for example, executing agreements with third parties regulating the transfer and processing of personal data. Step by step we are leaving behind those days in which companies believed that merely having a privacy notice was sufficient to comply with their legal obligations. However, we are still very far from full compliance.

Personal data has also transcended the idea of merely protecting an individual's personal information. Under Mexican telecommunications laws, any authorised telecommunications company is legally obliged to preserve certain personal information about their clients that, based on a judicial order, will be shared with security agencies to either provide a certain location in real time or share certain information regarding the length and location of a user's conversations.

This is done with the understanding that this information can help fight crimes such as kidnapping or extortion. In these kinds of cases, the exercise of ARCO rights has been at the very centre of the discussions by both those who defend these provisions and those who argue that they are a blatant invasion of subscribers' rights.

In this same context, and maybe due to the fact that data protection has not been fully understood in some sectors of the Mexican population, we have seen an increase in cases before INAI where private entities are being accused of infringing their data protection obligations by individuals that have suffered identity theft or have had their credit cards cloned, causing financial loss. There have not yet been any sanctions imposed by INAI against the companies responsible for these kinds of cases; however, many of these cases remain under investigation.

Another very relevant development comes not from how the private sector deals with personal data but how public entities do so. This is not a minor issue considering the vast amount of personal data governments and other public and social institutions collect from citizens, affiliated users and the like.

On 26 January 2017, the Federal Government published in the official gazette the General Law on the Protection of Personal Data Held by Mandated Subjects ('the Public Sector Law'), which came into effect the following day. This law, which is based on, and regulates portions of, the Mexican Federal Constitution, seeks to establish, in its own words 'bases, principles and proceedings to warrant the right of any person to the protection of their personal data' that falls into the hands of certain 'mandated subjects.'

The definition of mandated subjects is quite broad as it encompasses any authority or public organisation (including political parties, public trusts and public funds) from any of the branches of government (executive, legislative or judicial) or any level of government (federal, state or municipal). The idea was to create a specific law that deals with how these entities process, store and use personal data from the general public. It foresees provisions that oblige them to publish privacy notices explaining which personal data are collected and for what purposes. It also contains provisions on how data subjects can exercise their ARCO rights.

Other relevant provisions include:

- the creation of the National System for Transparency, Access to Information and Personal Data Protection ('the System') which, in connection with the latter, aims to coordinate and evaluate the public policies enacted to protect personal data and achieve full compliance by mandated subjects. The System is also responsible for the creation of the National Programme for Personal Data Protection, which is an instrument designed to outline specific goals and objectives to be complied with or achieved by the mandated subjects with regard to protecting personal data;
- outline which conducts are considered to infringe the Public Sector Law and foresees criminal and administrative sanctions;
- regulate how a mandated subject can transfer personal data to third parties;
- create specific obligations for gathering, maintaining and using personal data by security and law enforcement agencies; and
- foresee diverse enforcement mechanisms in connection with personal data in the possession of mandated subjects.

Due to the recent enactment of the Public Sector Law, data related to its enforcement does not provide sufficient elements to determine whether or not it is being properly complied with. However, due to the federal elections that will be taking place in Mexico in July, it has been put to the test since the National Electoral Institute, which is the authority in charge of organising the elections, is currently in charge of preserving not only the data of all voters but also the data of those who support an independent candidate for any public position, which is clearly not an easy task.

New legislation to make accountable those who were not in the past; judicial and administrative cases and criteria tackling, at least by Mexican standards, innovative approaches and practical applications of data protection; and an increase in public awareness regarding the importance and relevance of protecting personal data, as well as the risk associated with not doing so properly, allow us to predict that Mexico will continue moving forward on this matter amid a young and perfectible data protection system.