The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Mexico: Technology

This country-specific Q&A provides an overview to technology laws and regulations relevant in Mexico.

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the technology market.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Galicia Abogados SC

The Legal 500

Carlos Chávez, Partner
Regulated Industries, Compliance, Anti Trust

cchavez@galicia.com.mx

Diana Gonzalez, Associate
Infraestructure

dgonzalez@galicia.com.mx

Maite Celorio, Associate
Anti Trust, Compliance, Regulated Industries

mcelorio@galicia.com.mx

Arturo Portilla, Associate
Tax

aportilla@galicia.com.mx

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

Since 2014, telecommunications (namely, transmission or reception of signs, signals, data, images, sounds or information of any nature through physical or electromagnetic means), the networks through which such signals and information are transmitted, and the provision of telecommunication services (which services are considered as public services), are regulated by the Federal Telecommunications and Broadcasting Act ("FTBA" or "LFTR" for its acronym in Spanish).

With respect to telecommunications networks, the FTBA regulates the use and exploitation of the radio spectrum and orbital resources (that is, orbital slots), as well as the deployment, operation, access, interconnection, infrastructure sharing and neutrality of said networks. Under the FTBA, it is not mandatory to obtain a license for the deployment and maintenance of a telecommunications network, unless such network requires the use of public goods, such as radio spectrum or orbital slots, the use and exploitation of which does require a license.

Notwithstanding, the foregoing, the FTBA requires that a concession (i.e., a license) be obtained for the provision of wholesale or retail telecommunications services. This license (the "sole concession" or concesión única) is granted for the provision of all kind of telecommunication services in a convergent manner through a public network, regardless if the relevant network is owned by the concessionaire, a third party or a combination thereof. The scope of the sole concession is determined pursuant to the type of services that the concessionaire intends to provide.

In addition to the sole concession, under the FTBA the following activities require a specific authorization: installing telecommunications equipment and

transmission means that cross the borders of Mexico; exploiting signals and frequency bands related to foreign satellite systems for the provision of services in Mexico (landing rights); installing, operating or exploiting earth stations for the transmission of satellite signals; use radio spectrum frequency bands for diplomatic visits; and establishing and operating a telecommunications services broker (reseller). Brokers are able to resell services using third parties' capacity or networks, or to market their own telecommunications services.

2. **Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?**

The Federal Telecommunications Institute ("IFT" for its acronym in Spanish) is the Mexican regulator of the telecommunications and broadcasting sectors. IFT is a collegiate independent constitutional entity, meaning that IFT does not depend from any governmental authority or power and that it is empowered with technical and administrative autonomy. IFT was created with the following general purposes: regulating and promoting competition in the telecommunications and broadcasting sectors; regulating the telecommunications public networks from their deployment to their operation; granting, regulating and supervising the provision of telecommunications services; and safeguarding the rights of the users and audiences.

IFT possesses full technical authority and is designed as a specialized entity in telecommunications, broadcasting and competition in such sectors. Therefore, in principle, only the specialized courts on economic competition, broadcasting and telecommunications can exercise control (in the form of judicial review) over IFT. Notwithstanding the foregoing, these courts can exclusively review the legality of the actions of the regulator, but should in principle defer to the technical and regulatory discretion of the former.

3. **Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?**

Mexico's federal constitution allows up to 100% foreign investment in the telecommunications and satellite industries up to 49% in the broadcasting industry.

The FTBA, however, mandates that sole concessions and radio spectrum and orbital resources concessions, and all authorizations, be issued only to Mexican individuals or entities. Mexican entities (that is, entities incorporated in Mexico), in turn, are in principle domiciled in the country. The rationale of this requirement is that IFT may have and assert jurisdiction over all holders of concessions and authorizations that render telecommunications services in Mexico.

4. **Are there any regulations covering interconnection between operators? If so are these different for operators with market power?**

In order to promote competition in the telecommunications sector, the FTBA provides that concessionaries that operate telecommunications public networks shall interconnect their networks on a non-discriminatory basis, consequently, concessionaries operating public networks shall adopt open architectural network designs.

Given that IFT must ensure prompt and effective interconnection between networks, if the concessionaries do not agree on interconnection terms and conditions or if a concessionaire refuses to negotiate such interconnection, the regulator may intervene and determine the terms upon which two networks must interconnect.

IFT has the authority to declare that an economic agent (i) is the preponderant agent in the telecommunications or broadcasting industries and/or has market power in a relevant market or service within the telecommunications or broadcasting industries. Such declarations result (in the case of preponderance, and may result, in the case of market power) in the imposition of asymmetric regulation on the relevant agent, which in turn create obligations that other concessionaries do not have. Generally speaking, these measures consist in: (i) the obligation to provide access to infrastructure, (ii) rate regulation, and (iii) certain obligations with respect to acquisition of contents and/or entering into certain type of agreements.

5. **What are the principal consumer protection regulations that apply specifically to telecoms services?**

Consumer protection in the telecommunications space is a complex area in which both IFT and the Office of the Consumer Protection Attorney General (Procuraduría Federal del Consumidor or "PROFECO") share jurisdiction. IFT, on the one hand, has powers under the FTBA to set quality standards and monitor and enforce compliance with the same by the different telecommunications carriers. It can also enforce the rights of telecommunications services' users under the FTBA.

PROFECO, on the other hand, gets its authority under the Federal Consumer Protection Act (Ley Federal de Protección al Consumidor or "CPA"), which is a comprehensive statute setting forth the rules applicable to the relationship between consumers and suppliers in the marketplace across all industries, including telecommunications. Under the CPA and certain official standards issued thereunder, PROFECO ensures that telecommunications services providers comply with their obligations with respect to, among others, fair disclosure, fair dealing, marketing practices, clearance sales, remote sales, financing, product guaranties, claims, spare parts and repairs, warranty of services, standard form contracts (contracts of adhesion, which must be

registered with PROFECO) , consumer information and privacy (it should be noted that in Mexico there is a specific regulator for privacy matters, INAI, which also has jurisdiction over telecommunications services providers with respect to their collection and treatment of personal data of subscribers and the exercise of the latter of the ARCO rights, among others), collection efforts and liability

6. **What legal protections are offered in relation to the creators of computer software?**

Software programs are regulated under the Copyrights Act (Ley Federal del Derecho de Autor) and are protected as literary works. Creators of software programs hold moral and economic rights. Moral rights are inalienable, do not lapse and may be inherited. Economic rights vest upon the holder the exclusive right to reproduce, translate, adapt, distribute, and decompile the software. Economic rights may be transmitted and lapse after 100 years from the author's death.

Pursuant to the Industrial Property Act, software programs are not subject to patentability.

7. **Do you recognise specific intellectual property rights in respect of data/databases?**

Data, as such, is not subject to intellectual property protection.

Under the Copyrights Act, databases that as consequence of their selection and arrangement constitute intellectual creations, are protected as compilations, enjoying the same protections as literary works (100 years of exclusivity after the author's death).

Creators of unoriginal databases enjoy exclusivity rights for 5 years, only.

Holders of economic rights of both, compilations and unoriginal databases, have the exclusive right to reproduce, translate, adapt, distribute, and decompile the relevant compilation or database.

8. What key protections exist for personal data?

The processing of personal data is regulated under the Personal Data held by Private Parties Act (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*) and the Personal Data Held by Government Entities Act (*Ley General de Protección de Datos Personales en Posesión de los Sujeto Obligados*) (the "Data Protection Legal Framework").

The key protections for data subjects, under the Data Protection Legal Framework, are the following:

- Controllers must process personal data in accordance to the principles of legality, consent, information, data quality, proportionality and liability provided under the Data Protection Legal Framework;
- Prior to processing personal data, data controllers must provide data subjects a privacy notice containing, among others: (i) the personal data subject to processing; (ii) the purposes of processing; (iii) the mechanisms through which data subjects may access, rectify, cancel and limit the use of their personal data or oppose to the processing of such data, (iv) any potential transfers of data and the purpose of said transfers; (v) the use of cookies, when applicable; (vi) the means through which the controller will notify any amendments to the privacy notice;
- All processing of personal data is subject to the data subjects' consent, except in certain situations provided under the Data Protection Legal Framework (for instance, when data is publicly available, when the same is necessary for medical attention or when processing is permitted under applicable law). Consent may be tacit (opt out), when general personal data (i.e. name, email, telephone number, etc.) is processed, but must be explicit (opt in) when processing financial data (i.e. credit card number, bank account statements) and/or sensitive data (i.e. health condition, sexual preference and political affiliation), in which

cases the written consent must be obtained from data subjects; and

- Data controllers and processors must implement adequate physical, administrative and technological security measures to guarantee the integrity and confidentiality of the personal data.

9. **Are there restrictions on the transfer of personal data overseas?**

Overseas transfers are not per se prohibited under the Data Protection Legal Framework.

All transfers of personal data, however, are subject to the consent (in the forms described above) of the relevant data subjects, except for the limited cases set forth below. Controllers must inform data subjects about data transfers through the relevant privacy notice. Transfers must be limited to the purposes described in the privacy notice and the data controller must provide to the data recipient the privacy notice to which data subjects consented in connection with the processing of their personal data, for the purposes set forth therein.

All data transfers, domestic and international, must be documented. Data controllers and data recipients must enter into a data transfer agreement in which the recipient acquires the same data processing obligations as those imposed to the controller by the Data Protection Legal Framework. Additionally, the agreement must contain the terms under which data subjects consent to the processing of their personal data.

The data controller may transfer personal data without obtaining prior consent from the data subjects when the transfer is:

i. required or exempted from consent under Mexican law or an international treaty;

ii. necessary for medical purposes;

iii. made to data controller’s related entities;

iv. necessary as a consequence of an agreement executed or to be executed between the data controller and the relevant data subjects;

v. necessary or legally required to safeguard public interest or for law enforcement purposes;

vi. necessary for the recognition, exercise or defence of a right in a legal proceeding, or

vii. necessary to maintain or fulfil a legal obligation between the data controller and the data owner.

10. **What is the maximum fine that can be applied for breach of data protection laws?**

Breach of data protection laws can result in significant fines that range from approximately US$435 to US$1.39 million. In the case of systematic violations to privacy laws, an additional fine for up to the aforementioned cap can be imposed on the infringer. Also, if sensitive personal data is used in violation of the privacy laws, applicable fines can increase to up to twice the aforementioned amounts.

It is also worth noting that improper use of personal data or breaching personal data databases is considered a criminal offense that may result in imprisonment for up to 3 or 5 years, or twice as many if the offense involves unlawful treatment of sensitive personal data.

11. **Are there any restrictions applicable to cloud-based services?**

Pursuant to the Regulations to the Privacy Act, Data controllers may only hire cloud-based data processing services if the relevant vendor:

i. Operates under data protection policies in compliance with the principles provided under the Data Protection Legal Framework;

ii. Provides information about subcontracted processing services;

iii. Does not claim ownership of the personal data subject to processing;

iv. Guarantees the confidentiality of the personal data;

v. Has in place mechanisms to disclose any amendments to privacy policies;

vi. Allows data controller to limit the purposes of the processing of personal data;

vii. Keeps adequate security measures for the protection of the personal data;

viii. Guarantees to supress the personal data once the services has been provided;

ix. Prevents access to the personal data by unauthorised users.

12. **Are there specific requirements for the validity of an electronic signature?**

The Federal Commerce Code (Código de Comercio) was amended in August 29th, 2003, for the sole purpose of regulating the use of the electronic signature. In this regard, the Federal Commerce Code recognized the existence of two kinds of electronic signatures: (i) the regular electronic signature and (ii) the advanced electronic signature.

The regular electronic signature is referred to as “Data stored in electronic, usually included or attached to a data message or logically associated to it by any technology. It is used to match any given signer with a specific data message, indicating that the signer approves the information contained in the data message, and producing the same legal effects as autograph signatures, being admissible as evidence in legal proceedings”.

On the other hand, the Federal Commerce Code provides that the advanced electronic signature is a regular electronic signature which additionally complies with the following requirements:

i. The creation data of the relevant signature belongs exclusively to the signatory;

ii. At the moment of use, the creation data of the signature was under the signatory’s exclusive control;

iii. It’s possible to detect any modification made to the relevant electronic signature after it was used; and

iv. As regards to the integrity of the information contained in any given data message, it is possible to detect modifications made to such information after

the relevant signature.

Under applicable law, authorized Certification Services Providers (Proveedores de Servicios de Certificación), assess if at the moment of a data message signature, the electronic signature met the requirements needed to be deemed as advanced, and therefore, were valid for such purposes. Likewise, the Tax Administration Service (Servicio de Administración Tributaria) provides this certification free of charge.

In January 11th, 2012, the Advanced Electronic Signature Act (Ley de Firma Electrónica Avanzada), was enacted to regulate, from a technical perspective, the use of the advanced electronic signature, the digital certificate issuance and the services related to the use of the advanced electronic signature among others.

Said act provides that in order to use the advanced electronic signature, signatories must have a valid digital certificate issued by a Certification Services Provider (only valid for up to 4 years) and a private key generated under their exclusive control.

13. **In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?**

No, outsourcing does not result in an automatic transfer of employees, assets or contracts, although certain legal consequences may be triggered.

Generally speaking, the transfer of employees to another entity requires giving notice of the transfer to the employees, who may opt-out and be entitled to severance payment. The transfer of third party contracts requires, in general

terms, the consent of counterparty and the execution of an assignment, provided that the relevant agreement does not provide specific transfer mechanisms.

14. **If a software program which purports to be an early form of A.I. malfunctions, who is liable?**

The use of A.I. has not been specifically regulated by Mexican law and therefore general liability principles would apply. Thus, pursuant to the Consumers Protection Act, in general terms, the vendor would be liable before the final consumer for any malfunction of the relevant software program.

In case the supplier is not the manufacturer of the software program, the manufacturer would be liable before the supplier of any damage caused by the relevant malfunction.

15. **What key laws exist in terms of obligations as to the maintenance of cyber security?**

There are no specific laws on cybersecurity. However, the Personal Data Protection Legal Framework provides that data controllers and processors must put in place adequate technological security measures taking into consideration the nature of the personal data subject to processing, the vulnerability of the processing system and the technological developments in the market. Such security measures must be reviewed and updated regularly.

Additionally, banking and financial regulations require entities that use electronic means to perform financial services and operations to have cryptographic safeguards and develop policies to protect information stored,

processed or transferred through such means.

16. **What key laws exist in terms of the criminality of hacking/DDOS attacks?**

Cyber-attacks, hacking, virus infection and other cyber-crimes may constitute punishable criminal offenses pursuant to the Federal Criminal Code, which offences may be punished with imprisonment for up to twelve years.

17. **What technology development will create the most legal change in your jurisdiction?**

Blockchain, along with distributed ledger technology and self-executing codes (e.g. on-chain/ledger smart contracts) form part of a series of technologies which have the potential of bringing long-waited advancements to our jurisdiction and fundamentally cause a change in the legal framework applicable to all kinds of commercial, financial and governmental activities.

The self-enforceable, decentralized, counterparty-absent modus operandi of distributed protocols can help bring legal certainty, traceability and fraud-avoidance attributes to emerging economies that lack said characteristics, fostering both foreign and local investments into domestic markets.

Some of the business and/or governmental activities that could be fundamentally disrupted in our jurisdiction by such technologies are (including, without limitation) the following:

1. Payments and remittances;
2. Mortgage initiations;

3. Securitization;
4. Trade finance;
5. Crowdfunding;
6. Identity;
7. Supply chain;
8. Open banking;
9. Insurance;
10. Regtech;
11. Audit processes; and
12. Governmental registries.

With respect to other characteristics of distributed protocols, the immutable and real-time verification of the conducted transactions can lead to a perfectly traceable history of the assets placed/traded on-ledger, enabling first world compliance standards over local and international regulatory provisions, such as: (i) know your customer verification; (ii) anti-money laundering; (iii) terrorism financing; (iv) data and privacy protection; (v) anti-bribery & corruption, and (vi) government budget execution, among others.

18. Which current legal provision/regime creates the greatest impediment to economic development/commerce?

Our current General Law of Mercantile Corporations (Ley General de Sociedades Mercantiles) dates from 1934 and has been scarcely amended as to corporate government and other relevant corporate mechanisms. This has led to significant regulatory slippage regarding voting and decision-making processes to say the least, driving legal uncertainty and cumbersome corporate practices into corporations, causing investors and/or potential shareholders to seek for exit strategies and/or re-think their investments.

As to other legal issues that translate into economic development disincentives, our jurisdiction often shows a serious lack of coordination between Federal, State and Municipal levels, as well as between the legal competences of different regulatory authorities, which under certain scenarios could lead to redundant, unproductive and expensive compliance situations, including without limitation (i) excessive (sometimes duplicative) paperwork; (ii) long waiting response times from the authorities; (iii) uncertainty upon authorizations and/or licenses requests; (iv) contradictory criteria; and (v) legal uncertainty in general, among others.

19. **Do you believe your legal system specifically encourages or hinders digital services?**

Our regime has gradually become more technology friendly as several technologically oriented bill proposals and initiatives have become a reality in the last years, allowing a fundamental change in certain processes and the implementation of digital alternatives on commercial transactions.

For instance, our Federal Commerce Code (Código de Comercio) has been amended, so merchants are entitled to conclude agreements through electronic means, this is, through the exchange of data messages and both, electronic signatures and advanced electronic signatures, granting such mechanisms with the same probative value than autograph signatures provided they fulfill certain requirements. In this regard, we also have an Advanced Electronic Signature Act in force (see question 11 above) that provides legal certainty accordingly.

As to other matters, we have an extremely efficient real-time settlement mechanism created by the Central Bank (“SPEI” for its acronym in Spanish), which enables near real-time interbank money transfers and payments, and has been the driver for innovation, development and adoption of fast, efficient and secure digital payments alternatives, drawing the attention of numerous

Fintech players.

This, along with the surge of several new companies that offered funding alternatives through digital means, resulted in the enactment of the Mexican Fintech Act (Ley para Regular las Instituciones de Tecnología Financiera) in effect as of March 2018, which introduced specific regulations for e-money and crowdfunding institutions, as well as cryptocurrencies' utilization. Such law also introduced novel regulations as regards to financial regulatory sand box, open banking, digital authentication mechanisms, and regtech, among others.

From a tax perspective, it is important to note that the Mexican Tax Administration Service (Servicio de Administración Tributaria), has undertaken a significant digital transformation initiative and has positioned itself as one of the world's leading tax authorities regarding technology adoption. Their efforts have resulted in the creation and adoption of: (i) digital authentication tools (e.g. tax electronic signature and digital certificates issuance); (ii) electronic invoicing systems; (iii) cloud storage services for taxpayers' information; (iv) electronic filing of accounting records, returns and other relevant notices; and (v) electronic filing of administrative appeals, among others.

In sum, we believe that the introduction of recent amendments to the regulatory framework, such as the ones described above, among others, along with certain efforts by the authorities to introduce new digital alternatives, will encourage and foster the development and adoption of several digital services.

20. **To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?**

The regulatory framework in Mexico might face challenges in dealing with A.I., as certain provisions thereof, especially those relating to liability and criminal behaviour often consider the "intent" of an individual for the imposition of legal

sanctions. To the extent these new technologies become more common in everyday activities, Mexican legislators will be forced to amend the relevant legal framework in order to make it compatible with such reality.

Another aspect to consider is the judiciary system. There are few (if any) precedents in the utilization of digital tools and/or evidence (e.g. electronic signature and digital authentication). Alternative dispute resolution methods, such as arbitration, may thus become more appealing, although their use is currently not the general rule.