Article **Journal-International Economy**
June 2022 Vol.6 No.10 12-21

Data Privacy

Privacidad de datos

VAZQUEZ, Adrian†

Universidad Iberoamericana

ID 1st Author: *Adrian, Vazquez*

DOI: 10.35429/JIEC.2022.10.6.12.21 Received March 07, 2022; Accepted June 15, 2022

Abstract

We define personal data as name, telephone number, address, photograph, or fingerprints, as well as any other data that can identify you, it is critical that we take care of this data for security reasons and because it is our right. Data must be protected against misuse such as identity theft, improper or unlawful transmissions or unauthorised access. The new legislation places individuals at the centre of the State's protection Mexicans now have legislation that protects personal information that can be found in the databases of any natural person or company, such as insurance companies, banks, department stores, telephone companies, hospitals, laboratories, universities, etc. This legislation contains a series of clear rules for the protection of personal information. This legislation contains a series of clear rules respectful of the privacy, dignity and information of individuals, derived from principles internationally observed by other countries around the world. The law regulates how and under what conditions companies should use your personal data.

Resumen

Definimos datos personales como nombre, número de teléfono, dirección, fotografía o huellas dactilares, así como cualquier otro dato que pueda identificarle; es fundamental que cuidemos estos datos por razones de seguridad y porque es nuestro derecho. Los datos deben protegerse contra usos indebidos como la usurpación de identidad, transmisiones indebidas o ilegales o accesos no autorizados. La nueva legislación coloca a las personas en el centro de la protección del Estado Los mexicanos contamos ahora con una legislación que protege la información personal que se encuentra en las bases de datos de cualquier persona física o moral, como aseguradoras, bancos, tiendas departamentales, compañías telefónicas, hospitales, laboratorios, universidades, etc. Esta legislación contiene una serie de normas claras para la protección de la información personal. Esta legislación contiene una serie de normas claras y respetuosas con la intimidad, la dignidad y la información de las personas, derivadas de principios internacionalmente observados por otros países del mundo. La ley regula cómo y en qué condiciones las empresas deben utilizar sus datos personales.

Citation: VAZQUEZ, Adrian. Data Privacy. Journal- International Economy. 2022. 6-10: 12-21

† Researcher contributing first Author.

Theoretical framework

The Federal Law on the Protection of Personal Data in Possession of Private Parties, also referred to as LFPDPPP, was published in the Official Journal of the Federation on 5 July 2010 and came into force one year later. It is the first law of its kind to be passed in Mexico, although there are precedents on data protection laws, it is the first law that covers data protection in a broad sense with standard rules. It has certain similarities with existing data protection laws in the European Union, mainly Spain, and also with existing laws in Argentina, which is leading the change in Latin America.[1] This law applies only to the processing of personal data, but also to the processing of personal data.

This law applies only to the processing of information carried out by private individuals, so that government credit reporting institutions and companies that collect information for non-profit purposes are exempt from compliance. On the other hand, compliance is mandatory for individuals and companies residing in Mexican territory regardless of where the data subject resides, which implies that internet companies residing in Mexico must comply with the regulation even if their customers are not Mexican; however, foreign internet companies are not obliged to comply with the law's status for their Mexican customers.

The model law includes the use of general definitions, allowing control over the collection, use, including access, management, transfer or disposal, publication or storage of personal information through any medium belonging to an identifiable individual, prohibiting by default all processing without the individual's consent. With respect to information held in public sources, the law is much more permissive than in the European Union, allowing the use of such information without any notice or express justification.

The general principles of this law follow the inspiration of the OECD by delimiting the following:

- Notification: Every individual must be notified when his or her personal data are being collected.
- Purpose: The notification should outline the purpose for which the data will be collected and the data should only be used for that purpose.
- Consent: Personal data may not be published without the explicit consent of the data subject.
- Security: The information collected must be protected from potential abuse.
- Transparency: Data subjects must be informed about the identity of the person collecting the data.
- Accountability: Data subjects should have a method to hold the data collector accountable for any breach of the above principles.

Notifications made by entities collecting personal data should contain the following points [2]:

- Identity and address of the entity collecting the data
- The purpose for which the personal data will be collected
- The options and methods available to the collecting entity for limiting the disclosure and use of the information collected
- The mechanisms that data subjects may use to request access, correction, cancellation and opposition to the procedure in accordance with the provisions of the law
- The procedure by which the collecting agency will communicate to data subjects about any changes in the provisions.

Law on the protection of personal data

Personal Data Protection Principles, ARCO Rights and their exercise [3].

On the Personal Data Protection Principles

The law is based on principles that have been internationally recognised for many years in the field of privacy and personal data protection. Those responsible for the processing of personal data must observe the principles of lawfulness, consent, information, quality, purpose, fairness, proportionality and accountability provided for in the Law. Some important points in relation to the mandatory adoption of these principles are the following [4]:

Personal data must be collected and processed in a lawful manner. Personal data must not be obtained by misleading or fraudulent means.

In all processing of personal data, there is a presumption of a reasonable expectation of privacy.

All processing of personal data shall be subject to the consent of the data subject, subject to the exceptions provided for by law.

Consent shall be express when the will is expressed verbally, in writing, by electronic, optical or any other technology, or by unequivocal signs.

It shall be understood that the owner tacitly consents to the processing of his data when, having been provided with the privacy notice, he does not express his opposition.

Consent may be revoked at any time without retroactive effect. In order to revoke consent, the data controller shall, in the privacy notice, establish the mechanisms and procedures for doing so.

Financial or patrimonial data shall require the express consent of the data subject, except for the exceptions provided for in the law.

In the case of sensitive personal data, the data controller must obtain the express written consent of the data subject for its processing, by means of his or her autograph signature, electronic signature, or any authentication mechanism established for this purpose.

The Data Controller shall ensure that the personal data contained in the databases are relevant, correct and updated for the purposes for which they were collected.

The processing of personal data shall be limited to compliance with the purposes set forth in the privacy notice.

The processing of personal data shall be that which is necessary, appropriate and relevant in relation to the purposes set out in the privacy notice.

The data controller shall ensure compliance with the principles of personal data protection established by the Law, and shall adopt the necessary measures for their application. The foregoing shall apply even if such data are processed by a third party at the request of the data controller.

The data controller shall be under the obligation to inform the data subjects of the information that is collected from them and with is collected from them and for what purposes, through the privacy notice.

The aforementioned -privacy notice‖, which is a key document on which a large part of the -responsibilities‖ of this law revolves, must be made available to data subjects through printed, digital, visual, audio or any other technology. Such notice should contain at least the following information:

The identity and address of the data controller that collects the data; The purposes of the data processing;

The options and means offered by the data controller to the data subjects to limit the use or disclosure of the data;

The means to exercise the rights of access, rectification, cancellation or opposition, in accordance with the provisions of the Law;

The procedure and means by which the data controller shall inform the data subjects of changes to the privacy notice, in accordance with the provisions of the Law; and In the case of sensitive personal data, the privacy notice shall expressly state that it concerns this type of data.

Within the -catalogue‖ of obligations set out in this law, one of the most important is undoubtedly that established in Article 19: -Any data controller who processes personal data must establish and maintain administrative, technical and physical security measures to protect personal data against damage, loss, alteration, destruction or unauthorised use, access or processing.‖ The most important part of this obligation is that established in Article 19: -Any data controller who processes personal data must establish and maintain administrative, technical and physical security measures to protect personal data against damage, loss, alteration, destruction or unauthorised use, access or processing.

The most important part of this security obligation does not end there, as Article 20[4] states that: -Security breaches occurring at any stage of the processing that significantly affect the economic or moral rights of the data subjects shall be immediately reported by the data controller to the data subject, so that the latter may take the measures corresponding to the defence of his or her rights.

At the end of this chapter, a generic obligation of confidentiality of the information is determined, specifically in Article 21: The data controller or third parties intervening in any phase of the processing of personal data must keep such data confidential, an obligation that will subsist even after the end of their relations with the data subject or, as the case may be, with the data controller.

Law and data privacy

The presence of the IFAI in all these cities aims to disseminate the exercise of the right to the protection of personal data in its two aspects: the first, from the perspective of data subjects, as a fundamental guarantee, and the second, from the point of view of data controllers, in terms of compliance with the Federal Law on the Protection of Personal Data in the Possession of Private Parties.

According to the Institute, the intention is to raise awareness among data subjects and controllers of the importance and impact of the quantitative and qualitative value of personal data within a global and digital context, and to raise public awareness of the responsibility involved in sharing personal data with third parties, among other objectives.

It is also intended to disseminate the tools that the Institute has developed to facilitate the compliance of data controllers with their obligations and the promotion of procedures for data subjects, and to publicise the sanctions imposed in strategic sectors.

With regard to these tools, IFAI makes available to all data controllers the Privacy Notice Generator (GAP), so that they can create their privacy notice free of charge.

According to the study Termómetro: De la Privacidad de datos, carried out by the company Deloitte Mexico, despite the entry into force of the Ley de Protección de Datos Personales en Protección de los Particulares, the regulatory and data protection guidelines in Mexico, as well as the culture of privacy, are rudimentary.[5] The analysis gathers the opinion of executives from the private sector.

The analysis gathers the opinion of Mexican industry executives, showing that 74% of respondents are even partially aware of the law. However, 54% of employees are not aware of the responsibility they must fulfil in the process.

Similarly, the report found that 77% of respondents' main objective is to increase or gain the trust of customers, followed by ensuring regulatory compliance with 74%76

This makes it clear that beyond compliance, companies are looking to maintain or increase customer trust and loyalty, which will become more important as the country's data protection culture strengthens,‖ said Eduardo Cocina, IT risk partner at Deloitte Mexico.

On the other hand, the study revealed that the main risk that organisations face in the misuse of personal information is the loss that occurs via mobile or memory devices.

In order for companies to adopt the law correctly, it is a priority to implement a series of actions that include the development of a privacy model applied to the reality of the organisation; assign roles and responsibilities for the management of information; establish measurement and assurance mechanisms and, finally, exhibit the results obtained to the audiences involved.

Mexican companies have identified that they are vulnerable and need to make certain changes in the way they protect and treat information,‖ said the specialist.

According to the Deloitte study, more than half of those interviewed said that their organisation does have the necessary internal resources to comply with the law. They consider internal processes and practices, policies and standards, as well as knowledge and the number of people, to be key factors in achieving compliance with the law.

As companies become more sensitive to the relevance of processes and advance in their self-analysis, they can determine the level of effort required and begin to act to realise various benefits.

The protection of personal data dates back to 1948, when the General Assembly of the United Nations adopted the document known as the Universal Declaration of Human Rights, in this document the human rights known as basic human rights are expressed. Article 12 states the following:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Currently, a large amount of personal data, including what is known as biometric data, is stored in computer systems, making it susceptible to cyber attacks.

In several countries around the world there are efforts to create legislation that establishes limits, permissions and penalties for the proper handling of data contained in information systems, especially those defined as personal data. This research seeks a legal precedent of how biometric data are considered by the personal data protection laws of different countries around the world.

Some concepts relevant to this issue are described below:

Personal data. This refers to all information associated with a person or individual that makes him or her identifiable from other persons and/or as part of a particular group of individuals, for example: name, address, telephone number, photograph, fingerprints, gender, nationality, age, place of birth, race, affiliation, political preferences, date of birth, iris image, voice pattern, etc. The thrust of this concept is common to the data protection legislation that different countries have drafted.

Sensitive personal data. Commonly refers to all those data that relate to the most intimate level of its owner and whose disclosure may cause discrimination or generate a severe risk for its owner. In general, sensitive data are considered to be those that reveal characteristics such as ethnic or racial origin, health status, religious beliefs, political opinions, sexual preference, trade union membership, philosophical and moral beliefs, among others. This kind of information must be treated with greater responsibility and stricter protection measures must be established.

Biometric data. By common definition, biometric data are those physical, biological or behavioural traits of an individual that identify him or her as unique from the rest of the population. Computer systems in which biometric data are measured, as part of the identification and/or authentication process of a subject, are known as biometric security systems or simply biometric systems.[6] The following are some examples of biometric data.

The following list are some examples of biometric data:

- Fingerprints
- Hand geometry
- Iris analysis
- Retinal analysis
- Veins on the back of the hand
- Facial features
- Voice pattern
- Handwritten signature
- Typing dynamics
- Walking gait cadence
- Gesture analysis
- DNA analysis

Data protection laws around the world

The European model seeks to protect the information and its ownership, in order to preserve the honour of the individual even if he or she is deceased, the motivation of this model is based on the human rights of the individual. The US model aims to protect the information of individuals with the concept of the right to privacy, which can be extinguished with the death of the subject, the model arises from commercial reasons as companies used this information indiscriminately.

Various countries have enacted personal data protection laws and each country has sought to adapt the bases of one of the two existing personal data protection models to its own cultural, economic and political conditions.
78

The following are some relevant cases of personal data protection laws in different countries, organisations and regions of the world:

1. United Nations (UN). In 1948, it adopted the document known as the Universal Declaration of Human Rights, in which Article 12 states that individuals have the right to the protection of their personal data under the law.

2. Germany. In 1970, the first data protection law (Datenschutz) was passed. In 1977, the German Federal Parliament passed the Federal Bundesdatenschutzgesetz. These laws prevent the transmission of any personal data without the consent of the data subject.

3. Sweden. In 1973, one of the first data protection laws in the world was published.

4. United States of America. Data protection is based on the Privacy Act of 1974.

5. European Union. The first international data protection convention was signed in 1981 by Germany, France, Denmark, Austria and Luxembourg.

Germany, France, Denmark, Austria and Luxembourg. It is known as -Convention 108‖ or the -Strasbourg Convention‖. In the 1990's, a common standard is established which was called Directive

95/46/EC. The directive concerns the protection of individuals with regard to the processing of personal data and the free movement of such data.

6. Spain. The Organic Law 15 of 1999, establishes the Protection of Personal Data. This law has been important for Latin America because it has been used as a firm reference for the European model.

7. Latin America. In Latin America, personal data protection laws arise as a necessity derived from the increase in the use of information technologies and the increase in associated vulnerabilities. Most of these laws are similar to the European model: in Argentina, Law 25.326 (2000), Chile (1999), Panama (2002), Brazil (1997), Paraguay (2000), Uruguay (2008).

8. Russia. A comprehensive personal data protection law was passed in 2006.

9. Peru. Law 29.733 of 2 July 2011 is the most recent personal data protection law in the world.

10. Mexico. The Ley Federal de Protección de Datos Personales en Posesión de Particulares was published in the Diario Oficial de la Federación on 5 July 2010, entered into force one day later and is effective as of January 2012.

This law aims to safeguard respect for the privacy, dignity and information of individuals. It establishes four fundamental rights that individuals have over their information held by any individual or private company (insurance companies, banks, department stores, telephone companies, hospitals, laboratories, universities, etc.), known as ARCO rights: Access, Rectification, Correction and Opposition.

ISSN-On line: 2524-2032

The law also indicates that private parties must notify each person from whom they obtain personal information about the processing they plan to give to their data. This must be done by means of a privacy notice, which must be respected by the individual, and each person notified will be free to give or withhold consent to the processing of his or her information.

Personal data protection map

A map of the personal data protection laws applied in the world has been published The classification seems to assess only the European model of personal data protection, as it does not include the United States as part of the countries with personal data protection legislation [5].

Figure 1

Finally, after two months of waiting, the Federal Law on the protection of data held by private individuals has been published in the Official Journal of the Federation. In Mexico, data protection only existed for personal information that appeared in state or government archives, through the Federal Law on Transparency and Access to Information (Ley Federal de Transparencia y Acceso a la Información).

With the new law, private companies will have a period of one year to appoint a data processor.

A period of one year was also stipulated for the issuance of the regulation of the law, which will contain the specific provisions. We hope that this will have the characteristics of the Spanish RD 1720/2007, with the security measures for files containing personal data.

The law, of course, contemplates the figures of data processor, data controller and third party, as well as the concept of sensitive data, which will have to be given special treatment.

In subsequent issues, we will discuss this law in greater detail, its positive aspects and those that could be improved.

It is difficult to give a definition of "privacy" as it is a subjective matter. For personal reasons, some people prefer to live anonymously in society without anything interfering in their affairs. Others are not reluctant to give away their personal details in exchange for access to information, goods or services. For most, privacy is simply a security issue.

People have a preference for accessing services without having to fill in complicated forms or undergo reference checks. To this end, they may agree to allow information systems to track their movements and purchases.

Security is intimately linked to privacy. Secure information systems should never disclose data inappropriately. We cannot claim that the disclosure of any information is an act without ulterior motives. Information is always collected and processed for a specific purpose.

The intention of those who collect personal information or do business with it and store it in a database is to create individual profiles for a specific purpose. The ways in which personal data are disclosed, used and stored will help us determine whether information technologies are being used for empowerment or repression.

In considering ways of measuring privacy and security, we must distinguish between different kinds of privacy:

Privacy means to most people "intimacy" or the right of the individual to have nothing and no one interfere with their home, property or private life. This can be thought of as "real world" privacy.

The right of individuals to be protected from medical or genetic testing is the basis of their bodily privacy; it also includes the right to have information about their personal health and well-being protected by those who have access to it (doctors, employers, insurers, etc.).

ISSN-On line: 2524-2032

Privacy in communications" refers to protection against interference with telephone or Internet communications. Respect for privacy in communications is a prerequisite for the maintenance of human relations through technological means of communication.

Confidentiality of information" is probably the most debated aspect of the use of computers and information systems. Information systems have the capacity to rapidly store and process data from a large number of people. It is important to ensure that such information is used only for the purposes for which it was collected and that it is not disclosed to third parties without the consent of those concerned.

Threats to privacy on the Web

When surfing the Web, we are not completely anonymous; there are several ways in which information about users or their activities can be collected without their consent [7]:

Cookies (mini web page user ID file) HTTP BrowsersThere may already be information about you posted on the web. Downloading free and shared software Search engines E-commerce E-mail E-mail and cryptography Spam Dangers in IRC Chat.

In Mexico, the fundamental right to the protection of personal data is guaranteed by the Constitution (Article 16) and the corresponding implementing Law on the Protection of Personal Data in Possession of Private Parties (LFPDPPP) and its regulation.

The former appeared in 2010 and the latter at the end of last year. Thus, this human right has become fundamental since its inclusion in the Magna Carta and, among other aspects, implies guarantees derived from it, such as the precepts regarding the rights of access, rectification, cancellation or opposition (Arco rights) to the processing of personal data.

As private individuals, as individuals, as holders of these personal data, but above all as subjects of fundamental rights, it is necessary and quasi-obligatory to be informed about the way in which the right we are analysing is protected, but also the way in which we can carry out its authentic exercise.

The Federal Institute for Access to Information and Data Protection is the guarantor body. That is, the institution to which we can turn to learn about the two aspects mentioned above and also the one that will support us in the event that our rights are violated.

On the other hand, and as a counterpart, the regulatory body for the business sector is the Ministry of Economy, which has powers in this area to raise awareness among organisations about their obligations regarding the protection of personal data (including making available to their users or clients the privacy notice, which must indicate the categories of personal data that will be collected, as well as the purpose for which they will be used), and the purpose for which they will be processed and the duration of such processing - and the appointment of a person in charge of the personal databases - which, depending on the size of the companies, may be an individual or a department -) and fostering the culture of adopting binding self-regulatory schemes, as provided for in the aforementioned regulation.

The adoption of self-regulatory measures, which consists of the inclusion of ethical codes that, on the part of companies, complement the measures to comply with the legislation, reduce security breaches or holes and, likewise, reduce the amounts of sanctions to which a natural or legal person may be liable for non-compliance with the provisions of the LFPDPPP and its regulations, as well as for any attack on their personal databases, which, in addition to incurring such a penalty, may entail an enormous risk in the loss of valuable information (bearing in mind that personal data are one of the main assets of companies), as well as an enormous loss of prestige, lack of customer loyalty, or even the termination of contracts with them. Now, one of the aspects that must be taken into consideration in relation to the processing of personal databases by practically all companies (the Law obliges all of them whenever they hold such data and use them for dissemination and/or marketing purposes), is the use of Information and Communication Technologies (ICT) in such processing. There are many challenges that both companies and individuals face in the use of technology, and even ICTs themselves are the reason why in several countries the concern to regulate these aspects began.

That is, the technology that increasingly proliferated in the 1980s and which even led to the development of many theoretical analyses to analyse the phenomena it raised, from a sociological or communicational point of view, also led to studies and amendments at the legal level, since it was considered to have the potential to violate the spheres of already protected human rights, such as privacy and honour and self-image.

The international instruments that stand out in this regard, even when the ICT boom had barely or not yet begun, are the 1948 Universal Declaration of Human Rights and the 1966 International Covenant on Civil and Political Rights. In several European countries, the debate on the rights set out therein began, but with the consequent aggravation that technology could bring. Germany, for example, was one of the first countries to provide protection for privacy-related rights. In Spain, these legal developments also began early on, in such a way that the 1978 Constitution established a right to personal and family privacy and stipulated that the law would limit the use of information technology in order to protect it.

This is a clear allusion to the beginnings of the development of ICTs, which started with the aforementioned computer science, but later converged with the telecommunications and audiovisual sectors.

It is for all these reasons that privacy and personal data protection legislations have considered the implications of technology on the privacy of individuals since their beginnings, but do so with much more emphasis and frequency nowadays. For example, Mexico's LFPDPPP Regulation already considers the issue of cloud computing as one of the possible threats to the handling of data of persons with fundamental rights.

As mentioned above, in addition to the measures promoted by legislation, there is the possibility of adopting additional security measures and codes of conduct and ethics, which combine best practices, in order to protect personal databases for several reasons. One of them is the integrity of such databases, finally, because of the importance they have for the organisation, one of the most important of which is that penalties derived from legal non-compliance are avoided, since the sanctions regime of the LFPDPPP is extremely strong.

Additional security measures and binding self-regulatory schemes include those related to the use of technology to combat technology. That is, if ICTs can be potentially privacy and personal data infringing, with other ICTs this process can be combated, reversed or minimised. -This is the case of PETs (Privacy Enhancing Technologies), which are already being worked on in different countries and which, for our part, we are already designing, with a theoretical and doctrinal basis, at Infotec. [8].

C**onclusions**

The protection of personal data is an important step forward for the exercise of our rights regarding the use of such data, in my personal opinion and from my own experience, many times people spoke to me and I did not know how these data reached them, I think it is very important because it is a very delicate issue, since not having control over our data, any company or person could use them.

I think that Mexico has taken a big step forward in terms of the right that we citizens have to take care of our data. I think that the only thing that is missing is the strengthening of the institutions to impose stronger fines on organisations or companies that misuse our data, for example, the fine for BANAMEX is not enough compared to the size of the company.

References

[1] J. T. Eustice y M. A. Bohri, «NAVIGATING THE GAUNTLET: A SURVEY OF DATA PRIVACY LAWS IN THREE KEY LATIN AMERICAN COUNTRIES,» Sedona Conference Journal, pp. 137-153, 2013.

[2] L. Determann y S. Legorreta, «New Data Privacy Law in Mexico.,» Computer & Internet Lawyer. , pp. 8-11, 2010.

[3] F. Solares Valdes, «Ley Federal de Protección de Datos Personales,» de Ley Federal de Protección de Datos Personales, Distrito Federal.

[4] Cámara de Diputados, «Ley Federal de Protección de Datos Personales en Posesión de los Particulares,» Diario Oficial de la Federación, Distrito Federal, 2010.

[5] b: Secure, «México aún no está preparado para la ley de protección de datos: Deloitte,» 15 Febrero 2012. [En línea]. Available: http://www.bsecure.com.mx/featured/mexico-aun-no-esta-preparado-para-la-proteccion-de-datos/.

[6] UNAM, «Leyes de protección de datos personales en el mundo y la protección de datos biométricos,» [En línea]. Available: http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93.

[7] Asociación para el progreso de las comunicaciones, «Aspectos específicos relativos a las políticas sobre internet y su regulación,» [En línea]. Available: http://derechos.apc.org/handbook/ICT_21.shtml.