Protecting data in Mexico: what you need to know

The Mexican statute governing the processing, transfer, use and storage of personal data has been in place for six years, as **Begoña Cancino** of Creel, García-Cuéllar, Aiza y Enriquez reports.

In the last few years, the creation, storage and general use of databases in Mexico have been subject to new legal treatment in relation to personal data.

The Mexican Copyright Law, enacted in December 1996, included the primary approach to protecting databases when the selection and arrangement of data showed some originality. However, such protection was not bestowed to the data itself.

The only specification contained in the copyright law covering databases that contain personal data is that the access to such private information shall be subject to the prior authorisation of the interested parties, except in cases where a court order is required.

The lack of a proper legal mechanism intended to protect the rights of personal data owners was a clear issue until the enactment of the Federal Law of Personal Data held by Private Parties (DPL) in 2010. Before that, we had a legal mechanism to protect the database as a work of authorship, but not one for the rights of individuals to protect their own personal information per se.

Before the DPL, the only way to prevent the unauthorised disposal of a database containing personal data was through the initiation of an administrative action whereby the owner of the copyright to the database enforced its exclusive rights. Even in such a scenario, there was no possibility for the owner of the related data to enforce its own right to challenge the unauthorised use of its personal information in the administrative ground.

In July 2010, the statute that governs every aspect of the processing, transfer, use and storage of personal data in Mexico became effective. This legal instrument included provisions to regulate the purposes for which companies collected such information, the way they stored it, with whom they shared it, and when and how they deleted the information after it was used (these activities as a whole are defined as "processing" by the DPL). It also governed the protection afforded to the owner of the copyright to the corresponding database.

In general terms, the DPL imposes obligations on all business or individuals that process personal data ("data controllers"); governs how individuals ("data subjects") may control the way data controllers use their personal data, mainly through the exercise of their rights of access, rectification, cancellation and opposition; and provides for several penalties aimed at deterring and sanctioning conduct that violates the use of personal data.

1. **Obligations on processing personal data**
   According to the DPL, data controllers must collect and process personal data in a lawful manner. The general rule is that data controllers must obtain the consent of data subjects in order to process their personal data. When personal data cannot be associated with the data subject by way of its structure, content or degree of dissociation, then consent will not be necessary to process such personal data.
2. **Obligations on transfer of personal data**
   With respect to the transfer of personal data to domestic or foreign third parties other than the data controller, the DPL establishes that it does not require a notification to the Federal Institute for Access to Public Information and Data Protection. However, the data controller must inform the data subject about the transfer in the privacy notice and provide the transferee with such a document so it can process the information.
3. **Information shared with employees**
   According to the DPL, data controllers are legally bound to inform data owners about which personal data is collected from them and for what purpose through the privacy notice.
4. **Domestic data security measures**
   In terms of the DPL, all responsible parties involved in the processing of personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorised use, access or processing. The DPL is silent on the specific measures that shall be taken, but it clarifies that data controllers will not adopt security measures inferior to those they keep to manage their own information.
5. **Other relevant points**
   It is important to consider that the processing of sensitive data deserves special treatment under the DPL. For example, for the creation of databases containing sensitive data, the DPL establishes that such databases may not be created without justification of the purposes, which must be legitimate, concrete and consistent with the explicit objectives or activities pursued by the data controller.

"FOR THE CREATION OF DATABASES CONTAINING SENSITIVE DATA, THE DPL ESTABLISHES THAT SUCH DATABASES MAY NOT BE CREATED WITHOUT JUSTIFICATION OF THE PURPOSES."

The processing and transfer of sensitive data is not prohibited by the DPL, but this type of information deserves special treatment which should be observed during its processing in order to avoid further risks (such as the imposition of sanctions in specific cases).

Mitigating factors will depend on the specific activity that would be sanctioned under the DPL and should be determined case by case, but in practice, dissociation of information becomes a useful course of action to avoid the obligation to obtain the consent for processing data, only to the extent that such a process is sufficient to avoid the identification of the data subject. The issue with dissociation then becomes a risk from the copyright perspective, when such dissociation is conducted without the proper authorisation of the author or copyright owner of the database.

When we refer to works of authorship related to databases and such databases contain personal data, fair use from the copyright standpoint is not the only issue to be aware of. In fact, in such cases, the more important aspect to consider is avoiding unauthorised disclosure and any kind of harm to the data subject that might be caused with the disclosure of its personal data.

In any case, the right to use a database shall not be misunderstood as the right to freely exploit personal information without observing the provisions contained in the DPL. ■

Begoña Cancino is a partner at Creel, García-Cuéllar, Aiza y Enriquez, where she heads the intellectual property and entertainment practice. She has experience in all aspects of IP, data privacy and administrative litigation including counselling and litigating patents and trademarks. She can be contacted at: begona.cancino@creel.mx

Bennian / Shutterstock.com