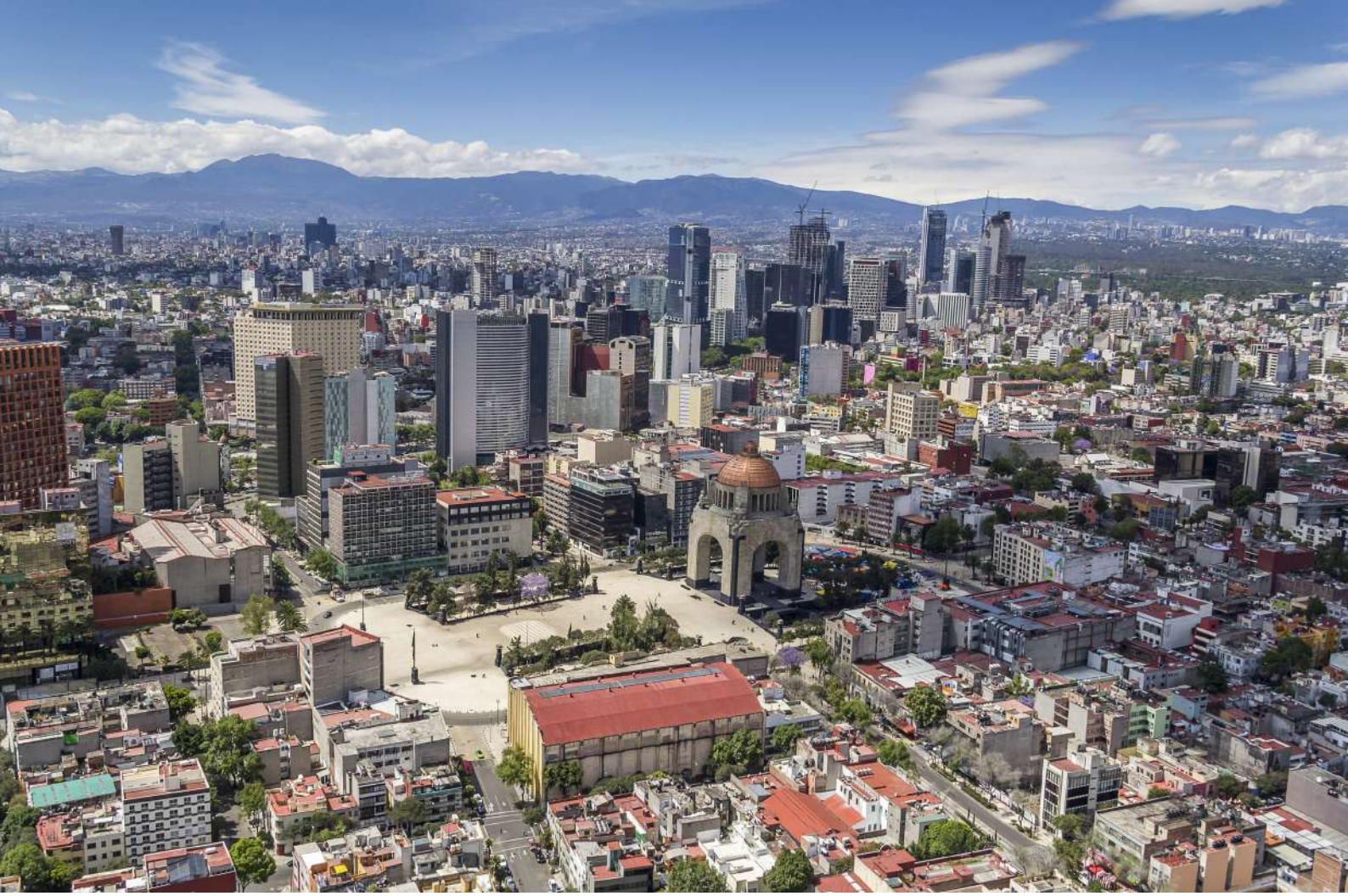


PRIVACY AND CYBERSECURITY IN

MEXICO

Begoña Cancino, partner of the IP practice at Creel, García-Cuéllar, Aiza y Enriquez, SC, has taken the lead from the issuance of the Mexican Privacy Law, this approach of the firm to handle data privacy matters from the basis of an IP expert has been very successful, as personal data is assembled in databases that constitute a work of authorship under the Mexican Copyright Law and also constitute confidential information that may qualify as a trade secret under the Mexican Industrial Property Law. Begoña's IP background gives her a better sense of her clients' needs and the different angles that should be considered when providing the most specialised advice in the field.

Recognised as Up and Coming in 2017 by *Chambers and Partners*, Begoña has authored several articles for the *World Intellectual Property Review* (Protecting Data in Mexico: what you need to know) as well as published in the 2015 and 2016 editions of *The Data Protection and Privacy Global Guide* and *IP in Business Transactions* by Thomson Reuters. She also authored the Mexican chapters for the *International Comparative Legal Guide on Data Privacy 2017, Cybersecurity 2018*, as well as *Gambling 2018*.

Begoña received her law degree from Universidad La Salle in 2001; postgraduate studies at the University of Buenos Aires; Universidad Nacional Autónoma de Mexico and participated in the Leadership and Management Program for Lawyers, both at the Yale School of Management.

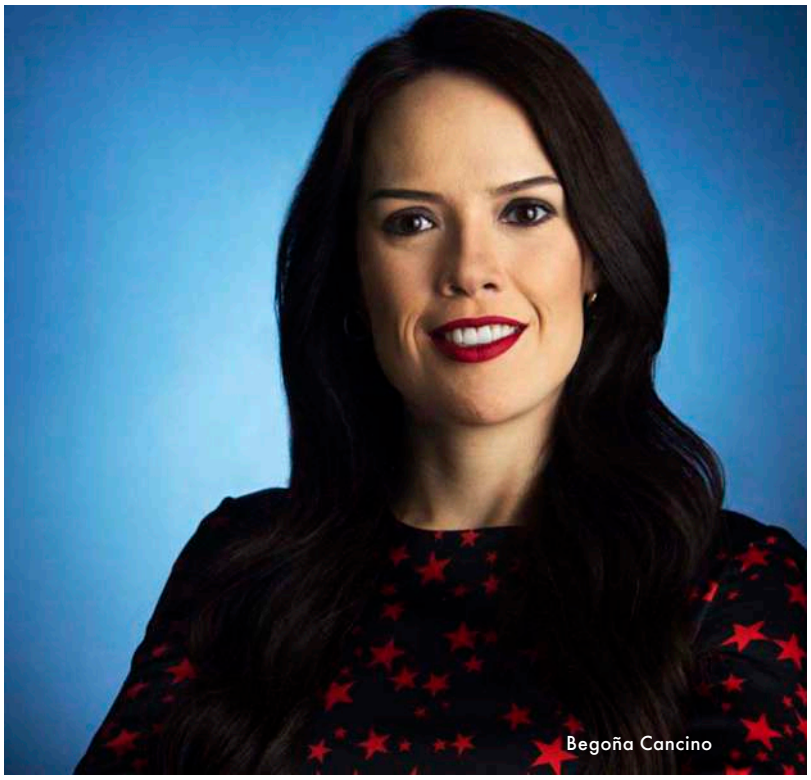
GTDT: What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

On 7 November 2017, members of the Chamber of Deputies (mainly from the green party) proposed a legal initiative with the aim to introduce specific provisions into our federal criminal system, as well as to adopt the Convention on Cybercrime (Budapest Convention) for Mexico to be part of a global net of countries devoted to secure information in cyberspace and use it as the basis of all required legal reforms. Currently, the Federal Criminal Code provides for certain crimes related to IT systems protected by security measures; however, it does have failures that range from the absence of a specific definition for the term 'security systems' and 'cybercrime' (the latter only defined in the National Cybersecurity Strategy, whose provisions are non-binding until they are elevated to law), to cyberbullying or malware not being treated as a crime. In particular, legal initiative is intended to designate as cybercrime the following conduct: (1) hacking; (2) phishing; (3) identity theft; (4) child pornography/grooming and (5) cyber fraud; as well as to incorporate into the National Code of Criminal Procedure all the investigative steps required to obtain evidence stored digitally to preserve data and obtain such data, while protecting personal data and collaborating effectively with other jurisdictions to comply with data transfer and other processing restrictions.

On a separate note, on 12 June 2018, the Mexican Official Gazette published that Mexico has adopted the Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross-border data flows. Both are binding international instruments that protect the individual against any abuse of the collection and processing of personal data and they seek to regulate at the same time, the cross-border flow of personal data.

GTDT: When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The Federal Law for the Protection of Personal Data held by Private Parties includes the data controller's obligation to 'immediately' notify the breach to any data subjects that may be affected significantly in terms of their economic or moral rights, but no requirement to notify the federal regulator is set forth in the relevant law. In this regard, the key factor to be assessed by organisations when deciding whether to notify


Begoña Cancino

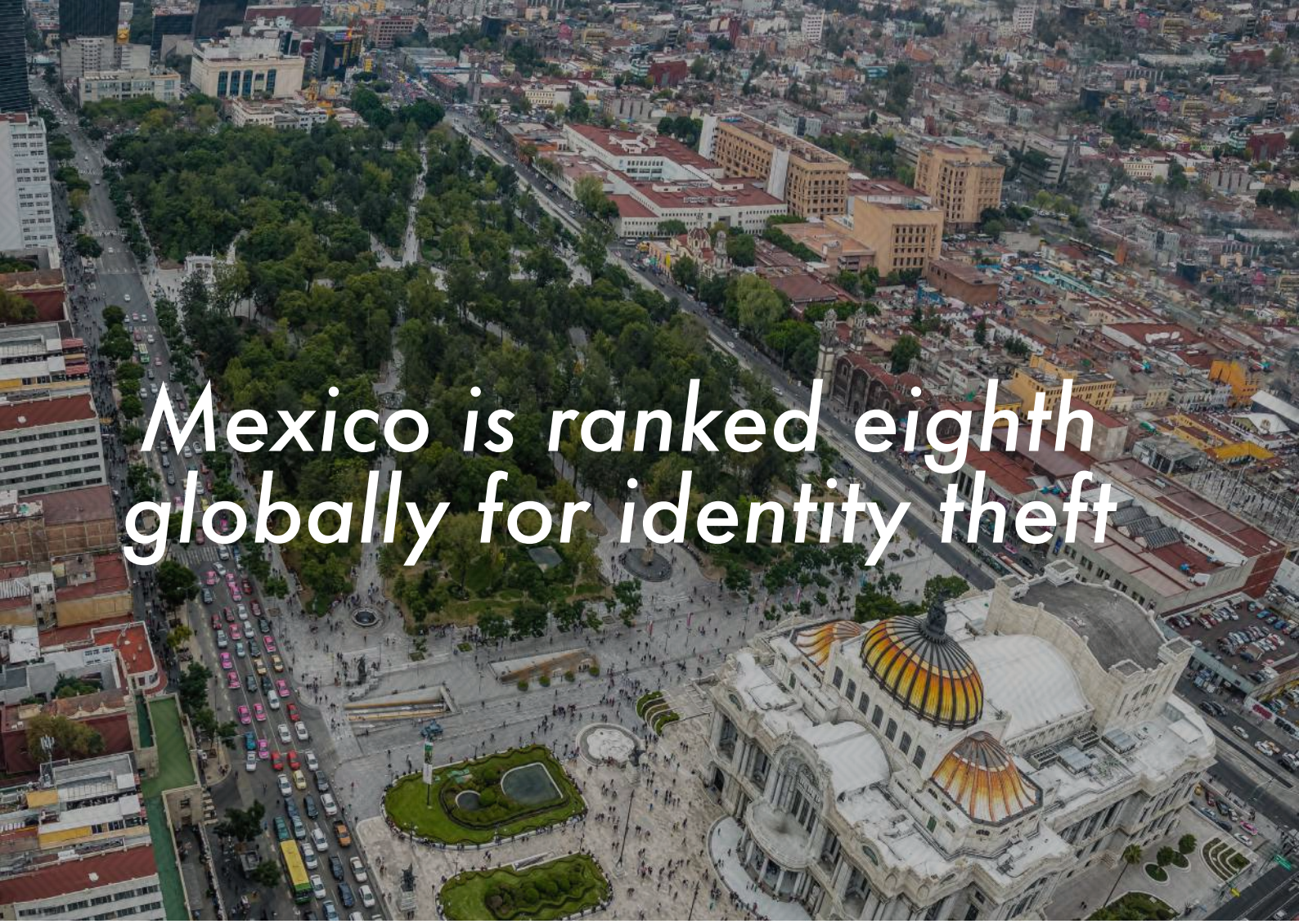
data subjects or not would be the sensitivity of the personal data compromised and to what extent its misuse could affect data subjects, not only from an economic but also from a moral perspective.

GTDT: What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The biggest issue in a data security incident is assessing the extent of the breach (and therefore, the need for reporting it to affected parties) by first confirming whether personal data is compromised and if so, what type of personal data (sensitive or not) and how many subjects are affected by the breach (this, along with the proper identification of the affected parties, is crucial for notification purposes). In addition to the assessment of the extent of the breach, companies should implement corrective, preventive and improvement measures to make security measures adequate to avoid a repeat breach. Such measures should be notified to data subjects, along with the nature of the breach, the personal data compromised, the recommendations to data subjects after the breach and the means available for data subjects to obtain more information of the event, if that notification is necessary, under Mexican provisions.

GTDT: What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

To be prepared for a security incident and improve security measures within the company, the Mexican regulations provide for certain obligations to data controllers, such as: prepare an



Mexico is ranked eighth globally for identity theft

inventory of personal data and processing systems; determine the duties and obligations of those who process personal data; make a risk analysis of personal data identifying, by level, dangers and estimated risks; establish security measures and identify those effectively implemented so far; analyse the gap between existing security measures and those missing but necessary for the protection of personal data; prepare and update a work plan for the implementation of the missing security measures arising from the gap analysis; train personnel and keep a record of personal data storage media.

Likewise, the Mexican regulator, the Federal Institute for Transparency, Access to Information and Protection of Personal Data (INAI), has set out a document including 10 security recommendations for preventing theft of personal data in the digital environment.

GTDT: Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud-hosting environment?

Under Mexican Regulations on personal data held by private parties, data controllers (companies that collect and process personal data for commercial purposes) should only use services that ensure the proper protection of the personal data they gather. Cloud computing is a model for the external provision of on-demand computer services that involves the supply of infrastructure, platform or software distributed in a flexible manner, using virtual procedures on dynamically shared resources. The data controller should enter into service agreements with at least the following contractual conditions for the service provider: (1) it shall use similar policies to protect personal data to those reflected in Mexican law; (2) if the service provided involves subcontracting, such provisions should be transparent; (3) it should not assume any ownership of the information about which the service is provided; (4) it should maintain confidentiality with respect to the personal data it holds. In addition, the service provider should as a minimum have mechanisms in place for: (1) disclosing changes in its privacy policies and the services provided; (2) permitting the data controller to limit the type of processing of personal data included in the service provided; (3) establishing and maintaining adequate security measures to protect data included in the service provided; (4) ensuring the suppression of data after the service has been provided; (5) impeding access to non-authorised parties and informing the data controller if there is an official request of data from a competent authority, and last but

THE INSIDE TRACK

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

A multidisciplinary team that can provide legal advice and coordinate the required technical assistance to solve client's issues, either for prevention or remediation. A team experienced not only in investigations but also in explaining the legal framework required by each industry in terms of data security, able to advise its clients and give training sessions to its employees so they can have a better sense of their duties in processing data in the course of each business.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Pursuant to the existing laws, pulverised provisions as well as lack of specific provisions to define cybercrimes. Difficulties encompassing legal and technical advice. The fact that Mexico is not party to any international instruments such as the Budapest Convention, nor has it been acknowledged as a country that ensures adequate data protection standards, are some of the difficulties that lead us to enter into private agreements or find other ways to revise our standards in corporate or other transactions.

How is the privacy landscape changing in your jurisdiction?

Although the Federal Law remains the same from its issuance in 2010, the Mexican landscape has been changing and it is expected to continue due to the international commitments adopted by Mexico with the aim of collaborating with other jurisdictions to ensure good practice in processing personal data.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

In this regard, companies should be able to differentiate between material and non-material harm under Mexican privacy laws by conducting a risk analysis. In so doing, companies will be able to determine if a breach should be notified to data subjects or if the company only needs to identify the gap between existing security measures and those missing but necessary for the protection of personal data and updating a work plan for the implementation of the missing security measures arising from the gap analysis. Material harm should be prioritised over non-material harm and will always depend on the business, scope, context and processing of the data compromised in the incident. Industry-specific risk identification of material and non-material harms is crucial then for all companies facing a cybersecurity incident, certain sectors such as the healthcare and banking should provide companies the required latitude to adapt their own internal policies.

Begoña Cancino
Creel, García-Cuéllar, Aiza y Enriquez, SC
México
www.creel.mx

not least, (6) informing the data controller of the events of the breach immediately after its occurrence, and providing the data controller with all the necessary information for assessing the extent of the damage caused by the breach, in accordance with Mexican legal provisions.

GTDT: How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

According to INAI and figures obtained from the official source of the National Commission for the Protection and Defence of Users of Financial Services, Mexico is ranked eighth globally for identity theft, 67 per cent of those reported cases, is owing to loss of documents; 63 per cent for robbery and 53 per cent for information taken directly from their credit accounts. In the third quarter of 2017, cyber fraud grew by 102 per cent compared with the same period in 2016, and represent a proportion from 13 per cent to 51 per cent per year. In 2016, one out of every 131 emails contained malware, since email was the first source of disseminating malware. In addition, Mexico takes second place in Latin America with the greatest number of cyber attacks to mobile devices. On 9 September 2017, the Officer of the General Prosecutor (PGR) announced in the Mexican Official Gazette a new investigation unit to combat cyber and technological crimes and enhance investigations. To March 2018, 312 files were opened by the unit to investigate crimes related to the distribution, storage and production of child pornography, initiated upon notices received from Interpol. The PGR unit is also actively working with the Bank of Mexico to identify and sanction all those responsible for a cyber attack on several financial institutions on the bank's interbank electronic payments system.

GTDT: When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Companies must conduct risk assessments (risk-based approach) arising from privacy and data security issues in M&A deals for them to make a decision. This is necessary not only when it comes to the target, but also for awareness of the mechanisms for exchanging personal data during the due diligence process. The risks in processing personal data should be assessed by reviewing

the applicable laws in the relevant jurisdictions, specifically concerning data security policies, security transfers, security breach notifications, limitation purposes and fair processing. Processing activities should be classified in terms of their risk in order for the company to prioritise compliance and devise appropriate remedies to reduce potential negative impact in people. It should be noted that there is an industry-specific risk in certain sectors, for example, in the acquisition of a private health institution, clearly there would be sensitive patient information involved that should be preserved during the due diligence process and safely transferred to the buyer post-closing. The global context should also be considered in cross-border transactions, where companies should assess the risk posed by their operation not only in their own but also in other jurisdictions with different legal regimes on data privacy that should also be respected. In short, each company has an obligation to consider the risk elements that apply to its own business and scope.