REVISTA DE CIENCIAS SOCIALES Y HUMANAS XXI
NIVERSITAS

https://doi.org/10.17163/uni.n35.2021.08

Access to information and processing of personal data. Visions from the academy

Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia

Yadira Rosario Nieves-Lahaba
Autonomous University of Nuevo León, Mexico
yadira.nieveslahaba@gmail.com
https://orcid.org/0000-0001-8465-4869

Gloria Ponjuan-Dante
University of Havana, Cuba
gponjuan@infomed.sld.cu
https://orcid.org/0000-0003-2063-0934

Recibido: 09/03/2021 **Revisado:** 08/05/2021 **Aceptado:** 16/06/2021 **Publicado:** 01/09/2021

Abstract
Currently, the access and use of data rank high in any human activity. People, organizations, and countries pay attention no only to their use, but also to the need of studying how they are obtained, shared, protected, both at the personal and institutional level as social communication is magnified and occupies a higher place in the human behavior, not only face-to-face but also in social networks. This article summarizes a research accomplished in the academic environment of a Mexican university aiming to reflect the behavior of a sample of over 300 students relating to the access to information and data management, highlighting the most significant concerns they have on these topics. An analysis of the results of the survey and research technique used is presented. The main result obtained was that the students granted great importance to have rights on the personal data and, specially, to be able to oppose or annul that these can be obtained or used. On the other hand, they are not very cautious with the privacy of the data as most of them share personal information with friends and acquaintances. This means that this type of behavior towards data management is little congruent

Keywords
Open data, personal data, data processing, data privacy, data security, data regulations.

Suggested citation: Nieves-Lahaba, Y., & Ponjuan-Dante, G. (2021). Access to information and processing of personal data. Visions from the academy. *Universitas-XXI, 35*, pp. 163-181. https://doi.org/10.17163/uni.n35.2021.08

Resumen
Hoy en día, el acceso y uso de datos ocupa un lugar destacado en cualquier actividad humana. Cada vez hay más atención no solo a su uso, sino también a la necesidad de estudiar cómo se obtienen, cómo se comparten, cómo se protegen, tanto en el plano personal como en lo institucional, ya que la comunicación social se magnifica y ocupa un altísimo lugar en el comportamiento humano empleando no solo lo presencial. Este trabajo sintetiza una investigación realizada en la Facultad de Filosofía y Letras de la Universidad Autónoma de Nuevo León en México con el objetivo de describir el comportamiento de una muestra de más de 300 estudiantes en relación con el tratamiento de los datos personales destacando las preocupaciones más significativas que tienen sobre estos temas. Se presenta el análisis de los resultados de la encuesta, técnica de investigación empleada. El principal resultado fue que los estudiantes conceden gran importancia a tener derechos sobre los datos personales y en especial a poder oponerse o cancelar que estos se obtengan o se usen, pero por otra parte no son muy cuidadosos con la privacidad de estos pues comparten en su mayoría datos personales con amigos y conocidos. Se concluye que este tipo de comportamiento hacia el tratamiento de los datos es poco congruente, lo que advierte de la necesidad de un mejor y mayor conocimiento sobre el tratamiento de los datos personales.

Palabras clave
Datos abiertos, datos personales, procesamiento de datos, privacidad de datos, seguridad de los datos, normatividad de datos.

Introduction

At present, different approaches are being developed that allow strengthening the individual action of different segments of society regarding the access and use of data and information, in such a way as to be able to elevate and improve the behavior of different groups. The specialized literature reports isolated experiences that address the treatment of data with different scopes, developed mainly in educational contexts, in order to know behaviors, propose scenarios and mechanisms that facilitate the capture, storage, and dissemination of data and information that are used in different moments of individual activity. (Barreau, 1995, 2008, 2009; Cotino et al., 2020). Ferran-Ferrer and Pérez-Montoro (2009) investigated individual behavior in a sample of students at a university in Barcelona. The study took into account variables such as: access to information (needs/sources/forms

of access-subscriptions.), Information management (treatment and integration/recovery and preservation/selection criteria/satisfaction criteria), information uses (creation/integration/communication channels/information sharing/collaborative ways of working), informational skills (expert/non-expert), among others. The advances that are reported in the social sciences, locate in a prominent place everything related to the management of personal data. Contemporary society gives priority to communication in all its manifestations, giving special attention to communication in digital environments in order to facilitate different activities and responsibilities of the community and where the processing of personal data is of great interest to everyone (Arellano & Ochoa, 2013). However, the study of the perception of university students about the processing of personal data has not been widely approached in such a way as to allow the exploration of qualitative or quantitative data to account for generalized behaviors: therefore, this study aims to contribute to the formation of ideas around the theme. Much progress must be made even in terms of technological means having elements that contribute to the respect of these rights and that facilitate a flow of quality data and information. It is the era of truth, and it is an obligation that the messages and data that are transmitted through various channels carry information and not disinformation.

Data management and information security

Informational self-determination is an essential right to take into account in the design and operation of information systems, whether automated or not, therefore data processing must not only comply with regulations, but must also contribute to the Citizens' literacy in this matter, so that they are informed about the rights of the owner of the data and, at the same time, the principle of data quality is maintained (Sánchez-Castañeda & Márquez, 2017; Hernández & Zavala, 2018; Garriga, 2009; Porcelli, 2019; Domínguez, 2016).

A few decades ago, Páez (1992) expressed: "in ancient times, Western man wanted to be wise; then modern man wanted to be knowledgeable; contemporary man seems to be content with being informed (and possibly future man is not interested in anything other than having data)" (p. 10).

The data allow us to represent facts, concepts, dimensions and are part of our language, of our management, they also make it possible to establish relationships to determine behaviors in different processes. Information is generated, distributed, and used from the data.

In recent years, projects and experiences have been presented in relation to data management, not only for research, but for any personal activity. The volume of electronic data and its exchange through different channels are increasing rapidly. Being such a vital aspect for different facets of civic life, it is to be expected that studies will be developed around it, and policies that lead to its protection are generated since erroneous data when multiplied, can lead to falsehoods, and it continues to grow and multiply in inappropriate applications. Public policies in relation to data management have emerged, although unfortunately there are still examples of non-compliance and mishandling, intentional or not, of personal data (Ortega, 2015).

The exercise of rights over personal data, in legal matters, has been the object of observation from different angles and at different times (González, 2019; Requena & Sánchez, 2014; Araujo, 2016). Its scope and significance have been gradually modified to show policies that strive to strengthen collective guarantees (Aparicio & Pastrana; 2017, Hernández, 2006). In Mexico, Article 6 of the Mexican Constitution has been modified at different times, currently, it not only expresses the right of freedom of expression but also the right to access information. Article 16, modified on June 1, 2009, is specific when it mentions that everyone has the right to protect their personal data. This right is ratified and established (Feregrino, 2012), in the regulatory body of the Federal Law on Protection of Personal Data Held by Private Parties (Chamber of Deputies of the H. Congress of the Union, 2010) approved by the Congress of the Union in 2010, through the ARCO rights that have to do with access, rectification or correction of personal data obtained from individuals, as well as the right to object to their being collected (ARCO Rights: Access, Rectification, Cancellation or Opposition).

In addition to these rights, the regulation attached to this law (Chamber of Deputies of the H. Congress of the Union, 2011) addresses eight guiding principles for the protection of personal data, these are: legality, consent, information, quality, purpose, loyalty, proportionality, and responsibility.

By interrelating these principles with the context of the informational phenomenon, Ozmen-Ertekin and Ozbay (2012) present their vision about data quality, through the accessibility and security dimensions. They consi-

der accessibility as the ease and breadth of access to information and security with respect to whether or not there is protection against unauthorized access. Quality dimensions refer to the set of quality attributes to which consumers consistently react. (Wang et al., 2001; Portilla-Romero, 2017). Other more enlightening elements are provided by Páez (1992) when he offers a series of parameters to evaluate the quality of the data, these are: "volatility, comparability, timeliness, reasonableness, sensitivity, functionality" (p. 104).

Mendoza (2018) emphasizes its importance within the domain of companies when he states:

> It is important to know the dimension of the regulation of the right to protection of personal data in possession of the service companies established in Mexico, through the normative logical reasoning that allows analyzing the principles and the fulfillment of obligations and duties in the matter, according to the characteristics of this human right. (p. 269)

There is no doubt that the value of data has increased both from an economic and social point of view (Mendoza, 2018; Monsalve, 2017).

> Currently, personal data has an economic value, comparable to certain intangible assets, such as software or the commercial value of domain names. This has led to consider them as the oil of the information and knowledge society. (Mendoza, 2018, p. 269)

The information as a result of the logical combination of the data, which shows a reasoned significance, is an essential asset for the performance of the organizations "the security of said information and the systems that process it is a first-level objective" (Orrego, 2013, p. 21).

The relevance of the relationship between data and information, "does not lie in the data itself, but in the treatment, association with other data and the utility that it is given" (Mendoza, 2018, p. 269). Organizations must carry out security processes (Meraz, 2018, Hernández, 2006, Galvis & Pesca, 2019, Chamber of Deputies of the H. Congress of the Union, 2017) and "implement a system that addresses this task in a methodological, documented way and based on clear security objectives and an accurate assessment of the risks to which the organization's information is subjected" (Orrego, 2013, p. 21).

Materials and methods

The objective of this research was to explore the behavior of university students towards the processing of personal data. The methodology was based on the analysis of documents on the subject, definition of variables, definition of the technique to be applied, survey design, survey pilot test, survey application, data standardization, analysis results, and communication results. The spatial limit was made up of the undergraduate students of the Faculty of Philosophy and Letters of the Autonomous University of Nuevo León. The selected population was of the intentional type, as it was a population that we had access to. The population size was 5000 students. A sample of 420 students was randomly taken from this population. The data was obtained through a survey, which was applied online, with the support of the electronic tool QuestionPro. Of the 420 surveys, 383 were valid. 91.73 % of the respondents were between 18 and 30 years old.

The variables are described below:

- Rights on personal data: Refers to the rights to access, rectify, correct or oppose the collection of personal data (ARCO Rights in Mexico).
- Personal data security: It refers to the routines to protect personal data in digital environments, as well as with whom the personal data is shared
- Privacy of personal data: It refers to the types of consequences of losing personal data Regulations in Mexico: It refers to the regulatory instruments that exist in Mexico to protect personal data and guarantee access to information

Analysis and results

Rights over personal data

This variable was addressed using a Likert scale (very important, not very important, and not at all important). The situations that were included are related to the exercise of ARCO rights that exist in Mexico.

The operationalized results can be observed in the following table 1. The high percentage of responses in the very important indicator points to the positive recognition of those surveyed in situations related to ARCO rights.

Table 1
Distribution of responses on ARCO rights for the indicator "Very important"

Situations that exemplify the rights over personal data	Response percentage Very important
Request the cancellation of personal data when they are being used improperly.	98 %
Oppose the processing of your personal data if they have been collected without your consent.	96 %
Have access to the privacy notice to which the processing of my data is subject.	94 %
That your personal data can be deleted when, for example, you cancel your bank account.	94 %
Know the treatment of which my personal data is subject, as well as the transfers made.	94 %
Know where I can rectify my personal data.	94 %
Request and be informed about your personal data, its origin.	93 %
Know the means by which organizations provide information on the use of your personal data.	90 %
Request the rectification of your personal data when they are inaccurate.	89 %
Oppose the processing or collection of personal data when this is not carried out by a public entity.	89 %

In the context of educational institutions, especially universities, these rights are very significant because they establish a culture that must prevail in all actions of students during their responsibilities and future actions.

Data privacy

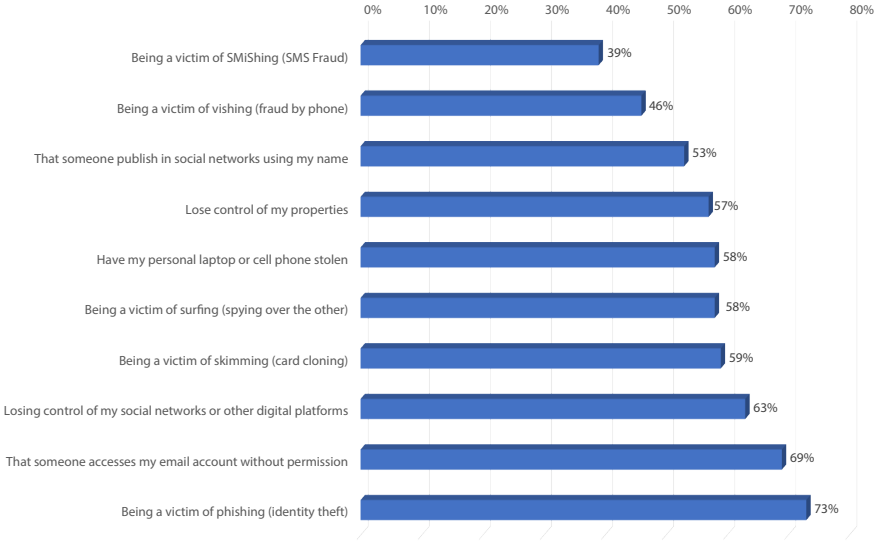
Data privacy was addressed by asking who is personal data shared with on social media, as well as the consequences of losing it.

Another aspect to analyze in relation to data privacy is the one that addresses the consequences in the event of it being violated. Respondents were presented with some of these consequences and asked to reveal which ones

they were most concerned about. Figure 1 shows the results in order of greatly to least concern.

The consequence that most worries respondents is being a victim of phishing (identity theft, 73 %), and the least they worry about (39 %) is being a victim of SMiShing (SMS Fraud).

Figure 1
Distribution of consequences when the privacy of personal data is violated



When linking the previous results with the gender variable, convergences and divergences in opinions are observed (see table 2).

Both for the male gender (13.82 %) and for the other gender (25.00 %), someone accessing their email account without permission is what concerns them the most with regard to the privacy of their data. However, for the female gender, this aspect occupies second place (11.41 %).

What worries women the most is being a victim of phishing (identity theft, 12.83 %). In this case, this aspect, both for the male gender (11.98 %) and for the other gender (16.67 %), this aspect occupies the second place of importance.

The third most neuralgic aspect regarding data privacy behaves as follows: the male gender is concerned about three situations: being a victim of skimming (card cloning, 10.83 %), losing control of social networks or other digital platforms (10.83 %), in this case, it shares this third place with the female gender (11.07 %) and lose control of the properties that it shares with the other gender (16.67 %).

Table 2
Distribution of crossover between the data privacy variable and the gender variable

Consequences	Male	Female	Other
That someone accesses my email account without permission	13.82 %	11.41 %	25.00 %
Have my personal laptop or cell phone stolen	9.68 %	10.11 %	8.33 %
That someone publish in social networks using my name	9.45 %	9.09 %	8.33 %
Being a victim of surfing (spying over the other)	9.45 %	10.34 %	8.33 %
Being a victim of phishing (identity theft)	11.98 %	12.83 %	16.67 %
Being a victim of SMiShing (SMS Fraud)	6.45 %	6.81 %	0.00 %
Being a victim of skimming (card cloning)	10.83 %	10.16 %	8.33 %
Being a victim of vishing (fraud by phone)	6.68 %	8.46 %	0.00 %
Losing control of my social networks or other digital platforms	10.83 %	11.07 %	8.33 %
Lose control of my properties	10.83 %	9.71 %	16.67 %
Total	19.66 %	79.79 %	0.54 %

The concern about the loss of personal data when being a victim of identity theft, or when losing control of social networks, digital platforms, or card cloning, to be specific in the case of this study, involves at least two aspects; the fear of the people towards the loss of their privacy and the interference in their privacy, both infringe on the exercise of people's rights, by people not having control of their personal information, the unauthorized use of bank funds that result in debts damaging the financial situation and credit history of the person, as well as repercussions on public image by damaging the reputation of the person affected by these circumstances.

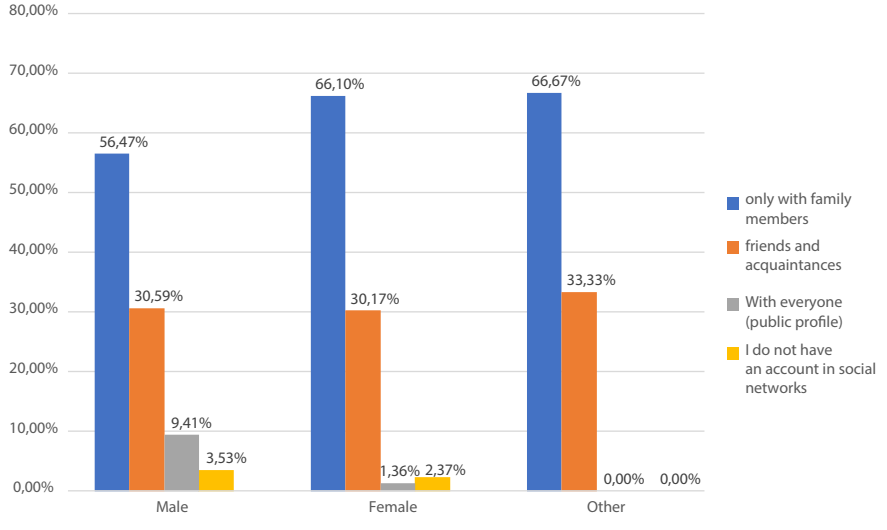
Personal data security

The security of personal data was investigated from the routines used to protect personal data in web environments, as well as with whom data is shared on social networks.

When addressing with whom personal data is shared, 64 % responded that they share data with friends and acquaintances, 30 % only with family members, and 3 % with everyone. Only 3 % responded that they do not have social networks.

When delving into the analysis and relating these results to the gender variable, the results indicate that Male, Female, and Other respond in a similar way when it comes to sharing information with family, friends, and acquaintances, or when making the decision not to have social networks (Figure 2).

Figure 1
Distribution of crossover between the data privacy variable (data sharing) and the gender variable



However, the distance increases —that is— there is no longer so much similarity when it comes to sharing data publicly. In this case, the male gender tends significantly and mainly to carry out this practice (see table 4).

When examining how data protection is carried out, in this case, the responses were, in the first place, the elaboration of a complicated password (81 %), in second place, to avoid publishing data on social networks (64 %), as well as not downloading from suspicious sites and thirdly to avoid chatting with strangers (57 %) (see table 3).

Table 3
Distribution of routines to protect personal data in web environments

Routines to protect personal data	Percentage
Create a complicated password	81 %
Do not publish my data on social networks	64 %
Don't download from suspicious sites	64 %
Don't chat with strangers	57 %
Check emails if they invite you to click on a link	49 %
Change my password every so often	36 %
Use security or two-step filters on my accounts	36 %
Browse incognito window	29 %
Use ad blocker	26 %
Call my financial institution in case of suspicion of interference	17 %
Publish with false information	17 %

The routines that respondents use the least to protect their accounts correspond to publishing with false data (17 %) or calling a financial institution in case of suspicion of intrusion (17 %).

It is possible to corroborate the previous data (table 4) by relating them to the results of Figure 2. Creating a complicated password is the most commonly used routine.

Table 4
Relationship between routines to protect personal data and with whom data is shared in web environments

Indicators	Friends and acquaintances	Family	I do not have an account in social networks	With everyone (public profile)
Create a complicated password	18.12 %	14.93 %	13.11 %	22.45 %
Change my password every so often	7.21 %	7.99 %	9.84 %	10.20 %
Call my financial institution in case of suspicion	3.61 %	3.82 %	4.92 %	2.04 %
Do not publish my data on social networks	13.72 %	14.76 %	11.49 %	6.12 %
Publish with false information	2.55 %	4.86 %	8.19 %	4.08 %
Use ad blocker	5.54 %	4.69 %	6.56 %	8.16 %
Browse incognito window	5.80 %	6.77 %	4.92 %	4.08 %
Don't download from suspicious sites	13.19 %	12.67 %	11.48 %	16.33 %
Check emails if they invite you to click on a link	10.38 %	9.72 %	9.84 %	12.24 %
Use security or two-step filters on my accounts	7.74 %	7.47 %	6.56 %	8.16 %
Don't chat with strangers	12.14 %	12.33 %	13.11 %	6.12 %
Total	62.37 %	31.60 %	3.35 %	2.69 %

The routine of not publishing data on social networks is in second place regarding the preferences for the security of personal data in web environments, both for those who share with friends and acquaintances and for those who share with relatives. However, for those with a public profile, second place corresponds to avoid downloading from suspicious sites.

This same routine is the third place for the remaining groups. For those in the group that shares information publicly, the third preferred routine for data security is to verify the security of emails which invite you to click on a link.

These results reveal that respondents are aware of the basic issues regarding the security of their personal data in web environments. However, issues of the more advanced users such as browsing in an incognito window

or using an ad blocker were not among the most selected by the respondents. Although these actions are not an absolute guarantee for the security of personal data, they do indicate that the use of routines that have to do with so-called *cookies* is not taken into account.

Users a little more experienced in digital environments carry out actions such as warning the financial entities with which they conduct financial services, verify emails with links, as well as using ad blockers in conjunction with reviewing the policies for the use of cookies to be aware that type of data is collected and choose whether or not to allow its use. Understanding the functions of cookies, the types or levels that exist, the processes for their management, or the types of data they collect, is part of contemporary literacy. Cookies, small text files that allow to navigate the website and make use of its functions, as well as having information and differentiating site visitors can also, depending on the category, collect data and personal information. A website can use its own and/or third-party cookies or it can also use anonymous cookies, protecting users so that their activity is not tracked when browsing other websites.

Regulations in Mexico

In relation to the regulatory instruments that exist in Mexico for the protection of personal data and guarantee access to information, the results give an indication of the need for education and training in regulatory matters as one of the ways to promote a coherent informational behavior and safe in digital environments.

In this case, the knowledge (through a Likert scale A lot, Little, Nothing) of laws and other normative instruments were investigated. Approximately only 7.5 % expressed knowing a lot: the Open Access Law, the Science and Technology Law, the Law of Transparency and Access to Public Information, and Articles 6, 7, and 8 of the National Constitution. A slightly higher percentage, but also not very significant, was that 15 % referred to being very familiar with the sites of national information transparency in which the university's transparency pages were included.

Discussion and conclusions

University students of social sciences and humanities consider the right to personal data very important. That they allow; access, rectify, correct, or oppose (ARCO rights) to its treatment. In this sense, they highlight the importance of the right to oppose or cancel personal data when they are being used improperly or collected without consent. This recognition not only notes not oly the importance they attach to it from a pragmatic point of view, but also to the concordance with the principle of informative self-determination (Sánchez-Castañeda & Márquez, 2017; Garriga, 2009).

Taking into account that personal data refers to what makes a natural person identifiable (Rivera, 2019; Remolina, 2013; García, 2007) and that when combined they become information that describes, characterizes, or differentiates individuals, it is necessary to have and know the right to the treatment to which these data are subjected to. In this sense, Ferrán-Ferrer and Pérez-Montoro (2009) mention the importance of:

> Having the exact information, in the right place, in the right format, at the right time, and sufficiently complete and of quality to satisfy all the information needs that arise in the different areas of daily life. (p. 366)

Data privacy is an aspect that reflected the concerns of university students, in relation to the consequences of their data being exposed. This situation must be addressed from different spheres, either from the different levels of formal education or informally by the government institutions in charge of monitoring and protecting personal data so that this uneasiness is not an element that limits freedom and the effectiveness of their rights. The use of digital environments and technologies should not limit the scope of freedom and data protection (García, 2007; Castellanos, 2020), however, as they develop, new ways to infringe on privacy appear. The findings indicate that the people surveyed are concerned about being a victim of phishing (identity theft), that someone accesses their email account without permission or to lose control of social networks or other digital platforms and it is to be expected since, in Mexico, identity fraud is a growing problem. In 2015 it ranked eighth worldwide in this crime, in that same year 100,000 complaints were received throughout the financial system, with this figure, complaints had increased more than 500 % compared to 2011 (Juárez, 2016).

However, the findings indicate that the actions carried out to secure personal data, in digital environments, are basic. Respondents protect themselves mainly by creating a complicated password. Although there are at least three specific routines that are also used: do not post data on social media, do not download from suspicious sites, and do not chat with strangers, these underscore the basic nature of the employed routines. The need for education on data protection and informational behavior is noted, something that Swigon (2013) proposes as personal knowledge and information management or what Gray et al. (2012) called data literacy. This proposal not only refers to the management of personal information but to the development of informational competencies that are essential to increase the level of competencies that enable reaching this objective. The finding also coincides with the study carried out by the Federal Institute of Telecommunications in Mexico (2019), which advocates for the need for public and private actions to expand the skills of the population in the use of ICT with special focus on adolescents.

This study suggests that little is known about the regulations for the treatment and protection of personal data existing in Mexico. It is evident that this time requires public policies that regulate everything related to data and information (Araujo, 2016; Requena & Sánchez, 2014) and that said regulations to be known by all social groups that in turn, aware of their rights, behave in accordance with what is regulated and established and also contribute to its dissemination and compliance. This finding makes us reflect on the performance of government organizations in the education of the population, if one takes into account that among the generic obligations of the general law of transparency and access to public information in Mexico, it is stated in article 66 that It is an obligation to establish the technological conditions and to use means of disseminating information to develop the knowledge of the population in matters of transparency and protection of personal data (Sánchez-Castañeda & Márquez, 2017; Chamber of Deputies of the H. Congress of the Union, 2020).

On the other hand, the fact that the best-known regulations by the respondents are those related to the university's transparency pages, corresponds to the role of public universities in establishing and publicizing an open data model that is useful for their community (Domínguez, 2016; Islas 2017).

The results achieved by this research provide an opportunity to set new goals and objectives that allow other generations to master these issues and act

accordingly. A true information society requires that its components be educated, becoming literate in everything related to the handling of data, information, and knowledge, but that they also master policies, rights, and obligations.

A limitation of the study is that no studies were found with which broad comparisons could be made. Another limitation is the fact that in Mexico the subject has been only relatively recently approached outside the business sphere.

Bibliography

Aparicio, J., & Pastrana, M. (2017). Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México. *Revista latinoamericana de derecho social*, 24, 175-193. http://bit.ly/3uu2v15

Araujo-Carranza, E. (2016). El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. *Revista IUS, 3*(23). https://doi.org/10.35487/rius.v3i23.2009.195

Arellano, W., & Ochoa, A. (2013). Derechos de privacidad e información en la sociedad de la información y en el entorno TIC IUS. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C., VII*(31),183-206. https://bit.ly/3pZcZSM

Barreau, D. K. (1995). Context as a factor in personal information management. *Journal of the American society for information science*, *46*(5), 327-339. https://bit.ly/3qY2EYo

Barreau, D. K. (2009). Gestión de información personal, no solo recuperación de información personal. *El Profesional de la Información, 18*(4), 61-364. https://doi.org/10.3145/epi.2009.jul.01

Barreau, D. K. (2008). The persistence of behavior and form in the organization of personal information. *Journal of the American Society for Information Science and Technology*, *59*(2) 307-317. https://bit.ly/3qY2EYo

Cámara de diputados del H. Congreso de la Unión (2010). Ley Federal de Acceso a la Información y Protección de Datos personales. https://bit.ly/3kmw2F7

Cámara de diputados del H. Congreso de la Unión (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. https://bit.ly/3bB5OuB

Cámara de diputados del H. Congreso de la Unión (2020). Ley General de Transparencia y Acceso a la Información Pública. https://bit.ly/3uzesm0

Cámara de diputados del H. Congreso de la Unión (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. http://bit.ly/2MoLHr9

Castellanos, J. (2020). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos de Información*, *11*(21), 59-82. https://dx.doi.org/10.5557/IIMEI11-N21-059082

Cotino-Hueso, L., Rebollo-Delgado, L., Vidal-Fueyo, María del Camino, Troncoso- Reigada, A., García-Mahamut, R., Rallo-Lombarte, A., Murillo de la Cueva, Pablo Lucas, & Medina-Guerrero, M. (2020). Encuesta sobre la protección de datos personales. *Teoría y Realidad Constitucional*, (46), 15-118. http://bit.ly/3smSZej

Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*. Dykinson, S.L.

Feregrino, E. (2012). *Ley Federal de Protección de Datos Personales en posesión de los particulares*. Ediciones Fiscales ISEF. 100.

Ferran-Ferrer, N., & Pérez-Montoro, M. (2009). Gestión de la información personal en usuarios avanzados en TIC. *El profesional de la información*, *18*(4), 365-373. http://bit.ly/37Kwo3r

Galvis-Cano, L., & Pesca-Mesa, D. A. (2019). Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y comunicación en la era digital. *Iusta*, (52), 51-76. https://doi.org/10.15332/25005286.5482

García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, *40*(120), 743-778. http://bit.ly/3snKSy4

Garriga, D. A. (2009). *Tratamiento de datos personales y derechos fundamentales*. Dykinson.

González, L. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros *Revista Estudios Socio-Jurídicos*, *21*(1), 209-244. https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941

Gray, J., Chambers, L., & Bounegru, L. (2012). *The Data Journalism Handbook*. O'Reilly Media.

Hernández, A., & Zavala, O. (2018). Datos personales en las relaciones laborales del sector privado. *Revista Latinoamericana de Derecho Social*, (27). http://bit.ly/3aRWC6b

Hernández, V. (2006). Referentes legales para un marco protector de datos personales. *Ra Ximhai*, *2*(3), 567-580. https://doi.org/10.35197/rx.02.03.2006.02.vh

Instituto Federal de Telecomunicaciones en México (2019). *Uso de las TIC y actividades por internet en México: impacto de las características sociodemográficas de la población* (versión 2019). IFT. https://bit.ly/2ZTF1UM

Islas, J. (2017). *Estudio sobre los alcances del derecho de acceso a la información en Universidades e Instituciones de educación superior públicas dotadas de autonomía derivado de la Reforma Constitucional en materia de transparencia*. INAI. https://bit.ly/3srbcXY

Juárez, R. (2016). Iniciativas. Senado de la República. *Gaceta del Senado*. México, 2016. http://bit.ly/2MnapYO

Kettinger, W. J., & Marchand, D. A. (2011). Information management practices (IMP) from the senior manager's perspective: An investigation of the IMP construct and its measurement. *Information Systems Journal*, *21*(5), 385-406.

Mendoza, A. O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista del Instituto de Ciencias Jurídicas de Puebla*, *12*(41), 267-291. https://bit.ly/3uGgAZs

Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales *Revista IUS*, *12*(41) 293-310. https://bit.ly/3qRZSDW

Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. *Prolegómenos. Derechos y Valores*, *XX*(39),163-195. https://bit.ly/3ko0JtJ

Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano*, *4*(6). http://bit.ly/2O3BYHi

Ortega, A. (2015). La desprotección "internacional" del titular del derecho a la protección de datos de carácter personal barataria. *Revista Castellano-Manchega de Ciencias Sociales*, *19*, 37-56. http://bit.ly/3uyioTY

Ozmen-Ertekin, D., & Ozbay, K. (2012). Dynamic data maintenance for quality data, quality research. *International Journal of Information Management*, *32*, 282-293. https://doi.org/10.1016/j.ijinfomgt.2011.11.003

Páez, I. (1992). *Gestión de la inteligencia, aprendizaje tecnológico y modernización del trabajo informacional. Retos y oportunidades*. Universidad Simón Bolívar. https://bit.ly/3dHkKKs

Porcelli, A. M. (2019). La protección de los datos personales en el entorno digital, los estándares de protección de datos en los países iberoamericanos. *Quaestio Iuris*, *12*(2). https://doi.org/10.12957/rqi.2019.40175

Portilla-Romero, J. (2017) Gobierno de datos, un potenciador de los sistemas de gestión de calidad. *Signos*, *9*(2)159-172. https://doi.org/10.15332/s2145-1389.2017.0002.10

Requena, E. J., & Sánchez, L. F. J. (2014). El derecho a la información y la protección de datos personales en la constitución mexicana. *Acalán Revista de la Universidad Autónoma del Carmen*, *1*(4), 27-31. http://bit.ly/3swHYqZ

Remolina, N. (2013). Tratamiento de datos personales en el contexto laboral. *Revista Actualidad Laboral*, *175,* 19-24. https://bit.ly/2ZRoHnA

Rivera, V. (2019) Realidad sobre la privacidad de los datos personales en Costa Rica. E-*Ciencias de la Información, 9*(2), 68-81. https://doi.org/10.15517/eci.v9i2.37503

Sánchez-Castañeda, A., & Márquez, D. (2017). *Estudio sobre transparencia y acceso a la información en personas físicas y morales. Alcances de la reforma constitucional y legal*. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://bit.ly/37NPbeh

Swigon, M. (2013). Personal knowledge and information management-conception and exemplification. Journal of Information. *Science*, *46*(5), 832-845. https://doi.org/10.1177/0165551513501435

Wang, R. Y., Ziad, M., & Lee, Y. W. (2001). *Data quality*. Kluwer Academic Publishers.