Article **Journal-Law and Economy**
December, 2020 Vol.4 No.7 14-19

Personal data protection

Protección de datos personales

LÓPEZ-JARQUÍN, Sergio Benigno†*

Universidad Iberoamericana

ID 1st Author: *Sergio Benigno, López-Jarquín*

DOI: 10.35429/JLE.2020.7.4.14.19 Received July 31, 2020; Accepted December 19, 2020

Abstract

Historically, information has played a very significant role in human life, but nowadays with the adoption of Information Technology as an essential part of our daily life, the properties of reliability, integrity and availability become indispensable in our daily activities, can be said to be obligatory for its proper use, and making the best decisions. Being an important asset, the information becomes a very desired object for other individuals or organizations, either for their use that allows them to have legal gains, to have illegal profits or even for non-profit organizations. Therefore, the importance of protecting our personal data takes on a transcendental relevance in this digital age, and Mexico has already taken a very important step by having a law already established in 2010 in this area. There is still much to be done, since policies and laws by themselves do not serve much, as individuals, we must have a culture of protecting our data and helping to spread and raise awareness among the population in general.

Resumen

Históricamente, la información ha jugado un papel muy importante en la vida humana, pero hoy en día con la adopción de las Tecnologías de la Información como parte esencial de nuestra vida diaria, las propiedades de confiabilidad, integridad y disponibilidad se vuelven indispensables en nuestras actividades diarias, se puede decir que son obligatorio para su correcto uso, y para la toma de las mejores decisiones. Al ser un activo importante, la información se convierte en un objeto muy deseado por otras personas u organizaciones, ya sea por su uso que les permita tener ganancias legales, tener ganancias ilegales o incluso para organizaciones sin fines de lucro. Por tanto, la importancia de proteger nuestros datos personales adquiere una relevancia trascendental en esta era digital, y México ya ha dado un paso muy importante al contar con una ley ya establecida en 2010 en esta materia. Aún queda mucho por hacer, ya que las políticas y leyes por sí solas no sirven de mucho, como individuos, debemos tener una cultura de protección de nuestros datos y ayudar a difundir y concienciar a la población en general.

Citation: LÓPEZ-JARQUÍN, Sergio Benigno. Personal data protection. Journal-Law and Economy. 2020. 4-7: 14-19

* Correspondence to Author (e-mail: A2023490@correo.uia.mx)
† Researcher contributing as first author.

General Concepts

The emergence of the right led to constitutional reforms in 3 articles:

Article 6, article 16 and article 73.

On July 20, 2007, article 6 of our Mexican constitution was amended, citing: "... The right to information will be guaranteed by the State. To exercise the right of access to information, [...] within the scope of their respective competences, they will be governed by the following principles and bases ... II. The information that refers to private life and personal data will be protected in terms and with the exceptions established by law ...

The reforms carried out were:

a. General principle of information publicity.
b. The right of access to public information.
c. The protection of personal data held by the authorities.

The constitutional article 16 modified on July 1, 2009 and which appointment: "Everyone has the right to the protection of their personal data, access, rectification and cancellation of them, as well as to express their opposition, in terms of the set of laws, which will establish the exceptions to the principles governing the processing of data, for reasons of national security, provisions of public order or to protect the rights of third.

The amendment was that the right to the protection of personal data was raised to "constitutional guarantee", as well as the ARCO (Access, Rectification, Cancellation and Opposition) rights.

Article 73, section XXIX, Section "O" was amended on April 30, 2009 and reads: The congress has the power: [...] XXIX to legislate on the protection of personal data held by private individuals.

The paragraph does not exist and is included: “It granted the faculty of the Union to legislate in the matter of protection of personal data in the possession of individuals”.

The regulation applicable to the Private Sector is:

– Federal Law for the Protection of Personal Data in Possession of Individuals: LFPDPPP (DOF 5/07/2010)
– Regulation: LFPDPPP (DOF 21/12/2011)
– General Criteria for the Instrumentation of Compensatory Measures: (DOF 17/01/2013)
– Guidelines for the Privacy Notice (DOF 17/01/2013)
– Parameters for the development of schemes self- regulation binding. (DOF 16/07/2013)
– Recommendations on Personal Data Security (DOF 10/09/2013)
– Obligatory Subjects (newly published in 2017)
– Authorities and control bodies:

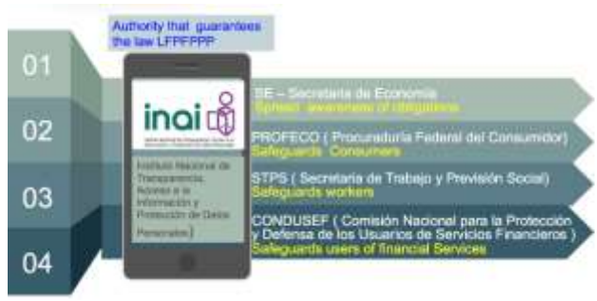

Figure 1 Authority & control bodies
Source: INAI. (2018). Marco Normativo. Mexico. Available in: http://inicio.inai.org.mx/SitePages/marcoNormativo.aspx?a=proteccion

The obliged subjects are private individuals or corporations that carry out the processing of personal data.

The law provides exceptions for:

1. Credit information societies.
2. Persons who carry out the collection and storage of personal data, which is exclusively for personal use, and for purposes of disclosure or commercial use.
3. Relating to moral persons.
4. The one that refers to physical persons in their capacity as merchants and professionals.
5. Individuals who provide their services for any legal entity or individual with business activities, provided that the information is processed for the purposes of representing the employer or contractor.

Personal Data: It is the information belonging to an identified or identifiable natural person. The data alone have no value, only when they relate to someone is when they acquire value. The sensitivity of the data depends on the impact it might have on the most intimate sphere of its owner or failing that the misuse of it may have a risk for it or lead to discrimination.

For example:

- **Standard Data (Normal):** Name, age, address, sex, RFC, CURP
- **Sensitive Data (Special):** Patrimonial, legal, academic, physical location, authentication, financial (bank accounts, balances), physical and mental health status, racial or ethnic origin, genetic information, religious or political beliefs, union affiliation, sexual preference etc.
- **Special Data (Critical):** Bank card keys, fingerprints, iris, voice, handwritten signature, high risk holders etc. ...

Rights:

It is the power of disposition and control that empowers its owner to decide on which of its data it provides to a third party, as well as who owns that data and for what, being able to oppose that possession or use (Informative self-determination). It is the legality that everyone has to know and decide, who, how and in what way they collect and use their personal data.

Figures involved:

- **Owner:** The individual to whom the personal data belongs.
- **Responsible:** Private or moral, national or foreign person who decides on the processing of personal data. Decide the purpose, content and use of the treatment.
- **Person in charge:** Individual or legal entity that alone or jointly with others treats personal data on behalf of the person in charge, this one does not have the capacity of decision on the treatment, only treats the data following the mandate of the person in charge. For a healthy relationship between the responsible and the person in charge, contractual clauses or a legal instrument decided by the responsible must be established.
- **Third:** Anyone to whom data is communicated, either responsible (transfer) or charged (referral).

Information processing:

The treatment of the information whatever the means of its obtaining, storage, use, disclosure must be legitimate, controlled and informed, manually or automatically and must have a temporary or permanent accommodation.

Obtaining: It is the moment in which the data of the owner is obtained, either directly or indirectly.

Treatment: refers to the Obtaining, use, disclosure, access, storage, exploitation, transfer and disposal of information.

Third parties: Transfer and Remission.

Transfer: it is the communication of data between two responsible, which will decide the treatment of the data and requires the consent of the owner. When a data transfer is made, third parties must be notified of the privacy notice and the purposes to which the owner gave consent to the processing of their data, the owner must give their consent to the transfer of their data in a clause within the privacy notice so that the recipient acquires the quality of responsible, assuming the same obligations.

In some cases, the law considers that the holder's consent in a transfer is not needed, such as:

- Law or treaty in which Mexico is part
- Necessary for medical benefit
- Society of the same responsible group
- Under a contract in the interest of the owner
- Legally required to safeguard a public interest
- Necessary for a judicial process
- Legal relationship between the owner and the responsible

Remission: It is the communication of data between the responsible and the manager, where the receiver is limited to the provision of services and the consent of the owner is not required.

ARCO Rights

Figure 2 ARCO Rights
Fuente: INAI. (2018). Derechos ARCO. Mexico. Available in: http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

It refers to the right of a holder of personal data, to request access, rectification, cancellation or opposition on the processing of their data, before the Obligatory Subject who is in possession of them, are exercised by the owner or representative, prior accreditation of own identity and / or representation.

Access: Refers to the personal data being in place or through the issuance of simple copies or any means and that is provided in the privacy notice, and access to them must be in readable and / or understandable formats for the owner.

Rectification: Right to be able to modify data that may be inaccurate or incomplete.

Cancellation: It implies to finish the treatment on the part of the responsible and the suppression of the data. (When it is no longer necessary for the purpose for which the information was granted), being exceptions when:

- Contractual obligations
- Legal Provisions
- Judicial actions
- Legal interest of the owner
- Public interest
- Health issues

Opposition: It is the prerogative that consists in opposing the use of personal data for a certain purpose, this will not proceed when the treatment is necessary for the fulfillment of a legal obligation imposed on the person responsible.

In the case of individuals who are minors or in a state of disability, the policies considered in the Federal Civil Code must be reviewed.

To make a request for ARCO right, the owner or the representative must make the request through the means indicated in the privacy notice and with the following elements:

- Name, mail or address of the owner, where you want to be notified or contacted.
- Documents proving your identity or representation
- Description of personal data regarding which seeks to exercise any of the rights, written clearly and accurately.
- Any other element that facilitates the location of personal data

The responsible part is obliged to respond, regardless of the meaning of their response or if the personal data are in their databases and must refer only to the personal data specified in the application, they must be submitted in a common, understandable language and in an easy to access and readable format.

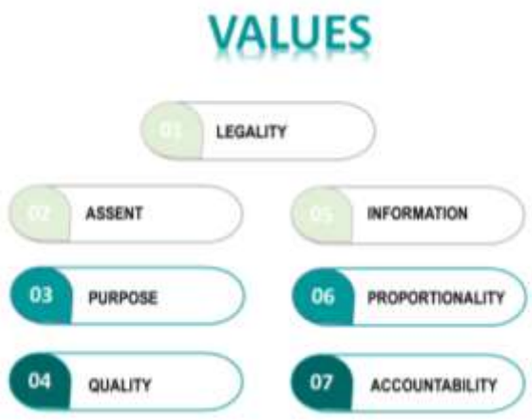

Figure 3 Values
Fuente: INAI. (2018). Valores. Mexico. Available in: http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

1. **Lawfulness and Loyalty (Legality):** Refers to the processing of personal data in compliance with Mexican laws and international law. Lawfulness indicates that the person in charge can only do with the personal data only what is allowed and Loyalty states that the obtaining of data cannot be done through deceptive or fraudulent means.

2. **Assent:** Refers to the processing of personal data will be subject to the consent of the owner, except for the exceptions provided by the same law, there are 2 types of consent: **Tacit:** is when the information is collected directly or personally, when the data is they obtain indirectly from the owner and / or when electronic communication is used. **Expressed**: an evident consent of the owner is required when dealing with sensitive data, such as financial or patrimonial data, when required by law and / or when it is an agreement between the owner and the person responsible.

3. **Purpose:** The reason for which personal data are required and that are the source of the legal relationship, there are primary and secondary, secondary are necessary for the legal relationship and are used for other targets such as marketing or transfer to other companies.

4. **Quality:** Refers to the personal data:
a. Be exact (they are true or faithful)
b. Complete
c. Pertinent (effectively corresponds to the owner and not to a homonym)
d. Updated (they refreshed and correspond to the real situation of the owner)
e. Correct (comply with the above characteristics)

5. **Information:** Let the owner know the main characteristics of the treatment to which his personal information will be submitted, which is specified in the privacy notice.

6. **Proportionality:** Indicates that only personal data that are necessary and appropriate for the purposes of the treatment are handled, limiting the period of this.

7. **Accountability:** It is to ensure compliance with the principles of those responsible for the owner and, where appropriate, the performance of accounts, considering how the owner authorized the use of personal data in the privacy notice. It is the obligation of those responsible to use the standards, best practices, corporate policies and self-regulation schemes that allow them to guarantee due treatment.

It is the obligation of those responsible for personal data to abide by the best information security practices to comply with the characteristics of an information security system, such as:

– Confidentiality
– Integrity
– Availability

And be able to maintain administrative, technical and physical measures to protect personal data against damage, loss, alteration, destruction, access or unauthorized treatment and ensuring the secrecy and custody to which it is bound by any person who treats, collects or transfers data personal at any stage of your treatment.

Privacy Notice: Its main purpose is to establish and delimit the scope, terms and conditions of the processing of personal data, so that the owner can make informed decisions regarding their personal data and maintain control and provision of information that It corresponds. There are three types of privacy notices:

Integral: which is the complete notice where it is identified and has the address of the person in charge; makes express signals of sensitive personal data; manifests the negative mechanisms for the secondary purposes; specifies the clauses of acceptance or not of the transfer; revocation mechanisms; what data will be subjected to the treatments; what is the purpose, means and procedures to exercise ARCO rights; means to limit the use or disclosure of personal data; and the means of how the changes in the privacy notice will be communicated to the owners.

Notices Simplified and short: is an immediate disclosure notice containing the identity and address of the person responsible; the purposes of the treatment and the mechanisms that the person in charge offers so that the owner knows the integral privacy notice.

Conclusions

As we mentioned at the beginning, data is a very important asset, its accumulation can be a valuable element, but we must also protect it against misuse and in that sense, we need laws that protect us. Although Mexico has taken a great step forward in issuing the Personal Data Protection Law, now it is up to each one of us to realize that the security and responsibility of the data starts with oneself. Almost always the privacy notices are signed without reading them, without knowing what we are authorizing the person in charge and what treatment of the information will be given; who else is going to transfer the data and this is very common in our lives. When we download some application, when we want some quote, information, or when we are stopped in the street to conduct surveys and then we complain that we have many calls offering services and / or products that we do not identify why they have our data, or worse still receive extortion calls.

Let's start with the care of our personal data, we orient the children and adolescents who provide a lot of data in social networks; let's see that a data protection program is implemented in organizations and when it is already implemented we have a comprehensive vision of the analysis and management of the risks of information processing. In this way the sensation of tranquility and security in the use of the Internet and proportion of data will come by itself.

References

[1] http:// http:// www.nyce.com.mx

[2] INAI. (2018). *Derechos ARCO*. Mexico. Available in: http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

[3] INAI. (2018). *Valores*. Mexico. Available in: http://inicio.ifai.org.mx/Publicaciones/02GuiaAte