ARTICLE

Mexico (Non-)Adequacy to European Standards on Personal Data Protection in the Context of Employment

María Solange Maqueo Ramírez*

This article analyses the main standards and regulations put in place by the European Union (EU) and the Council of Europe with respect to the privacy and personal data protection of workers. It demonstrates that there is a current tendency toward the establishment of specific rules aimed at strengthening employees' rights vis-à-vis employers' interests. It also shows that there is a preventive rather than a reactive approach in the European model. However, this article argues that, albeit strongly influenced by Europe, the Mexican legal framework on personal data protection does not follow this trend, due to legislative asymmetries between the public and private sector, as well as the lack of specific regulation in this field.

Keywords: Privacy, Data protection, Employment, Legitimate interest

1 Introduction

There is growing international concern regarding privacy and personal data protection in the context of employment. Technological advancements have driven a shift in employers' leeway to monitor and supervise their employees, search their possessions or even conduct a personal search. Additionally, there is widespread recognition that sensitive personal information used in employment shows an increasing tendency, encouraged by domestic regulations on health and welfare at the workplace.

In this context, this article focuses on the existing standards and regulations issued by the Council of Europe and the European Union (EU) on privacy and personal data protection in employment. Considering that Mexico's legal system has been strongly influenced by both pathways, the research question asks to what extent these influences can be observed in this field. This article concludes that the Mexican legal framework deviates from the route set by the European model, which encourages the development of specific rules to guarantee employees' privacy and personal data protection, as well as to devise provisions that seek to limit and clarify the scope of employers' lawful basis for the collection and processing of personal data.

2 Council of Europe's standards on privacy and personal data protection in the employment context

The first half of the 1980s is generally considered significant for the debate about the scope that employers have to monitor their employees,[1] which is in line with the beginning of international regulations on the protection of personal data in the face of advances in automated technology. It is not mere coincidence that the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (1981) (Convention 108), both considered pioneering instruments in the international development of the principles of the right to personal data protection, were issued in the same decade.[2]

Precisely, based on the Convention 108, in 1989, the Committee of Ministers of the Council of Europe issued Recommendation No. R (89) 2 (1989 Recommendation), which intended to apply the principles of personal data protection to 'the collection and use of personal data for employment purposes in both the public and private

Notes

* Director of the Legal Studies Division at the Centre for Research and Teaching in Economics (CIDE) in Mexico and former President of Advisory Council to the National Institute for Transparency, Access to Information and Personal Data Protection (INAI). Email: maria.maqueo@cide.edu.

1 Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 Cal. L. Rev. 735 (June 2017).

2 *See* Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

GLOBAL PRIVACY LAW REVIEW, Volume 2, Issue 2

sectors'.[3] It was a non-binding international instrument specifically aimed at establishing common standards in order to ensure privacy and personal data protection of employees vis-à-vis their employers.

The 1989 Recommendation introduces the principles provided for in the Convention 108 to the employment sector, including the following:

(1) Information and consultation of employees. The application of this principle requires that employers 'fully inform or consult their employees about the introduction or adaptation of automated systems for the collection and use of personal data or employees', as well as 'the introduction or adaptation of technical devices designed to monitor movements or productivity of employees'.[4] This principle also includes the obligation to inform employees about any decision that is made based on their personal data and that affects them.[5]

(2) Regarding data collection, the 1989 Recommendation establishes that 'personal data should in principle be obtained from the individual employee'. Otherwise, it is necessary to inform the employee that personal data would be obtained from different sources.[6]

(3) It also states that 'personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of employment as well as the evolving information needs of the employer'.[7]

(4) Regarding data storage, the 1989 Recommendation provides that personal data 'should be accurate, where necessary kept up to date, and represent faithfully the situation of the employee. They should not be stored or coded in a way that would infringe an employee's rights by allowing him to be characterized or profiled without his knowledge'.[8]

(5) Considering the purpose limitation principle, the 1989 Recommendation states that '[p]ersonal data collected for employment purposes should only be used by employers for such purposes'.[9]

(6) As to special category data processing, the 1989 Recommendation includes the so-called data minimization principle and makes special provision for the collection and use of employee health data. It states that particular categories of data 'should only be collected and stored in particular cases within limits laid down by domestic law and in accordance with appropriate safeguards provided therein. In the absence of such safeguards, such data should only be collected and stored with the express and informed consent of employees'.[10]

One measure to take into consideration regarding health data is that it should be collected directly from the employees concerned, unless they have given their express and informed consent, or in accordance with provisions of domestic law.[11] In addition, 'health data covered by medical secrecy should, in principle, only be stored by personnel who are bound by rules on medical secrecy',[12] and it 'should be stored separate from other categories of personal data held by the employer'.[13]

While the 1989 Recommendation was issued before the emergence of the Internet and social media in every-day life, it also comprised 'the introduction or adaptation of automated devices designed to monitor the movement or productivity of employees'.[14] But it should not overlook the fact that this Recommendation was issued in 1989, which means that it had to be adapted to new challenges as a result of the rapid advancements of information and communication technology.

Consequently, twenty-five years later, the Committee of Ministers of the Council of Europe issued another Recommendation on the processing of personal data in the context of employment that substitutes for the 1989 Recommendation.[15] As the Committee stressed in its Explanatory Memorandum, the main reasons that were taken into consideration for this new Recommendation CM/Rec(2015)5 (2015 Recommendation) were the growing use of information technologies, the tendency of employers to collect data on employees beyond what it is necessary and proportionate, and the introduction of

Notes

[3] Council of Europe, Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment Purposes, adopted by the Committee of Ministers on 18 Jan. 1989 at the 423rd meeting of the Ministers' Deputies, para. 1.1.

[4] *Ibid.*, paras 3.1 and 3.2.

[5] *Ibid.*, para. 6.1.

[6] *Ibid.*, para. 4.1.

[7] *Ibid.*, para. 4.2.

[8] *Ibid.*, para. 5.2.

[9] *Ibid.*, para. 6.

[10] *Ibid.*, para. 10.1.

[11] *Ibid.*, para. 10.3.

[12] *Ibid.*, para. 10.4.

[13] *Ibid.*, para. 10.5.

[14] *Ibid.*, para. 3.1.

[15] Council of Europe, Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, adopted by the Committee of Ministers on 1 Apr. 2015 at the 1224th meeting of the Ministers' Deputies.

specific risks to individuals, such as the processing of biometric or location data.[16]

Thus, like its predecessor, the 2015 Recommendation arose in the context of a profound change in the field of personal data protection.[17] By then, there was already an almost finished draft of the General Data Protection Regulation (GDPR) of the EU, which was eventually issued a year later and entered into force in 2018. At that time, preparatory work regarding the modernization of Convention 108 had also begun.

While the 2015 Recommendation takes up the principles previously set out in its predecessor, it introduces stronger requirements regarding proportionality, personal data minimization, accountability, and transparency principles, in order to ensure consistency with advances in other data protection legal frameworks, particularly that of the EU.

Related to the proportionality and data minimization principles, the 2015 Recommendation establishes that '[e]mployers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned'.[18] According to the principle of responsibility, the 2015 Recommendation notes that '[e]mployers should develop appropriate measures, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes'.[19] In this regard, 'employers should be able to demonstrate their compliance with such principles and obligations'.[20] In cases of sensitive personal data, including biometric or genetic data, those principles and measures are reinforced. Moreover, in accordance with the 2015 Recommendation, health data can only be collected under certain circumstances and in the cases provided for by law.[21] Finally, with reference to the principle of transparency, the 2015 Recommendation lists the information that employers should make available to the employees concerned. In general terms, it includes all personal information held by employers, the purposes and methods of processing, as well as any other information necessary to ensure fair and lawful processing.[22]

An innovation contained in the 2015 Recommendation is the inclusion of provisions on individual automated decision-making. In this regard, it notes that[23]

> '[a]n employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration'.

With this provision, the 2015 Recommendation is in line with the aim of strengthening the right to self-determination in terms of information, in a context of growing technological dependence.

3 EU'S STANDARDS AND REGULATORY FRAMEWORK

Privacy and protection of personal data in the work environment have also received particular attention in the EU. In this regard, the then existing Article 29 Data Protection Working Party (WP29),[24] set forth under Directive 95/46/EC of the European Parliament and the Council, issued two opinions related to data processing at work.

The first one, that is, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, states that, when processing workers' personal data, employers should always bear in mind the following fundamental data protection principles: finality, transparency, legitimacy, proportionality, accuracy and retention of the data, security, and awareness and training of the staff in charge in the processing of personal data.[25]

In this Opinion the principle of consent is subject to differential treatment in the employment context, considering the asymmetric relationship between employers and employees. In this respect, the WP29 emphasizes that employees' consent is a doubtful measure to be considered as a sufficient legal basis to justify the processing of their personal data. In that sense, Opinion 8/2001 states that '[r]eliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment'.[26] Of

Notes

[16] Council of Europe, Explanatory Memorandum to Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, adopted by the Committee of Ministers on 1 Apr. 2015 at the 1224th meeting of the Ministers' Deputies.

[17] For the preparation of its Recommendation CM/Rec(2015)5, the Council of Europe took into consideration the International Labour Office's Code of practice on the protection of workers' personal data, adopted in 1997, Geneva.

[18] *See supra* n. 16, para. 4.1.

[19] *Ibid.*, para. 4.2.

[20] *Ibid.*

[21] *Ibid.*, para. 9.4.

[22] *Ibid.*, paras 10.1 and 10.2.

[23] *Ibid.*, para. 11.4.

[24] Since the abrogation of the Directive 95/46/EC by the General Data Protection Regulation, the WP29 has actually replaced by the European Data Protection Board (EDPB), which includes representatives from the data protection authorities of each Member State of the EU.

[25] WP29, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 Sept. 2001, at 3.

[26] *Ibid.*

course, this does not apply if a legal provision requires the data to be processed or there are other criteria for making data processing legitimate under data protection rules, such as the performance of a contract and the legitimate interests of employers.

In its second opinion, that is, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, the WP29 restates the principles enshrined in its Opinion 8/2001 and its subsequent 2002 Working Document on the surveillance of electronic communications in the workplace. In general terms, this opinion complements the previous one in order to identify different risk scenarios of surveillance and monitoring employees in the current and future technological environment, as well as to consider the new obligations placed on data controllers by the GDPR.[27]

In this regard, Opinion 2/2015 reiterates the idea that 'for the majority of the cases of employees' data protection, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required'.[28] In that sense, this Opinion considers other possibilities such as contract performance, compliance with legal obligations or employers' legitimate interests. However, in any case, it is necessary to comply with the principles relating to privacy and data protection.

Regarding the new obligations of data controllers, which are provided for by the GDPR, this Opinion introduces the following considerations:

(1) Employers, viewed as data controllers, should implement data protection by design and by default as required by the GDPR.[29]

(2) Especially in those cases where processing is 'likely to result in a high risk', employers must carry out a Data Protection Impact Assessment (DPIA).[30] One example is 'a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing including profiling, and on which decisions are taken that produce legal effects concerning the natural person or similarly significantly affect the natural person'. Whilst the DPIA is not mandatory in cases where there is a legal basis for personal data processing, this process could be very useful for employers to comply with the principles and obligations of the right to personal data protection. In particular, this process is useful for assessing the necessity and proportionality of employee information processing when used systematically and extensively,[31] and when decisions based on automated processes produce legal effects or have serious consequences for workers' personal rights.

This Opinion also takes into consideration the provisions of Article 88 of the GDPR. In this regard, it should be noted that this regulation introduces a special mention to personal data processing in the context of employment. In fact, it explicitly recognizes the need to establish a specific regulatory framework for this kind of processing in order to ensure workers' fundamental rights. In accordance with this provision, all Member States of the EU 'may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment'.

Although it is surprising that this provision does not directly regulate the rights and obligations of employers and employees with respect to personal data processing, considering the nature of a Regulation,[32] the mere fact that it creates obligations for the Member States of the EU to issue specific regulations in this field represents an advance. This makes the idea explicit that employers should be subject to more specific and delimited rules in the case of processing of employee personal information. Accordingly, the GDPR takes the position that privacy and personal data protection at work contains more aspects than what have been recognized in the general legal framework, and that an adequate protection of workers' privacy requires a particular legal treatment.[33]

Moreover, the GDPR identifies a limited number of specific cases, other than consent, where the processing of employees' personal data by employers can be considered legitimate. These lawful bases include the performance of employment contracts, the compliance with legal obligations, and the exercise of the legitimate interest of employers, among others. In this regard, Opinion 2/2015 is consistent with the GDPR, regardless of its previous issuance.

Although this regulation explicitly establishes the assumptions that constitute a legitimate basis for the processing of employees' personal information, its implementation and enforcement require previous measures taken by employers in order to comply with the principles provided for in the GDPR.

Notes

[27] WP29, Opinion 2/2017 on data processing at work, adopted on 8 June 2017, at 3.

[28] *Ibid.*, at 6 7.

[29] *Ibid.*, at 8.

[30] *Ibid.*, at 8. In this regard, it should also be noted that the WP29 revisits its Guidelines on DPIA and determining whether processing is 'likely to result in a high risk' for the purpose of GDPR, adopted on 4 Apr. 2017.

[31] *Ibid.*, at 9.

[32] Olga Lenzi, *El control de la prestación laboral a través de fórmulas de videovigilancia: el concreto supuesto del trabajo doméstico*, 146 Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social 159, 174 (2019).

[33] About this position, *see* Elin Palm, *Privacy Expectations at Work What Is Reasonable and Why?*, 12 Ethical Theory & Moral Prac. 201, 202 (Springer Science 2009).

The effective implementation of those measures, such as the very existence of an employment contract that includes the conditions for personal data processing or even to achieve a balance between employers' legitimate interest and employees' privacy interests, is by no means a simple task. This issue will be discussed in the following sections.

4 Employers' legitimate interest

Traditionally, employers have been legitimated to supervise and control their employees. There is a global recognition that they have a legitimate interest in monitoring employees and processing their personal data. The main reasons given by employers are productivity, liability and information.[34] In this regard, the usual allegations for processing employees' personal data include the adequate fulfilment of work, the appropriate use of working tools, the prevention of misconduct or other hostile work environments, the protection of the company's business secrets and other intellectual property, and the taking of measures to avoid any possible liability for employees' actions.

Additionally, there are studies showing that monitoring and surveillance at the workplace could also be justified for the sake of health and welfare coverage for employees. In fact, there is a general perception that these working practices are 'a requisite for innovation and progress'.[35] These current trends can be observed within the International Labour Organization, which has issued 'more than 40 standards specifically dealing with occupational safety and health'.[36] This is also the case of Mexico, which recently issued an Official Mexican Standard (NOM-035-STPS-2018)[37] in order to incorporate a new health and safety standard to identify, analyse and prevent psycho-social risk factors at work.

However, it should be considered that employers' legitimate interests differ from other lawful basis, such as the performance of employment contracts or the compliance with legal obligations. As the Information Commissioner's Office (ICO) in the United Kingdom highlights[38]:

> It is not centred around a particular purpose (e.g. performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate interest is more flexible and could in principle apply to any type of processing for any reasonable purpose.

It is precisely in its flexible and open nature that its own complexity lies, because employers' legitimate interests must be subject to limits. As the WP29 has emphasized, 'the legitimate interest in itself is not sufficient to override the rights and freedoms of employees'.[39]

In the same vein, the GDPR establishes some parameters that serve to define the extent of data controllers' legitimate interests. For instance, as stated in Recital 47, it is necessary to consider the reasonable expectations of data subjects based on their relationship with controllers, in order to ensure that the interests and fundamental rights and freedoms of the data subject are not ignored or underestimated. In this respect, the GDPR mentions, as an example, the specific case of the relationship between employees and employers.

Therefore, employee privacy expectations constitute a relevant aspect to be considered upon assessing whether employers' legitimate interests exist. This is particularly helpful to balance the interests of employers against those of employees. However, this concept does not have clear limits since it depends on a subjective perception of the person concerned, in accordance with the particular situation that governs the employment relationship. In fact, employees do not constitute 'a homogenous group with equally homogenous privacy expectations'.[40] There is no single, universal definition for this term. This explains why this concept has been developed on a case-by-case basis, in accordance with its origins in the common law system.[41]

The European Court of Human Rights (ECHR) has examined in many cases related to the right to private life in the context of employment, in accordance with

Notes

[34] Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 Berkeley Tech. L.J. 979, 982 (2011).

[35] *See* Ajunwa, Crawford & Schultz, *supra* n. 1, at 105.

[36] International Labour Organization (ILO), *Safety and Health at Work*, https://www.ilo.org/global/topics/safety and health at work/normative instruments/lang en/index.htm (accessed 6 Feb. 2021).

[37] Published in the Federal Official Gazette on 23 Oct. 2018.

[38] ICO, *Guide to the UK General Data Protection Regulation* (updated on June 2019), https://ico.org.uk/for organisations/guide to data protection/guide to the general data protection regulation gdpr/legitimate interests/what is the legitimate interests basis/ (accessed 6 Feb. 2021).

[39] *See supra* n. 27, at 4.

[40] *See* Palm, *supra* n. 33, at 205.

[41] Despite the fact that the European regulation set out the criterion of reasonable expectation of privacy, the weight placed on it differs from other legal systems, such as the US regime. 'In the United States, privacy is legally protected only where an actual reasonable expectation of privacy exists. Employers are free to eliminate actual employee privacy expectations through detailed, specific notices and deploy even highly intrusive monitoring technologies […]'. *See* Determann & Sprague, *supra* n. 34, at 1034. On the contrary, in Europe the elimination of employees' reasonable expectation of privacy is by no means a sufficient justification to adopt monitoring or surveillance practices of data subjects. Moreover, 'in Europe, employees have [but do not need, as a condition of legal protection] reasonable privacy expectations […]'. *Ibid.*, at 1036.

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, whether the applicant (employee) had a reasonable expectation of privacy.[42] To do so, the Court has focused on the policies and guidelines of the company, as well as on whether there has been a prior notice of internal oversight activities or monitoring practices.

However, the Court has not been consistent with the value it places on this criterion. Indeed, there are cases where it has not even been subject to the Court's scrutiny.[43] This situation can be explained by the fact that a reasonable privacy expectation is not necessarily a prerequisite for the protection of employees' personal data and privacy. Data subjects may have been notified of the collection and processing of their personal data, but this notification is not sufficient reason to justify these activities on legitimate interest grounds. In all cases, data controllers (including, of course, data processors) must ensure that they comply with other conditions or prerequisites.

This last idea is consistent with the spirit of the GDPR, as well as the recommendations issued by the WP29 with respect to Directive 95/46/EC abrogated by that Regulation. In this sense, employers must not only prove that they have a legitimate interest in personal data processing, but they also need to demonstrate that such processing is necessary and proportionate.[44] These two conditions imply, at least, that employers should be clear about the purposes of data processing, that this processing is helpful to achieve those purposes, and that there is no less intrusive way to reach them.

Accordingly, in order to rely on legitimate interest as a lawful basis, employers have to carry out the so-called 'proportionality test'. According to such test, employers are required to (1) identify the legitimate interest (or purpose of the processing); (2) demonstrate that the processing is necessary to achieve that purpose, and (3) balance the privacy and personal data rights of employees against their legitimate interests in order to show that 'such interests are [not] overridden by the interests or fundamental rights and freedoms of the data subject …'.[45] This balance, in the words of the Court of Justice of the European Union (CJEU), '… depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject's rights …'.[46] In any case, employers, as data controllers, must carry the burden of proof showing why the processing of employees' personal data is legitimate, necessary and proportional.[47]

All these conditions, including the analysis of the reasonable expectation of privacy as a parameter to balance the opposing interests and rights between employers and employees, make legitimate interest a rather difficult lawful basis to use. In general terms, it implies that, in many cases, employers need to carry out a legitimate interest assessment (LIA) to demonstrate that the measures adopted on these grounds are necessary and proportionate, and that employees' rights do not override the interests of the data controller.[48]

All these requirements can be considered a way to protect the weakest party in labour relationships, while simultaneously reversing the traditional tendency to favour employers' legitimate interests to justify the processing of workers' personal data. Moreover, 'the essence of the approach can be summed up by the phrase: 'prevention should be given much more weight than detection'.[49]

5 The case of Mexico

With regard to the fundamental right to personal data protection, Mexico has been strongly influenced by both the EU and the Council of Europe. Considering the former, this influence can be observed in Mexico's constitutional framework. Indeed, Articles 6 and 16 of the Mexican Constitution recognize the right to personal data protection as an autonomous and fundamental right, distinct from – but interrelated with – that of private life. In doing so, the Mexican Constitution emulates the Charter of Fundamental Rights of the EU.[50]

In addition, the current law on the subject of personal data protection in the private sector, which was enacted

Notes

[42] *See* ECHR, *Halford v. The United Kingdom*, paras 49 50, 25 June 1997; ECHR, *Ribalda and Others v. Spain*, para. 57, 9 Jan. 2018, and ECHR, Fourth Section, *Bărbulescu v. Romania*, para. 38, 12 Jan. 2016.

[43] *See* ECHR, Fourth Section, *Libert v. France*, 22 Feb. 2018, and, with regard to this case, *see* María S. Maqueo, *La privacidad y la protección de datos personales en el ámbito laboral. Caso Libert vs. Francia, sentencia del Tribunal Europeo de Derechos Humanos del 22 de febrero de 2018, in Estudios de Casos Líderes Europeos, Vol. XII. Cuestiones actuales del derecho a la protección de datos personales en Tribunal Europeo de Derechos Humanos* 110 (Luis Efrén Ríos Vega & Irene Spigno eds, Mexico, Tirant lo Blanch 2019).

[44] *See* Miguel Recio Gayo, *Nuevo dictamen del GT29 sobre tratamiento de datos en el trabajo: el interés legítimo*, 8 Diario La Ley, Sección Ciberderecho, Wolters Kluwer (29 July 2017).

[45] CJEU (Third Chamber), Joined Cases C 468/10 and C 469/10 (ASNEF and FECEMD), Judgment of 24 Nov. 2011, para. 37. About the three cumulative conditions for the lawfulness of the processing of personal data, *see also* CJEU (Second Chamber), Case C 13/16 (Rigas satiksme), Judgment of 4 May 2017, para. 28.

[46] *See* Joined Cases C 468/10 and C 469/10 (ASNEF and FECEMD), para. 40. About the condition of balancing the opposing rights and interests, *see also* Case C 13/16 (Rigas satiksme), para. 31.

[47] *See* Palm, *supra* n. 33, at 213.

[48] *See* ICO, *supra* n. 38.

[49] Eddie Keane, *The GDPR and Employee's Privacy*, 29 King's L. J. 354, 360 (2018).

[50] Charter of Fundamental Rights of the EU, Art. 8.

on 2010,[51] took the content of Directive 95/46/EC as one of its main references.[52] In contrast to this previous regulation, the Governmental Data Protection Law, which was enacted on 2017, took the GDPR as a reference.[53]

Given this significant difference between the public and private legal frameworks, Mexico currently presents some asymmetries in terms of level of protection, depending on the nature of data controllers. In general terms, these differences correspond to the gap between the updated regulations in Europe and the previous ones. Hence, in Mexico, the level of protection is higher in the regulation that applies to the public sector than that which applies to the private sector.

An important point to note is that, although the Governmental Data Protection Law in Mexico is inspired in the GDPR, it does not contemplate the provisions referred to in Article 88 with respect to employees' processing of personal data in the employment context. In fact, the lack of provisions with respect to this issue is reproduced in the Standards on personal data protection issued by the Ibero-American Data Protection Network (RIPD), of which Mexico is not only part, but was also an active contributor in the elaboration of its preliminary draft.[54] Although this Standard takes into consideration the EU's regulatory framework,[55] with the aim of generating homogenous criteria in the region, it only adopts those provisions that allow a wide margin of legislative discretion to the Member States of the RIPD.

This means that Mexico has chosen to stand aside from the route set by the EU in order to encourage the development of specific rules to guarantee employees' privacy and personal data protection, as well as to set out provisions that seek to limit and clarify the scope of employers' lawful basis for personal data processing. In other words, Mexico is not part of the sectoral approach wave that prevails on the subject of privacy and personal data protection at work.[56]

In this regard, the influence of the current EU model on data protection on Mexico's legal system is not just incomplete in content, but also partial in scope, considering that the GDPR is only reflected in the Governmental Data Protection Law.

These legal asymmetries have consequences for the level of protection of employees' personal data, depending on whether they are in the public sector or in the private sector. For instance, the Federal Law concerning the private sector lacks provisions that are considered relevant to adopt a preventive rather than a reactive approach, such as the principles of data protection by design and by default. Additionally, private sector legislation does not include in any case the requirement to conduct a DPIA, as does the legislation for the public sector,[57] which makes it more difficult for private sector employers to identify (and demonstrate) whether the processing of their employees' personal data is necessary, proportionate and well-balanced.

At another level, as a party to the so-called 'global standard',[58] Mexico is required to comply with the principles and safeguards contained in Convention 108 and its Additional Protocol, through the adoption of appropriate measures in its domestic legislation. In principle, the assessment of whether Mexican law complies with this binding international instrument, in both public and private sectors, is positive. Otherwise, Mexico would not have been able to become a party to the Convention.[59]

It should be noted that the ratification of Convention 108 has important consequences at a constitutional level. In accordance with the provisions of Article 1 of the Mexican Constitution, all international treaties on human rights to which Mexico is a party are in the

Notes

[51] Federal Law on Protection of Personal Data Held by Private Parties, published in the Federal Official Gazette on 5 July 2010, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (accessed 22 Jan. 2021).

[52] *See* the Initiative from the former deputy Gustavo Parra Noriega of the Congress of the Union, submitted on 4 Nov. 2008, which was considered for the enactment of the Federal Law for the Protection of Personal Data in Possession of Individuals (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*), https://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=ni0ZTJvgiDQ2W7Em2qvUpvlkcaiqRseqnrSxbEpcJNsXt0eT37871b1p3trHFBU8nHCwOec54m+ff3FfAnKCDg== (accessed 22 Jan. 2021).

[53] General Law for the Protection of Personal Data in Possession of Governmental Entities (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), published in the Federal Official Gazette on 27 Jan. 2017, http://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm (accessed 22 Jan. 2021). In this regard, it should be noted that the law of each federated state in Mexico has to be harmonized with it.

[54] *See* RIPD, Standards for Personal Data Protection for Ibero American States, adopted on 27 June 2017.

[55] 'Taking into consideration that the European Union has adopted a new regulatory framework on the matter, with the purpose of modernizing its provisions and guaranteeing greater soundness and consistency in the effective protection of the fundamental right to personal data protection in the European Union, and with the purpose of generating trust in society in general and, in turn, to facilitate the development of a digital economy, both in its internal market as in its global relations, this regulatory framework is positioned as a benchmark for the preparation of the national laws for data protection in Ibero America'. (RIPD, Standards for Personal Data Protection for Ibero American States, para. 8).

[56] A current and strong defence of this position from academia can be seen in Ajunwa, Crawford & Schultz, *supra* n. 1.

[57] *See* Arts 3 XVI, 74, 75, 77, 78 and 79, and Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, *Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales*, published in the Federal Official Gazette on 23 Jan. 2018.

[58] *See* Alessandro Mantelero, *The Future of Data Protection: Gold Standard v. Global Standard*, Computer Law & Security Review: The International Journal of Technology Law and Practice (Apr. 2021).

[59] *See* Eduardo Bertoni, *Convention 108 and the GDPR: Trends and perspectives in Latin America*, Computer Law & Security Review: The International Journal of Technology Law and Practice (Apr. 2021). Even more, Mexico could not yet sign the Convention 108+ due to its legislative asymmetries between public and private sectors.

highest tier of the normative pyramid. It implies that all competent authorities, especially those authorized to exercise judicial power, are compelled to apply the principle of conforming interpretation as well as to carry out a conventional control in order to ensure the effectiveness of human rights in the most favourable interpretation for the person.[60] In this regard, both constitutional law and international law determine together the expansion of human rights through the application of the principle *pro persona.*

The implementation of the constitutional principles adopted regarding Convention 108 and its Additional Protocol represents a path to bring Mexico's constitutional and legal system closer to the European model on privacy and personal data in the context of employment. Certainly, this Convention does not specifically envisage provisions relating to privacy and personal data protection in labour relations. However, the Council of Europe, as noted above, has addressed this topic in the form of recommendations.

Whilst these recommendations are not mandatory, it cannot be ignored that they are formulated in accordance with Convention 108 and other international instruments on this matter. To a certain extent, these recommendations reflect a specific approach to the understanding of employees' personal data protection rights and its balance with respect to the interests of employers, from the perspective of the Council of Europe. In this sense, Mexico cannot disregard their content. They constitute an important reference to be taken into consideration. Moreover, these *soft law* instruments could be useful as standards to determine the scope and limits of employers with respect to the processing of employees' personal information.

However, the lack of specific norms in Mexico that regulate privacy and personal data protection at the workplace[61] makes the Council of Europe's standards – such as the employers' duty to inform employees about any decision they make based on their personal information and that affects them – more of a parameter for resolution on a case-by-case basis than a guidance for legal norms. In that sense, there is a wide margin of uncertainty to determine the scope of the principles of personal data protection in employment relationships. The foregoing is of greater relevance if it is considered that Mexico also lacks specific regulations on health data processing. Examples of the recommendations that are not considered by the Mexican legal framework are the requirement to store sensitive data by personnel who are bound by medical secrecy and the requirement to separate this kind of data from other categories of personal data held by employers. The absence of such requirements entails that, in Mexico, there is not a full recognition of the assumption that employers should be subject to more specific and delimited rules than those provided for by the general legal framework on personal data protection.

6 Conclusions

The analysis of the Council of Europe's standards and the EU's regulations demonstrates that, in Europe, there is a growing tendency toward establishing specific rules aimed at strengthening employees' privacy and personal data protection rights.

It also shows that it is necessary to adopt a sectoral approach in this field, considering the complexity of balancing employees' rights vis-à-vis employers' interests. Moreover, there is a clear inclination to encourage a preventive approach on the collection and processing of employees' personal data.

However, these trends are not fully adopted by the Mexican legal system, albeit strongly influenced by the European model. This can be explained by the current legislative asymmetries on personal data between the public and the private sectors, as well as by the absence of specific rules to govern labour relationships in this field, beyond collective contracts and internal company guidelines or policies, or even by the general legal framework on personal data protection.

Notes

[60] *See* Human Rights Office of Mexico's Supreme Court of Justice, Extract of the Contradicción de Tesis 293/2011, Mexico. *See also* José Luis Caballero, *La interpretación conforme en el escenario jurídico mexicano. Algunas pautas para su aplicación a cinco años de la reforma constitucional de 2011* [*The Principle of Consistent Interpretation in the Mexican Legal Scene. Some Guidelines for Its Implementation to Five Years of the Constitutional Reform of 2011*], 3 Revista del Centro de Estudios Constitucionales 37 62; Juan Carlos Hitters, *Control de constitucionalidad y control de convencionalidad. Comparación. Criterios fijados por la Corte Interamericana de Derechos Humanos* [*Constitutional Control and Conventional Control. Comparison. Criteria Established by the Inter American Court of Human Rights*], 7 Estudios Constitucionales 109 128 (2009).

[61] *See* Carlos Reynoso, *Privacidad y protección de datos personales en las relaciones laborales, 95 Alegatos* 119 146 (Mexico 2017).

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

CONSEJO CONSULTIVO DEL INAI

Otorgan el presente

RECONOCIMIENTO

a la

Dra. María Solange Maqueo Ramírez

Por haber desempeñado con responsabilidad y honorabilidad su nombramiento como la primera **Consejera Presidente** del **Consejo Consultivo del INAI**, de conformidad con las disposiciones legales aplicables.

[redacted]

Dr. Francisco Javier Acuña Llamas
Comisionado Presidente
del INAI

Lic. Isaak Pacheco Izquierdo
Secretario Técnico del
Consejo Consultivo del INAI

Ciudad de México, 27/sep/2019

CVU: 438470

Solicitud: 157450

Maria Solange Maqueo Ramirez

Con fundamento en los artículos 24, fracciones IV y V y 39 del Reglamento del Sistema Nacional de Investigadores, la suscrita Maria Del Carmen De La Peza Casares, en mi carácter de Directora adjunta de Desarrollo Científico del Consejo Nacional de Ciencia y Tecnología y, por ello, de Secretaria Ejecutiva del Sistema Nacional de Investigadores (SNI), le comunico el resultado de la evaluación a la solicitud que presentó en respuesta a la Convocatoria 2019 para Ingreso o permanencia en el SNI. El Consejo de Aprobación del SNI con fundamento en el artículo 7 fracción VII del Reglamento del SNI, aceptó la recomendación de la Comisión Dictaminadora del Área V: Ciencias Sociales de otorgarle la distinción de Investigadora Nacional Nivel I.

Emito el presente comunicado en el que se citan los fundamentos legales y los motivos en los que sustentó la Comisión Dictaminadora del Área V: Ciencias Sociales su determinación. Lo anterior con las facultades con las que cuenta la suscrita en los artículos anteriormente señalados.

FUNDAMENTOS

PRIMERO. - Acorde al artículo 11 del Reglamento del Sistema Nacional de Investigadores, las comisiones dictaminadoras tendrán por objeto evaluar, mediante el análisis hecho por pares, la calidad académica, la trascendencia y el impacto del trabajo de investigación científica y tecnológica, la docencia y la formación de recursos humanos, que con las solicitudes de ingreso o permanencia les presente la dirección del SNI, y de acuerdo al artículo 39, mediante dictamen emitirán las recomendaciones correspondientes al Consejo de Aprobación por conducto del Secretario Ejecutivo.

[redacted]

Con base en los criterios de evaluación el pleno de la Comisión Dictaminadora del Área V: Ciencias Sociales, después de analizar todos y cada uno de los puntos contenidos en la solicitud con número 157450 presentada en respuesta a la Convocatoria para 2019 para Ingreso o permanencia en el SNI y el Currículum Vitae Único del CONACYT con número 438470, acordó en sesión plenaria recomendar al Consejo de Aprobación que se le otorgue la distinción de Investigadora Nacional Nivel I por los siguientes:

GOBIERNO DE MÉXICO

CONACYT
Consejo Nacional de Ciencia y Tecnología

MOTIVOS

Dictamen:

El pleno de la Comisión Dictaminadora del Área V: Ciencias Sociales revisó su solicitud de reingreso vigente y ha recomendado aprobar su permanencia en el Sistema como Investigador Nacional Nivel I, lo anterior en virtud de que durante el período sujeto de evaluación presentó adecuada producción de investigación científica publicada por editoriales especializadas con reconocimiento en el área, así como una activa participación en la formación de recursos humanos, de acuerdo con los criterios vigentes.

La solicitante ha presentado una producción muy adecuada para mantener el nivel I, pues le han sido validados 6 productos: tres artículos (dos en coautoría) en revista arbitradas e indexadas (dos de alto impacto), y tres capítulos de libros en editoriales de reconocido prestigio (todos de autoría). Lo anterior permite afirmar que tiene capacidad para realizar investigación original y de calidad sobre los temas de derecho a la información, tales como la privacidad y la protección de datos personales, y que participa en la formación de recursos humanos tanto al dirigir tesis como al impartir algunas materias.
Es recomendable publicar como autora única artículos en revistas arbitradas, indexadas y de alto impacto, capítulos de libros y libros en editoriales de reconocido prestigio académico para acreditar que su investigación es original, constante, de una calidad reconocida, y que cuenta con liderazgo académico, así como la dirección de tesis de posgrado (debidamente documentadas) para poder acceder a los siguientes niveles.

Aprovecho la ocasión para enviarle un cordial saludo.

Atentamente

[redacted]

Maria Del Carmen De La Peza Casares
Directora adjunta de Desarrollo Científico
Sistema Nacional de Investigadores
Secretaria Ejecutiva

[redacted]

41

Hace 25 años que la colección Cuadernos de Divulgación de la Cultura Democrática convoca de manera constante a especialistas de diversas disciplinas a publicar textos breves, sencillos y con rigor académico, para apoyar la construcción de ciudadanía y ofrecer abrevaderos teóricos tanto para la comunidad académica como para los actores políticos y el público en general.

Esta edición de aniversario incluye notas introductorias de las y los autores que ponen al día sus trabajos publicados originalmente y los explican con esta buena distancia. Así, estos cuadernos conmemorativos ofrecen una lectura en movimiento que permite una visión documentada del pasado, del presente y del futuro de nuestra democracia.

Consulta el catálogo
de publicaciones del INE

INE
Instituto Nacional Electoral

CUADERNOS DE DIVULGACIÓN
DE LA CULTURA DEMOCRÁTICA

INE

Democracia, privacidad y protección de datos personales
María Solange Maqueo Ramírez | Alessandra Barzizza Vignau

41

Democracia, privacidad y protección de datos personales

María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

25 AÑOS

CUADERNOS DE DIVULGACIÓN
DE LA CULTURA DEMOCRÁTICA

41

INE
Instituto Nacional Electoral

Democracia, privacidad y protección de datos personales

María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

CUADERNOS DE DIVULGACIÓN
DE LA CULTURA DEMOCRÁTICA

41

INE
Instituto Nacional Electoral

Democracia, privacidad y protección de datos personales
María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

Primera edición, 2019

ISBN de la colección: 978-607-9218-44-7
ISBN: 978-607-8697-72-4

Impreso en México/*Printed in Mexico*
Distribución gratuita. Prohibida su venta

Contenido

Presentación

En México, desde la última década del siglo pasado y las casi dos que han transcurrido del siglo XXI, se han registrado importantes avances en el ámbito público gracias a la creación de organos autónomos que impactan en diversos aspectos que involucran a la sociedad. En ocasiones, han sido avances que, dados de forma tan vertiginosa, no se han alcanzado a dimensionar en su totalidad y tampoco se han encontrado las convergencias entre unos y otros.

A partir de dichos avances, también han surgido importantes cuestionamientos como los que se formulan a continuación: ¿Cuáles son los límites que signan la pequeña franja de lo público y lo privado? ¿Es o debe ser público todo aquello que concierne a un funcionario público? ¿El estado de salud de un funcionario o legislador debe ser conocido por la ciudadanía o sus electores o, por el contrario, ser motivo de reserva por considerarse un dato sensible y merecedor de una salvaguarda especial? ¿Qué nivel de

protección debe brindarse a la privacidad de los ciudadanos? ¿Los expedientes clínicos o los padrones de los programas sociales deben ser públicos? ¿La revolución de la información y la comunicación conlleva un nuevo estadio de la democracia?

En los últimos años, la mayoría de estas preguntas, con formulaciones semejantes o idénticas, han estado presentes en la discusión nacional. No es un hecho fortuito, ya que la construcción de la democracia, el ejercicio pleno del derecho al sufragio libre y secreto, así como la alternancia en el poder, demandaron información, implicaron participación social y exigieron instituciones autónomas, de Estado, garantes de éstos y otros derechos. Es en un marco de tales características que se crea el Instituto Federal Electoral, actual INE, y el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

No obstante, para llegar a ello, hubo un arduo camino que transitar: desde que los medios de comunicación tradicionales funcionaban como plataformas de difusión de los partidos políticos, hasta la llegada del internet y las redes sociales que implicaron un cambio significativo en la forma de transmitir información y propaganda electoral, así como el surgimiento de nuevos retos para garantizar la privacidad y la protección de los datos personales.

Mediante este cuaderno de María Solange Maqueo Ramírez y Alessandra Barzizza Vignau, el Instituto Nacional Electoral invita a sus lectores a incursionar en la relación que existe entre la democracia, el acceso a la información, la privacidad y la protección de datos; vinculación ineludible que demanda un esfuerzo constante a las instituciones encargadas de su garantía.

Instituto Nacional Electoral

Introducción

La relación entre democracia y privacidad, en el sentido común de ambos conceptos, no resulta necesariamente evidente. De hecho, las dimensiones en que ambas se proyectan podrían parecer inicialmente contradictorias. Por una parte, la democracia suele definirse como "un conjunto de reglas (primarias o fundamentales) que establecen quién está autorizado para tomar las decisiones colectivas y bajo qué procedimientos".[1] En ese sentido, la democracia comprende la interacción de individuos que conviven en una sociedad organizada a través de instituciones y procedimientos para la toma de decisiones para la vida pública, que reflejen la voluntad popular sea de manera directa o a través de sus representantes. Se trata de una forma de gobierno del pueblo y para el pueblo, "del poder público en público",[2] en la

[1] Norberto Bobbio, *El futuro de la democracia,* México, Fondo de Cu tura Económica, 1986, p. 14.

[2] *Ibid.,* p. 65.

que impera la llamada "regla de mayoría" para legitimar la toma de decisiones políticas.

Por otra parte, la privacidad evoca un sentido de solitud, de ausencia de los otros, de lo que pertenece a uno mismo, relativo a los sentimientos, emociones, vida familiar, entre otros.[3] Se trata, pues, de una concepción que supone la generación de espacios vitales que escapan del escrutinio público, misma que se relaciona de manera estrecha con el advenimiento del derecho a la protección de los datos personales, entendido como instrumento de la privacidad y, al menos inicialmente en nuestro país, como un mecanismo para clasificar con el carácter de confidencial la información personal en manos del poder público.

En estos términos, mientras que la democracia se manifiesta en la esfera de lo público, la privacidad se proyecta, valga la redundancia, en la esfera de lo privado o de lo íntimo; donde la *res publica* y la *res privata* se constituyen en conceptos históricamente antagónicos, separados de manera casi natural en la tradición romano-germánica y cuya herencia ha permeado en el desarrollo de los sistemas jurídicos occidentales, incluido el nuestro.

---

[3] Beate Roess er, "New Ways of Thinking about Privacy", en John Dryzek *et al.* (eds.), *Oxford Handbook of Political Theory,* 2009 (versión en ínea).

No obstante, esta contradicción entre las distintas dimensiones de la democracia y la privacidad (incluida la vertiente relativa a la protección de datos personales) es tan sólo una mera apariencia que parte de una concepción reduccionista o convencional de ambos términos. Tanto el sentido de democracia como el propio sentido de la privacidad y la protección de datos personales, en términos actuales, han extendido sus alcances de tal manera que es factible afirmar la existencia de una estrecha relación entre ambas, donde la democracia importa para garantizar la privacidad y la protección de datos personales y, a su vez, la privacidad y la protección de datos personales se constituyen en una condición *sine qua non* de la democracia moderna.

El objetivo de esta obra consiste precisamente en explorar las distintas dimensiones en las que se proyectan cada una de estas categorías, a fin de destacar la relación de condicionamiento recíproco entre ellas que hace que sin una no puedan existir las otras, y a la inversa. Además, por supuesto, de advertir aquellos espacios de posible tensión que requieren de la adopción de mecanismos y criterios generales que permitan generar condiciones adecuadas para su propia coexistencia.

Ciertamente no se trata de abordar exhaustivamente cada una de las dimensiones de la democracia, la privacidad

y la protección de datos personales, sino sólo de aquellas en las que se hace evidente su interrelación. Tampoco se pretende establecer el sentido histórico y cronológico del proceso evolutivo de cada uno de estos conceptos, aunque incidentalmente hagamos alusión a ello. Nuestra intención es mucho más modesta. Consiste en advertir aquellos aspectos que, sea por oposición o por su imbricación, permiten demostrar la necesidad de generar equilibrios que armonicen su existencia mutua o convivencia natural.

LEY GENERAL
DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, COMENTADA

María Solange Maqueo
Coordinadora Editorial

LEY GENERAL
DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, COMENTADA

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

DIRECTORIO

COMITÉ EDITORIAL

Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía de Coyoacán, Ciudad de México, C.P. 04530.

Primera edición, noviembre de 2018.

Impreso en México, *Printed in Mexico.*
Ejemplar de distribución gratuita.

ÍNDICE

Revista de Derecho Vol. XXX - Nº 1 - JUNIO 2017 Páginas 77-96

Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario

*María Solange Maqueo Ramírez**
*Jimena Moreno González***
*Miguel Recio Gayo****

Resumen

La protección de datos personales, como un derecho fundamental autónomo del derecho a la vida privada, ha tenido un desarrollo asimétrico en los diferentes sistemas de derechos humanos. A pesar de la rápida evolución de la tecnología, la globalización de la economía y la digitalización de las relaciones humanas, aún no hay un nivel común de protección de datos en el mundo. La sentencia del Tribunal de Justicia de la Unión Europea, que declara la invalidez de la decisión de la Comisión Europea sobre el Acuerdo de Puerto Seguro UE-EE.UU., es solo un ejemplo de las diferentes aproximaciones en el tema. Este artículo pretende contribuir a generar algunos estándares internacionales en la protección de datos personales.

Datos personales – privacidad y vida privada – derechos humanos

Data Protection, Privacy and Private Life: The Challenging Search of a Needed Global Balance

Abstract

Data protection, as an autonomous fundamental right from the right of a private life, has had an asymmetric development in the different human rights systems. Despite of the rapid evolution of technology, the globalization of the economy and the digitalization of the human relationships, there is not a common level of data protection all around the world. The judgement of the Court of Justice of the European Union, that declares invalid the European Commission Decision on the EU-US Safe Harbor Agreement, is just only an example of the different approaches to the subject. This paper aims to contribute to generate some international standards for the protection of personal data.

Personal data – privacy and private life – human rights

* Doctora en Derecho, Universidad de Salamanca, España. Profesora Investigadora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Correo electrónico: maria.maqueo@cide.edu

** Maestra en Derecho, Instituto Tecnológico Autónomo de México (ITAM). Secretaria General del Centro de Investigación y Docencia Económicas (CIDE). Correo electrónico: jimena.moreno@cide.edu

*** Maestro en Protección de Datos, Transparencia y Acceso a la Información, Universidad CEU-San Pablo (España), y DEA (LLM) en Derecho de la Propiedad Intelectual, *George Washington University Law School* (EE.UU.). Correo electrónico: miguelrecio@miguelrecio.com

Artículo recibido el 8 de febrero de 2016 y aceptado para su publicación el 1 de marzo de 2017.

Introducción

En materia de protección de datos personales, 2015 puede ser recordado como el año en el que se produjo un momento álgido en el escenario internacional, particularmente entre la Unión Europea y los Estados Unidos de América, que puntualiza la necesidad de contar con estándares comunes de protección entre países. Lo anterior se desprende del fallo del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) que declaró inválido[1], después de 15 años de funcionamiento, el llamado Acuerdo de Puerto Seguro[2]. Es posible observar que mediante este Acuerdo la Comisión Europea avalaba la transferencia de datos personales entre empresas de la Unión Europea y de los Estados Unidos de América, por considerar que dicho Acuerdo cumplía con un nivel adecuado de protección de datos.

Este caso en particular pone de manifiesto las diferencias en los distintos niveles de protección de la persona respecto del tratamiento de sus datos personales que, además de representar un trato desigual para los individuos, conlleva, a su vez, obstáculos importantes para el flujo de información, a veces tan necesario para el intercambio comercial y la cooperación internacional. La realidad actual es la de diferencias sustantivas, ya sea por la inexistencia de normatividad en algunos países o por las aproximaciones divergentes que se han seguido y que, en la práctica, pueden tener efectos negativos al crear notables desencuentros y, en buena medida, obstaculizar una protección efectiva de las personas.

En ese sentido, este trabajo pretende abordar el problema del desarrollo asimétrico, tanto normativo como jurisprudencial, del derecho a la protección de datos personales desde una perspectiva internacional, en el entendido de que ello, a su vez, se proyecta en una importante diferenciación entre países y regiones de todo el mundo. Esto nos lleva a cuestionarnos en qué consisten dichas asimetrías y cuáles son los criterios que permitirían la adopción de estándares comunes que sean aceptables entre países y regiones, si es que no es posible acordar un instrumento supranacional común. Ello, a su vez, implica la necesidad de considerar las razones por las cuales resultaría conveniente dicha estandarización. Es importante decir que las respuestas a estas interrogantes parten de la hipótesis de que en el ámbito internacional y, concretamente, en los sistemas internacionales de derechos humanos, existen disparidades en el reconocimiento del derecho a la protección de datos personales que poco han abonado a resolver esta situación, lo que genera desconfianza debido a la ausencia de niveles comunes de protección de la persona en su derecho a la protección de datos personales.

---

[1] Sentencia del Tribunal de Justicia (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, Caso Schrems.

[2] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Publicada en el Diario Oficial de la Unión Europea L 215, de 25 de agosto de 2000.

Es por ello que la búsqueda de un equilibrio global conlleva la necesidad de establecer una hoja de ruta que tome como referencia las principales aportaciones que, desde una perspectiva internacional, se han desarrollado en torno a la protección de datos personales y en su relación con el derecho a la vida privada, con el objeto de establecer aquellos parámetros que sirvan de guía para dar un próximo paso en el fortalecimiento de la protección de la persona respecto del tratamiento de su información y, con ello, evitar injerencias indebidas, sea del sector privado o, más grave aún, del sector público, que incidan en una vulneración de su privacidad.

Desde un punto de vista metodológico es admisible observar que adoptamos una aproximación diacrónica que nos permite seguir el desarrollo evolutivo del derecho a la protección de datos personales en su relación con el derecho a la vida privada, en los distintos sistemas internacionales de derechos humanos (incluido el ámbito específico de la Unión Europea). Para tales efectos se parte de la recopilación, análisis y sistematización de fuentes documentales a partir de los instrumentos y criterios internacionales más relevantes en la materia. En ese sentido, nuestro enfoque pretende, más que hacer una construcción teórica de los derechos en juego, identificar aquellos aspectos que podrían ser necesarios para generar estándares comunes con un alcance global.

I. Vida privada y protección de datos personales

Definir el derecho a la vida privada no es una tarea fácil[3]. De hecho, existe pleno consenso entre los tribunales internacionales de derechos humanos en el sentido de que se trata de un concepto amplio, no susceptible de definiciones exhaustivas, y cuyo contenido es más extenso que el del derecho a la privacidad[4]. De tal forma que se reconoce que el derecho a la vida privada y la privacidad no son sinónimos[5], a pesar de que el primero tiene un alcance mucho mayor que, en consecuencia, comprende al segundo. Si

[3] Cfr. Informe del Relator Especial de la ONU acerca de la promoción y protección del derecho a la libertad de opinión y expresión, de 17 de abril de 2013, numeral 21.

[4] CIDH, Caso Fernández Ortega y Otros vs. México, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 30 de agosto de 2010, párr. 129; CIDH, Caso Rosendo Cantú y Otra vs. México, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 31 de agosto de 2010, párr. 119; CIDH, Caso Artavia Murillo y Otros (Fecundación in vitro) vs. Costa Rica, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas, de 28 de noviembre de 2012, párr. 143); TEDH, Caso Amann v. Switzerland, Sentencia de 16 de febrero de 2000, párr. 65, entre otros.

[5] Cfr. Piñar Mañas, J. L., "¿Existe privacidad?", en *Protección de Datos Personales, Compendio de lecturas y legislación*, Tiro Corto Editores, México, 2010; Miller, A. R., *The Assault on Privacy: Computers, Data Banks, and Dossiers*, University of Michigan Press, 1971; Roagna, I., "Protecting the right to respect for private and family life under the European Convention on Human Rights", en *Council of Europe Human Rights Handbook*, Strasbourg, 2012, p. 12; y Kikelly, Ú., "The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights", *Human Rights Handbook*, núm. 1, Strasbourg, 2003.

bien la delimitación entre ambos excede los alcances de este trabajo[6], nos centraremos exclusivamente en el análisis del derecho de la vida privada (en el entendido de que la privacidad es parte de la misma), en relación con el derecho a la protección de los datos personales[7].

1. *Reconocimiento en convenios y otros instrumentos internacionales*

El derecho a la vida privada ha sido consagrado como un derecho humano tanto en el Sistema Universal de Derechos Humanos como en los sistemas regionales (específicamente en los sistemas europeo e interamericano). Por lo que hace al Sistema Universal, esto es, con un alcance global, la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17), la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares de 1990 (artículo 14) y la Convención sobre los Derechos del Niño de 1989 (artículo 16), lo contemplan prácticamente en los mismos términos. Asimismo, el derecho a la vida privada goza de un reconocimiento expreso tanto en el ámbito interamericano, mediante el artículo 11.2 de la Convención Americana sobre Derechos Humanos (Pacto de San José), como en el ámbito europeo, por medio del Convenio para la Protección de los Derechos y Libertades Fundamentales (también llamado Convención Europea de Derechos Humanos) en su artículo 8.

Cuestión distinta ocurre por lo que hace al derecho a la protección de datos personales, toda vez que estos instrumentos internacionales carecen de una referencia expresa al mismo. De hecho, en 1980, la Asamblea Parlamentaria del Consejo de Europa recomendó al Comité de Ministros, que a la vista de la aproximación que estaban adoptando varios Estados miembros de la actual Unión Europea en cuanto a legislar en materia de protección de datos personales, estudiase la posibilidad de incluir en la Convención Europea de Derechos Humanos una referencia al mismo, idea que fue rechazada por "no ser el momento adecuado" para ello, debido a la falta de experiencia en la materia y los avances hacia la aprobación del llamado Convenio 108 que, por entonces, era un borrador muy avanzado, en cuanto al derecho a la protección de datos personales.

Otros convenios e instrumentos internacionales, fundamentalmente regionales y con un alcance limitado por estar dirigidos solo a ciertos países, contemplan expresamente el derecho a la protección de datos personales y establecen en su texto una relación estrecha con el derecho a la privacidad. Al respecto es posible mencionar las Directrices de la

[6] En la práctica, hay menciones a la privacidad y a la vida privada como un mismo derecho humano. Sobre el particular véase la Resolución 68/167, 21 de enero de 2014, el derecho a la privacidad en la era digital, aprobada por la Asamblea General de la Organización de Naciones Unidas (ONU) el 18 de diciembre de 2013, misma que se refiere en español al "derecho humano a la privacidad" pero utiliza también el término vida privada, consagrado en los artículos 12 de la Convención Universal de Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

[7] A causa de que la privacidad puede concebirse como parte del derecho a la vida privada, aquella también se relaciona con el derecho a la protección de datos personales.

Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre protección de la privacidad y flujos transfronterizos de datos, adoptadas inicialmente en 1980 y actualizadas en el 2013. De acuerdo con las mismas, estas "suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal". Su objetivo, si bien recoge los principios que informan la protección de datos personales, consiste en adoptar estándares mínimos para garantizar la privacidad, ello a pesar de que carece de un carácter vinculante. De tal forma que en este documento la protección de datos personales adquiere un carácter instrumental para dotar de efectividad el derecho a la privacidad.

Asimismo, el Convenio (108) del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto del tratamiento automatizado de datos de carácter personal, establece en su artículo 1º que tiene por objeto proteger "a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, respecto del tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")". Se trata de un instrumento vinculante, abierto incluso a la firma o ratificación por Estados que no son parte del Consejo de Europa, siempre que se cumplan con los requisitos que el propio Convenio 108 establece.

Ahora bien, será en el marco de la Unión Europea donde el derecho a la protección de los datos personales encuentra su máximo desarrollo normativo. Acerca del particular resulta interesante mencionar la Directiva 95/46/CE, misma que establece en su Considerando 10 que "las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario". Si bien el 27 de abril de 2016 se adoptó el Reglamento General de Protección de Datos que substituye a la Directiva 95/46/CE, el mismo sigue en la misma línea, con una aplicación directa para evitar divergencias entre los Estados miembros de la Unión Europea.

En un paso histórico para la protección de los datos personales en su calidad de derecho al más alto nivel normativo, se recoge expresamente tanto en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) como en la Carta de los Derechos Fundamentales de la Unión Europea. Esta última lo contempla, en su artículo 8, de manera separada del derecho a la vida privada (previsto en el artículo 7 de la propia Carta). Es así que se establece de manera específica su autonomía, sin perjuicio de la relación que se establezca entre ambos derechos[8].

[8] Otras disposiciones relativas a la protección de datos personales en el ámbito de la Unión Europea pueden encontrarse respecto del sector de las comunicaciones electrónicas, de las propias instituciones y organismos de la Unión Europea o en el ámbito policial y judicial, Al respecto véanse, respectivamente, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por el que se

Es esencial decir que el artículo 8 de la citada Carta de los Derechos Fundamentales establece que el tratamiento de los datos personales tiene que realizarse conforme a unos criterios o principios que lo legitimen y que deberá existir una autoridad de control independiente que se encargue de supervisar el respeto de las normas acerca de la materia.

Así, de conformidad con lo anterior, puede decirse que el derecho a la protección de datos personales se ha desarrollado fundamentalmente en el ámbito europeo. Se consagra por primera vez en el Convenio 108 del Consejo de Europa, seguido por la Directiva 95/46/CE de la Unión Europea, como una proyección o faceta del derecho a la vida privada[9]. Sin embargo, desde entonces hasta la fecha, especialmente tras la adopción de la Carta de Derechos Fundamentales de la Unión Europea, este derecho adquiere vida propia, al margen del reconocimiento de que el tratamiento de datos personales que no cumpla con las condiciones de legitimidad aplicables, puede llegar a suponer una injerencia en la vida privada o la privacidad.

Este modelo europeo, también ampliamente desarrollado en el derecho interno de los países que lo conforman, ha sido una importante fuente de inspiración para diversos países del Continente Americano que, como en el caso de México, reconocen la protección de datos personales como un derecho humano diferenciado, aunque relacionado con el derecho a la vida privada. De ahí que, como veremos, sea necesario adoptar estándares comunes que excedan el ámbito nacional o, incluso, regional.

2. *Desarrollo de la jurisprudencia internacional*

El desarrollo jurisprudencial en los distintos sistemas internacionales de derechos humanos ha sido mucho más rico respecto del derecho a la vida privada que relativas al derecho a la protección de datos personales, no solo por su reconocimiento explícito en los instrumentos internacionales que les dan origen, sino además por su propia antigüedad.

De hecho, es valioso observar que hasta el momento la Corte Interamericana de Derechos Humanos (en adelante, CIDH) no se ha pronunciado de manera específica en ningún caso respecto del derecho a la protección de datos personales, a pesar de que un gran número de países sujetos a su jurisdicción lo contemplan dentro de su propio

modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (CE) no. 2006/2004 sobre la cooperación en materia de protección de los consumidores; el Reglamento (CE) no. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, y; la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008.

[9] Cfr. De Hert, P. y Gutwirth, S., "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", en Gutwirth, Serge *et al.* (eds.), *Reinventing Data Protection?*, Springer, 2009, Cap. 1, Sección 1.1.2.

derecho interno con el carácter de derecho humano. De tal forma que, como veremos, el desarrollo internacional de la protección de datos personales se produce a nivel regional y, fundamentalmente en Europa, a partir de la propia construcción expansiva del derecho a la vida privada hasta el reconocimiento de su propia autonomía.

2.1. Criterios de la Corte Interamericana de Derechos Humanos

En su sentido más tradicional, la CIDH ha puesto de manifiesto que el derecho a la vida privada implica una obligación negativa para el Estado. En un primer momento, ha establecido su vínculo con la inviolabilidad del domicilio. De tal forma que la intromisión en el domicilio familiar de las personas, sin el consentimiento de quienes lo habitan y sin autorización legal para ello, así como su propia destrucción, se consideran una violación grave, injustificada y abusiva en términos del artículo 11.2 de la Convención Americana de Derechos Humanos[10].

Asimismo, la Corte considera que "[…] el ámbito de la privacidad se caracteriza por quedar exento e inmune a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública". Además, establece que las injerencias en la vida privada de las personas deben: (1) estar previstas en ley, (2) perseguir un fin legítimo, y (3) ser idóneas, necesarias y proporcionales. En otras palabras, los requisitos que han de cumplir los límites al derecho a la vida privada comprenden tanto el principio de proporcionalidad en términos de Alexy (compuesto por sus tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto)[11], como el principio de legalidad. En caso de no cumplir con estos requisitos, las injerencias se consideran contrarias a los términos de la propia Convención[12]. Al respecto, este Tribunal manifiesta que, a pesar de no señalarse explícitamente en el texto de la Convención, la vida privada extiende sus alcances más allá del domicilio y la correspondencia, incorporando otros aspectos como la intervención, monitoreo, grabación y divulgación de conversaciones por vía telefónica[13]. En ese sentido se reconoce que "[l]a fluidez informativa que existe hoy coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente". De ahí que el Estado deba "asumir un compromiso aún mayor, con el fin de adecuar a los tiempos actuales las formas tradicionales de protección del derecho a la vida privada"[14].

---

[10] CIDH, Caso Masacres de Ituango vs. Colombia, Sentencia de Fondo, de 1 de julio de 2006, párr. 197; CIDH, Caso Escué Zapata vs. Colombia, Sentencia de Fondo (Reparaciones y Costas), de 4 de julio de 2007, párrs. 94 y 96. Más adelante, la CIDH retoma este criterio en el Caso Familia Barrios vs. Venezuela, Sentencia de Fondo (Reparaciones y Costas), de 24 de noviembre de 2011, párr. 140.

[11] Cfr. Alexy, Robert, "Constitutional Rights and Proportionality", *Revus, Journal for constitutional theory and philosophy of law*, núm. 22, 2014, p. 52.

[12] CIDH. Caso Tristán Donoso vs. Panamá, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 27 de enero de 2009, párrs. 55 y 76.

[13] *Idem.* y CIDH, Caso Escher y Otros vs. Brasil, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 6 de julio de 2009, párr. 114.

[14] *Ibídem,,* párr. 115.

Así, la Corte de manera consistente con sus resoluciones previas, manifiesta que "el concepto de vida privada es un término amplio no susceptible de definiciones exhaustivas". Sin embargo, este concepto comprende, entre otras cosas, "la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos". De tal forma que las violaciones sexuales vulneran la vida privada de las personas, toda vez que impiden "el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas"[15].

En una concepción expansiva del derecho a la vida privada y su estrecha relación con otros derechos humanos reconocidos por la Convención Americana, la Corte señala que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás". Asimismo, retoma los requisitos necesarios para considerar que una injerencia en la vida privada de las personas no se considere abusiva o arbitraria, señalando que tanto la idoneidad, la necesidad, como la proporcionalidad de las medidas adoptadas implican que sean "necesarias en una sociedad democrática"[16].

Finalmente, en una resolución histórica relativa a la prohibición general de la fecundación *in vitro* concebida como una injerencia en la vida privada de las personas, la CIDH adopta de manera expresa criterios provenientes del Tribunal Europeo de Derechos Humanos, en el sentido de que el ámbito de protección del derecho a la vida privada va más allá del derecho a la privacidad. De manera textual, la Corte ahonda en el concepto de vida privada, mediante la adopción de criterios cuyo desarrollo corresponde al ámbito europeo:

> La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo por ejemplo la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad. [...][17]

[15] CIDH, Caso Fernández Ortega vs. México, Sentencia de Fondo (Excepción Preliminar, Fondo, Reparaciones y Costas), de 30 de agosto de 2010, párr. 129 y Caso Rosendo Cantú y Otra vs. México, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 31 de agosto de 2010, párr. 119.

[16] CIDH. Caso Atala Riffo y Niñas vs. Chile, Sentencia de Fondo (Reparaciones y Costas), de 24 de febrero de 2012, párr. 162.

[17] CIDH, Caso Artavia Murillo y Otros ("Fecundación *in vitro*") vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012, párr. 143.

Es posible decir que este fallo de la CIDH, mismo que retoma los criterios emitidos por su homóloga europea en materia del derecho a la vida privada, permite anticipar el desarrollo armónico de este derecho en ambos sistemas internacionales de derechos humanos. No obstante, su distanciamiento, por lo menos hasta la actualidad, se produce precisamente con la incorporación del derecho a la protección de datos personales y su relación con otros derechos humanos de frontera (como la libertad de expresión).

2.2. Criterios de la Corte Europea de Derechos Humanos

De manera similar a lo ocurrido en la CIDH, la Corte Europea de Derechos Humanos (o TEDH), en sus primeras resoluciones respecto del artículo 8 del Convenio Europeo de Derechos Humanos, se ocupa de posibles violaciones que suponen una interferencia del Estado en la vida privada y familiar de las personas. Especialmente el TEDH se ocupa, en un primer momento, de la vigilancia secreta de los Estados, por medio de la posible o efectiva interceptación de comunicaciones, por consideraciones de orden criminal o de seguridad nacional[18]. Basado en lo anterior, este Tribunal comienza a interpretar los requerimientos para considerar que las interferencias del Estado que presentan un riesgo para la vida privada y familiar de las personas cumplen con el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales.

Así, el TEDH si bien admite que los Estados firmantes de la Convención tienen cierta discreción respecto de los términos en los que operan sus sistemas de vigilancia, no se trata de una discreción absoluta[19]. Para que la interferencia se apegue a los términos del citado artículo 8 es necesario que: (1) persiga un objetivo legítimo; (2) sea conforme con la ley, y (3) sea necesaria en una sociedad democrática. Todo ello implica la adopción de garantías adecuadas y efectivas contra los abusos que pudiera ocasionar la autoridad[20].

Por lo que hace a la persecución de un fin legítimo, el Tribunal ha analizado varios casos en los que se considera que se cumple este requisito, por ejemplo, en la adopción de medidas para garantizar la seguridad nacional y la prevención del desorden o el delito e, incluso, posteriormente, en relación con la transferencia de datos de salud de una autoridad a otra para la decisión de las autoridades respecto de la asignación de recursos públicos[21], entre otros. Por su parte, el requerimiento de que la interferencia esté de acuerdo con la ley, supone, de acuerdo con el TEDH, que además de encontrar sustento en la legislación doméstica, es necesario considerar la calidad de la ley y su *foreseeability*, esto es, que contribuya a fortalecer el estado de derecho. Así, la Corte establece que el requerimiento de que la medida sea "de acuerdo con la ley" supone que existe una previsión legal previa y que la ley sea accesible y suficientemente clara respecto de las

[18] TEDH, *Klass and others v. Germany*, Sentencia de 6 de septiembre de 1978, párr. 35 y ss.

[19] *Ibídem.*

[20] THDE, *Malone v. The United Kingdom,* Sentencia de 2 de agosto de 1984, párr. 63 y ss. y TEDH, *Kruslin v. France*, Sentencia de 24 de abril de 1990, párr. 27 y ss., entre otros.

[21] TEDH, *M. S. v. Sweden*, Sentencia de 2 de agosto de 1997, párr. 32 y ss; y TEDH, *Leander v. Sweden*, Sentencia de 26 de marzo de 1987, párr. 48 y ss.

circunstancias y condiciones en las que las autoridades están facultades para establecer estas interferencias, estableciendo a su vez medidas adecuadas de protección legal[22]. Finalmente, el requerimiento de que las interferencias sean necesarias en una sociedad democrática implica la identificación, dentro del ámbito más amplio del objetivo legítimo perseguido, de la necesidad social específica que deba abordarse, la proporcionalidad de la medida para alcanzar dicho objetivo legítimo y que existan razones relevantes y suficientes que la justifiquen en razón de otras posibles medidas[23].

Un paso decisivo para que el Tribunal Europeo pudiera adentrarse a campos propios del derecho a la protección de datos personales, inicialmente referido al acceso a la propia información personal que consta en archivos públicos, fue el reconocimiento de que si bien el artículo 8 del Convenio Europeo tiene esencialmente por objeto proteger a los individuos en contra de interferencias arbitrarias por las autoridades públicas, también podría comprender obligaciones positivas del Estado inherentes al respeto efectivo de la vida privada y familiar, de tal forma que incluso la negativa para conceder acceso a la información personal del individuo debe analizarse, "por una autoridad independiente" bajo la óptica de los requerimientos que establece el artículo 8 antes indicados, con el fin de garantizar la aplicación del principio de proporcionalidad[24]. Al respecto, la Corte reconoce que el artículo 8 protege, entre otros intereses, el derecho al desarrollo personal, lo que incluye el derecho de recibir información relativa a su identidad personal, necesaria para conocer sus orígenes y entender su infancia y posterior desarrollo[25].

Es esencial decir que las primeras referencias explícitas a la protección de los datos personales se presentan en el contexto de información sensible que contiene datos de salud[26]. En un primer momento, la Corte Europea se cuestiona si las medidas que se impugnan –consistentes en obtener y mantener por un periodo la confidencialidad de información médica de una pareja infectada por VIH, misma que consta en el expediente de un juicio seguido en contra de uno de ellos por delitos de carácter sexual– fueron necesarias en una sociedad democrática. Al respecto, la Corte señala que la confidencialidad de los datos de salud es un principio vital en los sistemas legales de los Estados parte del Convenio. Es crucial, señala, no solo en el sentido de respeto a la privacidad de los pacientes, sino también para preservar su confianza en la profesión médica y en los servicios de salud en general. Además, estas consideraciones cobran especial relevancia cuando se trata de la confidencialidad de información relativa a una persona infectada de

[22] *Ibídem.*

[23] Grupo de Trabajo del Artículo 29 sobre la Protección de Datos, Dictamen 1/2014 sobre la aplicación de los conceptos de necesidad, proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas, adoptado el 27 de febrero de 2014, p. 6 y ss.

[24] TEDH, *Gaskin v. The United Kingdom*, Sentencia de 7 de julio de 1989, párr. 49.

[25] TEDH, *Odièvre v. France*, Sentencia de 13 de febrero de 2003, párr. 25 y ss. y *X and Y v. Netherlands*, Sentencia de 26 de marzo de 1985, párr. 28 y ss.

[26] TEDH, *Z. v. Finland,* Sentencia del 25 de febrero de 1997, párr. 72 y ss.; TEDH, *M. S. v. Sweden*, Sentencia de 2 de agosto de 1997, párr. 32 y ss.

VIH, toda vez que la revelación de esta información puede afectar de manera dramática su vida privada y familiar, laboral y social, exponiéndola al oprobio y el ostracismo[27].

Con posterioridad, la Corte reconoce explícitamente que la transferencia de datos de salud de una autoridad a otra, sin el consentimiento del paciente y que, a su vez, ha servido para diferentes propósitos, constituye una interferencia en el derecho al respeto de la vida privada y familiar del paciente. En ese sentido, la Corte establece que las medidas adoptadas para la comunicación de la información entre autoridades se deben analizar a la luz de los requerimientos previamente establecidos[28].

De igual forma, bajo la idea de que el término de "vida privada" no debe ser interpretado de manera restrictiva, la Corte incluye dentro del ámbito de protección del multicitado artículo 8, el almacenamiento de datos relativos a una persona, con independencia de si los mismos son o no sensibles, lo que, de acuerdo con el propio Tribunal, es consistente con el Convenio 108 del Consejo de Europa[29]. Asimismo, estas consideraciones se hacen extensivas al uso de la información, lo que incluye su divulgación por parte de las autoridades, y a la carencia de medios para refutar el contenido de dicha información[30].

En sucesivas ocasiones, la Corte reitera las obligaciones positivas del Estado para proteger la vida privada de las personas que se derivan del párrafo 1 del artículo 8 del Convenio Europeo, lo que la lleva a considerar la posibilidad de que, incluso, la divulgación de información por parte de personas distintas a las autoridades, incluida la prensa y los medios de comunicación masiva, sea contraria a los términos de la Convención[31]. También dentro de este rubro, consistente en las obligaciones positivas que conlleva el citado artículo 8 del Convenio, el Tribunal reitera el deber de proporcionar a las personas "un procedimiento efectivo y accesible" para obtener el acceso a "información relevante y apropiada" de los archivos personales mantenidos por las autoridades[32].

De esta forma, como se puede observar, el TEDH va perfilando la inclusión del derecho a la protección de datos personales en relación con el derecho a la vida privada. Incluso, ya establece en sus decisiones esta conexión al indicar textualmente que "[l] a protección de datos de carácter personal juega un rol fundamental en el ejercicio del derecho al respeto de la vida privada y familiar consagrado en el artículo 8 de la Convención". Acerca del particular se señala que el mero hecho de que la legislación interna facilite la oportunidad de reclamar indemnizaciones por daños y perjuicios por la revelación ilegal de los datos personales, no es razón suficiente para proteger la vida

---

[27] TEDH, *Z. v. Finland, cit.,* párrs. 111 y 112. Sobre el particular también véase TEDH, *I. v. Finland,* Sentencia de 17 de octubre de 2008, párr. 35.

[28] TEDH, *M.S. v. Sweden*, *cit.*, párr. 32 y ss.

[29] TEDH, *Amann v. Switzerland*, Sentencia de 16 de febrero de 2000, párr. 65.

[30] TEDH, *Rotaru v. Romania*, Sentencia del 4 de mayo de 2000, párr. 46 y TEDH, *Peck v. United Kingdom*, Sentencia de 28 de enero de 2003, párr. 57 y ss.

[31] TEDH, *Von Hannover v. Germany* (No. 2), Sentencia de 7 de febrero de 2012, párr. 74 y ss.; y *Sciacca v. Italy*, Sentencia de 11 de enero de 2005, párr. 27 y ss.

[32] TEDH, *Haralambie v. Romania*, Sentencia de 27 de octubre de 2009, párr. 86.

privada, es necesario que los Estados firmantes de la Convención provean de una protección "real y efectiva" que excluya cualquier posibilidad de acceso no autorizado[33].

Lo anterior es consistente con la idea central de que el derecho a la vida privada "es un término amplio no susceptible de una definición exhaustiva, que comprende la integridad física y psicológica de una persona y puede comprender múltiples aspectos de la identidad de la persona, [...]"[34]. De ahí que desde esta perspectiva el alcance del término "dato personal" sea esencialmente amplio. De hecho, el Tribunal Europeo se ha referido a muy diversos ámbitos entre los que se incluye información relativa a una persona identificada o identificable que van desde el propio nombre, la fecha de nacimiento y el historial médico, hasta las huellas dactilares, muestras de células y elaboración de perfiles de ADN, entre otros[35].

En virtud de los precedentes antes mencionados, es posible observar que existe cierto consenso entre la Corte Interamericana de Derechos Humanos y el Tribunal Europeo respecto del amplísimo alcance del derecho a la vida privada, fundamentalmente en el sentido de que el derecho a vida privada comprende múltiples aspectos de la identidad de las personas y de cómo deciden relacionarse con otros seres humanos. Sin embargo, podemos observar que el desarrollo del contenido y alcance de este derecho ha sido asimétrico, específicamente por lo que se refiere al reconocimiento explícito del derecho a la protección de datos personales. Mientras que la Corte Interamericana hasta el momento no se ha pronunciado al respecto, el Tribunal Europeo ha dado pasos significativos que permiten profundizar acerca de la noción misma del derecho a la protección de datos personales en su relación con el derecho a la vida privada. En concreto, el Tribunal de Estrasburgo reconoce que bajo el concepto de vida privada puede quedar amparada "toda información relativa a una persona física identificada o identificable", esto es, con independencia de si se trata o no de información sensible que afecta la esfera más íntima de las personas, lo que a su vez es consistente con la amplia definición de "dato personal". De igual forma, en su jurisprudencia introduce la búsqueda de criterios interpretativos conformes con la normatividad específica en materia de protección de datos personales, como se puede observar en sus referencias al Convenio 108 del Consejo de Europa.

No obstante, es admisible advertir que la construcción del derecho a la protección de datos personales desde la perspectiva del Tribunal Europeo de Derechos Humanos aún se encuentra bajo la égida del derecho a la vida privada. Su carácter autónomo, en el ámbito internacional de los derechos humanos, se presenta con la Carta de Derechos Fundamentales y su interpretación jurisprudencial por parte del Tribunal de Justicia de la Unión Europea.

---

[33] TEDH, *B.B. v. France*, Sentencia de 17 de diciembre de 2006, párr. 61.

[34] TEDH, *Axel Springer AG v. Germany*, Sentencia de 7 de febrero de 2012, párr. 83.

[35] TEDH, *S. and Marper v. United Kingdom*, Sentencia de 4 de diciembre de 2008, párr. 71; *K.U. v. Finland*, Sentencia de 2 de diciembre de 2008, párr. 41 y ss.; *Khelili v. France,* 18 de octubre de 2011, párr. 56; y, *M.K. v. France*, Sentencia de 18 de abril de 2013, párr. 29.

2.3. Criterios del Tribunal de Justicia de la Unión Europea

El Tribunal de Justicia de la Unión Europea toma como base de interpretación no solo la Carta de Derechos Fundamentales de la Unión Europea, misma que ya reconoce de manera explícita y autónoma el derecho a la protección de datos personales, sino también la Directiva 95/46/CE antes citada, entre otros documentos normativos que regulan la protección de datos personales en la Unión Europea.

De esta forma, este Tribunal se adentra a cuestiones mucho más específicas para delinear los contornos del derecho a la protección de datos personales, que terminan por acentuar el carácter autónomo de este derecho frente al derecho a la vida privada, sin dejar de reconocer su estrecha vinculación. Entre otros asuntos, este Tribunal se ha ocupado de establecer criterios interpretativos en relación con la transferencia de datos a terceros países (no miembros de la Unión Europea), la conservación de datos relativos a comunicaciones electrónicas, la gestión de motores de búsqueda concebida como tratamiento de datos personales y los sistemas de videovigilancia operados por particulares[36].

En un caso relevante para la interpretación de la Carta de Derechos Fundamentales en consonancia con los criterios emitidos por el TEDH, el TJUE establece que "el respeto a la vida privada en lo que respecta al tratamiento de los datos personales" se aplica a toda información sobre una persona física identificada e identificable y, además, que "las limitaciones al derecho a la protección de datos personales de carácter personal que pueden establecerse legítimamente corresponden a las toleradas en el contexto del artículo 8 del CEDH". De tal forma que este órgano jurisdiccional, al referirse sobre quién puede ser titular del derecho a la protección de datos personales, reconoce que solo las personas físicas cuentan con esta facultad, pues "las personas jurídicas solo pueden acogerse a la protección de los artículos 7 y 8 de la Carta frente a dicha identificación en la medida en que en la razón social de la persona jurídica se identifique a una o varias personas físicas"[37]. Así, esta característica presenta una importante diferencia de alcance, en el contexto europeo, del derecho a la vida privada del Convenio y el derecho a la protección de datos personales reconocido en la Carta, toda vez que el ámbito de protección del primero alcanza efectivamente a las personas morales.

No obstante, el propio Tribunal ha reconocido que tratándose de "la protección de los derechos y las libertades fundamentales de las personas físicas, en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales", no es posible separar los casos de tratamiento de datos personales en dos categorías, a saber, una categoría en la que ese tratamiento sería examinado únicamente sobre la base del artículo 8 del Convenio Europeo y su interpretación jurisprudencial y otra categoría

[36] Al respecto véanse las Sentencias del Tribunal de Justicia, de 8 de abril de 2014, en el asunto C-293, Caso Digital Rights Ireland y Seitlinger y otros, apartado 34 y ss.; de 13 de mayo de 2014, en el asunto C-131/12, Caso Google Spain y Google, apartado 36 y ss.; y, de 11 de diciembre de 2014, en el asunto C-212/13, Caso Ryneš, apartado 21.

[37] Sentencia del Tribunal de Justicia (Gran Sala), de 9 de noviembre de 2010, en los asuntos C-92/09, Caso Volker und Markus Schecke GbR y C-93/09, Caso Hartut Eifert, acumulados, apartado 53.

en la que dicho tratamiento estaría sujeto a las disposiciones normativas de protección de datos personales en la Unión Europea[38]. De ahí que el TJUE reconozca la estrecha relación entre derechos, cuyo contenido puede ser en ocasiones coincidente.

Además, es factible considerar por lo que hace a la estrecha relación entre el derecho a la vida privada consagrado por el TEDH y la Carta de Derechos Fundamentales, que esta establece en su artículo 52, apartado 3, que "[e]n la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo [...], su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa".

De igual forma, este Tribunal en diversas ocasiones ha tenido oportunidad de referirse al carácter independiente de las autoridades de control de los datos personales, que exige la Directiva 95/46/CE. Sobre este aspecto en particular, el Tribunal ha establecido que "[l]a garantía de independencia de las autoridades de control nacionales tratan de asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y debe interpretarse a la luz de dicho objetivo". Todo ello implica que las autoridades de control actúen con objetividad e imparcialidad, esto es, libres de cualquier influencia externa, directa o indirecta, que pudiera poner en peligro de la tarea que les corresponde de lograr un justo equilibrio entre la libre circulación de los datos personales y el derecho a su vida privada (intimidad)[39]. Bajo estas consideraciones, el Tribunal constata que si bien la independencia funcional de las autoridades, "en el sentido de que no estén sujetas a instrucción alguna en el ejercicio de sus funciones", es una condición necesaria para garantizar el cumplimiento de sus tareas[40], esta independencia funcional no basta por sí sola, toda vez que es necesario que la misma también se ejerza de manera indirecta, esto es, que pueda excluir toda forma de influencia que pudiera orientar las decisiones de la autoridad, como podría ser una relación de supervisión jerárquica[41].

Es importante subrayar que precisamente la carencia de una autoridad de control independiente por parte de los Estados Unidos de América fue uno de los motivos que dio lugar a que el TJUE invalidara el Acuerdo de Puerto Seguro, al que nos hemos referido con anterioridad (apartados 41 y 42 de la Sentencia)[42], mismo que pone de manifiesto la relevancia de homologar criterios en beneficio de las personas.

Por tanto, deben quedar claras tres ideas en relación con las autoridades de control o garantes de los derechos y libertades fundamentales, en particular por lo que se refiere

---

[38] Sentencia del Tribunal de Justicia (Gran Sala), de 29 de junio de 2010, en el asunto C-28/08, Caso Bavarian Lager, apartado 61.

[39] Sentencia del Tribunal de Justicia (Gran Sala), de 9 de marzo de 2010, en el asunto C-518/07, Caso Comisión/Alemania, apartado 25 y ss.

[40] Sentencia del Tribunal de Justicia (Gran Sala), de 8 de abril de 2014, en el asunto 288/12, Caso Comisión/Hungría, apartado 51 y ss.

[41] Sentencia del Tribunal de Justicia (Gran Sala), de 16 de octubre de 2012, en el asunto C-614/10, Caso Comisión/Austria, apartado 42 y ss.

[42] Caso Schrems, *cit.*, apartados 41 y 42.

a la protección de datos personales. La primera es que exista y que sea independiente. La segunda, que dichas autoridades de control puedan ejercer sus competencias de manera que se proteja de manera efectiva el derecho a la protección de datos personales. Y la tercera, que la ausencia de dichas autoridades de control impide el reconocimiento del nivel adecuado de protección de un país, con independencia de otros elementos previstos para su tutela.

La sentencia del TJUE que invalidó el Acuerdo de Puerto Seguro entre la Unión Europea y los Estados Unidos de América explica que "debe entenderse la expresión 'nivel de protección adecuado' en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta"[43] y añade que "[a]unque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión"[44]. Si bien el territorio donde se encuentran los datos personales es un factor a considerar para determinar si un país cumple con un nivel adecuado de protección, no es el único. El nacionalismo de datos[45] no puede llevar a perder de vista que lo importante no es dónde están los datos personales, obviando otros mecanismos, como la regulación e, incluso, las normas corporativas vinculantes[46] que son necesarias para facilitar la libre circulación de datos personales a nivel internacional.

II. Un equilibrio global es necesario y posible

1. *Asimetrías de protección*

El reconocimiento del derecho a la protección de datos personales en los instrumentos internacionales, así como su interpretación jurisprudencial, pone de manifiesto las asimetrías que se presentan por región por lo que hace a su reconocimiento y alcance.

Como se ha podido constatar de la jurisprudencia emitida por los tribunales internacionales, el desarrollo del derecho a la protección de datos personales se ha presentado

[43] Caso Schrems, *cit.*, apartado 73.

[44] *Idem.*, apartado 74.

[45] Cfr. Castro, Daniel, "The False Promise of Data Nationalism", en *The Information Technology & Innovation Foundation*, diciembre, 2013; y, Gutiérrez, Horacio E. y Korn, Daniel, "Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America", en *Inter-American Law* Review. *University of Miami School of Law*, vol. 45, issue 1, 2014.

[46] Sobre dichas normas vinculantes y las Reglas Transfronterizas de Privacidad véase el *Common Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Privacy Rules System.* Disponible en: http://mddb.apec.org/Documents/2014/ECSG/ECSG1/14_ecsg1_013.pdf

fundamentalmente en Europa, sea mediante su vínculo con el derecho a la vida privada, reconocido en el artículo 8 de la CEDH, o de manera particularizada por medio del ámbito de la Unión Europea. El hecho de que la Carta de Derechos Fundamentales, de manera consistente con el Tratado de Funcionamiento de la Unión Europea, lo reconozca de forma autónoma y con un ámbito específico de protección, obliga a todos los Estados miembros de la Unión a adecuar su legislación doméstica al más alto nivel normativo y a adoptar los criterios que determinan su interpretación y alcance.

En términos generales, la base para garantizar una protección adecuada que se materialice en el control que la persona pueda tener sobre el tratamiento de sus datos personales, se constituye mediante unos criterios de legitimación, los principios de la protección de datos, la posibilidad de ejercer derechos por parte del titular de los datos y la supervisión, misma que puede concretarse en la tutela de la persona a la que se refieren los datos personales que son objeto de tratamiento, así como la atribución y el ejercicio de potestades de investigación y sanción por parte de una autoridad de control independiente. Si bien el TEDH se ha referido a algunos de estos aspectos en contextos específicos, la normatividad de la Unión Europea, así como los criterios que se han desarrollado sobre la misma, tanto en el ámbito jurisdiccional como no jurisdiccional (como es el caso del Grupo de trabajo del artículo 29 o, incluso, del llamado Grupo de Berlín, además por supuesto de las propias autoridades de control nacionales en la Unión Europea), han permitido establecer los contornos del derecho a la protección de datos personales.

Se trata, entonces, de garantías que tienen que darse de manera efectiva y que, al mismo tiempo, implican un claro compromiso europeo con el derecho humano a la protección de datos personales. Estas, a su vez, presentan un carácter transversal, cuyo alcance abarca cualquier ámbito o momento, con independencia de que el titular de los datos actúe en relaciones de subordinación (frente a las autoridades públicas) o de coordinación (frente a otros particulares).

Por tanto, la ausencia total o parcial de estas garantías, tanto desde un punto de vista formal, en cuanto a su reconocimiento en la legislación o mediante mecanismos de regulación sectorial o, incluso de autorregulación, como desde una perspectiva práctica, por lo que se refiere a la efectividad de las mismas, implica la imposibilidad en el ámbito europeo de reconocer un nivel de protección adecuado para quien carezca de las mismas.

Cuestión distinta ocurre en el ámbito americano y particularmente dentro del Sistema Interamericano de Derechos Humanos. Si bien ya existe una larga tradición que ampara el derecho a la vida privada, la protección de datos personales carece aún de una construcción propia, tanto normativa como jurisprudencial, a pesar de los incipientes esfuerzos y avances de la Organización de Estados Americanos (OEA)[47] y de la Red Iberoamericana de Protección de Datos (RIDP). Ello también, a pesar de que varios Estados parte del Sistema han adoptado, con una clara influencia europea, el derecho a

[47] Véase el informe 474/15 rev. 2, del Comité Jurídico Interamericano, sobre Privacidad y Protección de Datos Personales, de 26 de marzo de 2015.

la protección de datos personales con un carácter de derecho humano autónomo, aunque interrelacionado con el derecho a la vida privada, cuyo alcance se proyecta tanto en el reconocimiento del derecho a la autodeterminación informativa de las personas, como del *habeas data*. Este es precisamente el caso de Argentina, Chile, Uruguay, México y Colombia, entre otros.

En el caso concreto de Argentina y Uruguay, es admisible decir que la Comisión Europea les ha otorgado el reconocimiento como países que efectivamente establecen un nivel adecuado de protección de datos personales, lo que incluso ha llevado a Uruguay a ser el primer y único país en Latinoamérica en haber procedido a la adhesión al Convenio 108 y su Protocolo Adicional, mismos que tienen por objeto establecer las reglas generales para garantizar el respeto a la vida privada (por lo que se refiere al tratamiento automatizado de datos de carácter personal) y simultáneamente la libre circulación de la información[48].

2. *Necesidad de un equilibrio global*

La ausencia de criterios internacionales uniformes acerca del derecho a la protección de datos personales no solo dificulta la relación con Europa por lo que hace a los flujos de información entre autoridades y el sector privado, sino que además acentúa las diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debiera residir precisamente en su "universalidad".

La falta de estándares comunes entre regiones entorpece el cumplimiento de ciertos objetivos importantes para el progreso económico y social, el desarrollo del intercambio entre países y el bienestar de los individuos, como eliminar las restricciones en la libre circulación de los datos personales, falsear la competencia económica e impedir que las administraciones cumplan los cometidos que les incumben[49], así como problemas de seguridad de los datos.

Además, no debemos olvidar que la protección de la persona por lo que hace al tratamiento de sus datos personales es un instrumento necesario para garantizar la protección de otros derechos humanos y libertades fundamentales, toda vez que redunda, a fin de cuentas, en la dignidad de la persona. Como se ha constatado en las diversas resoluciones del Tribunal Europeo (y en cierta medida en la CIDH), el tratamiento adecuado de la información personal –mismo que incluye su recogida, uso, acceso, divulgación, transferencia, etc.– resulta indispensable para garantizar la vida privada de las personas. Asimismo, se relaciona con otros derechos humanos como la igualdad y la no discriminación, toda vez que la revelación de información "sensible" puede dar lugar al aislamiento de la persona o, incluso, a tratos segregacionistas. De ahí que el

[48] Maqueo, M. y Moreno, J., "Implicaciones de una ley general en materia de protección de datos personales", *DT-DEJ del Centro de Investigación y Docencia Económicas*, núm. 64, marzo de 2014, p. 3.

[49] Si bien estas ideas se han desarrollado en el ámbito de las relaciones entre los países miembros de la Unión Europea, concretamente en la Directiva 95/46/CE en su considerando 7, lo cierto es que son extrapolables a las relaciones con otros países en un contexto propio de la globalización.

derecho a la protección de datos personales busque tutelar a las personas, mediante el otorgamiento de un poder de control sobre su propia información, sujeto a ciertas restricciones susceptibles de ser valoradas bajo márgenes de apreciación que comprendan tanto los requisitos que permiten justificar una injerencia como la gravedad de la afectación respecto de otros derechos humanos.

Una cuestión adicional que es posible considerar para justificar la necesidad de generar estándares homogéneos a nivel global es el efecto que ello tendría en el fortalecimiento de la confianza en los usuarios de servicios o consumidores. La protección efectiva de la información personal, mediante el derecho sustantivo, la existencia de autoridades de control independientes, las normas procedimentales y sancionatorias, así como los mecanismos de cooperación adecuados, son la base para generar esta confianza, necesaria en todos los ámbitos, sea en las relaciones entre particulares y las Administraciones Públicas como respecto de los consumidores y proveedores de bienes y servicios que tratan datos personales.

Impulsar la confianza por medio de una protección adecuada, por tanto, depende, por una parte, de la adopción e implementación de diversas medidas tanto normativas como institucionales, y por otra parte, de que las mismas sean efectivas, lo que pasa por evaluar a lo largo del tiempo si responden a las circunstancias actuales en cada momento.

En este sentido, asegurar y proteger los derechos humanos y las libertades fundamentales, entre los que se encuentra el derecho a la protección de datos personales, debe ser una tendencia a considerar frente a los planteamientos ocurridos hasta hace apenas unas décadas, en el sentido de que aún no era el momento adecuado para reconocer este derecho en el texto del CEDH.

3. *Estándares comunes*

La generación de estándares comunes con un alcance global acerca de la protección de datos personales no solo es necesaria sino también posible, toda vez que sus cimientos ya han sido establecidos por el propio reconocimiento y desarrollo del derecho a la vida privada. A todo ello se añade el progresivo avance en la materia que se ha venido generando en algunos países del Continente Americano y, aunque con un alcance limitado, en el propio Sistema Interamericano de Derechos Humanos.

Ciertamente los mecanismos que permitan homologar estos estándares de protección adecuada pueden adquirir muy diversa naturaleza. No obstante, dos vías que consideramos pertinentes para tal fin, debido a su proyección y su carácter vinculante en el ámbito internacional, son, por una parte, la búsqueda de la adhesión al Convenio 108 y su Protocolo Adicional por aquellos países que, como México, aún no son parte del mismo y, por la otra, la adopción de criterios compatibles en los diversos Sistemas de Derechos Humanos. Esto último podría impulsarse con la solicitud de opiniones consultivas por parte de los países interesados o, a su vez, por los propios particulares que ven vulnerados sus derechos.

De acuerdo con todo lo anterior, algunos de los elementos que resultan clave para que la protección de la persona, por lo que hace al tratamiento de sus datos personales,

sea efectiva son: (a) el establecimiento de principios y deberes que legitimen el tratamiento de los datos personales, consistentes con la evolución social y tecnológica; (b) el reconocimiento de los derechos de los interesados y los procedimientos para garantizar su ejercicio, con el fin de que se les permita un control efectivo respecto de su información, y; (c) la existencia de autoridades independientes de control, en el sentido de que sean ajenas a cualquier influencia externa, tanto directa como indirecta.

III. Conclusión

El desarrollo evolutivo del derecho a la protección de datos personales desde una perspectiva internacional ha sido asimétrico, a pesar de la necesidad de generar estándares comunes consistentes con los riesgos que supone el desarrollo tecnológico y un mundo cada vez más global, con objetivos compartidos. La declaración de invalidez del Acuerdo de Puerto Seguro del Tribunal de Justicia de la Unión Europea es tan solo una manifestación más de este proceso desigual entre regiones y países.

Si bien el desarrollo de este derecho, en estrecha relación con el derecho a la vida privada, ha sido lento, los avances en la generación de criterios, la delimitación de su alcance, así como su relación con otros derechos humanos en contextos específicos, nos permiten suponer que la aducida falta de experiencia para su reconocimiento no es ya un argumento viable en la actualidad. Es necesario generar estándares comunes que permitan proteger de manera efectiva a las personas con una aproximación universal, para garantizarle el mayor disfrute de sus derechos y libertades, así como para contribuir con el desarrollo económico y social en un marco de economía global digital y una sociedad interconectada como la actual.

Bibliografía

Alexy, Robert, "Constitutional Rights and Proportionality", *Revus, Journal for constitutional theory and philosophy of law*, núm. 22, 2014, pp. 51-65.

Castro, D., "The False Promise of Data Nationalism", en *The Information Technology & Innovation Foundation*, diciembre de 2013.

Cate, Fred H. y Mayer-Schönberger, V., "Data Use and Impact Global Workshop", *Center for Applied Cybersecurity Research,* Indiana University, 2013.

_____, *Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes*, November, 2012.

Cate, F. H., Cullen, P. y Mayer-Schönberger, V., *Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines*, March, 2012.

De Hert, P. y Gutwirth, S., "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", en Gutwirth, S. *et al.* (eds.), *Reinventing Data Protection?*, Springer, 2009. [Versión electrónica]

Gutiérrez, H.E. y Korn, D., "Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America", *Inter-American Law Review*, University of Miami School of Law, vol. 45, issue 1, 2014.

Kikelly, U., "The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights", *Human rights handbook*, num. 1, Strasbourg. 2003.

Maqueo, M. y Moreno, J., "Implicaciones de una ley general en materia de protección de datos personales", Documento de Trabajo de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, núm. 64, marzo 2014.

Miller, A. R., *The Assault on Privacy: Computers, Data Banks, and Dossiers*, University of Michigan Press, 1971.

Piñar Mañas, J.L., "¿Existe privacidad?", en *Protección de Datos Personales. Compendio de lecturas y legislación*, México, Tiro Corto Editores, 2010.

Puente Escobar, A. (2008), "La Agencia Española de Protección de Datos como garante del derecho fundamental a la protección de datos de carácter personal", *Azpilicueta. Cuadernos de Derecho*, núm. 20, 2008.

Roagna, I. (2012), "Protecting the right to respect for private and family life under the European Convention on Human Rights", *Council of Europe Human Rights handbook*, Strasbourg, 2012.

Suárez Crothers, C., "El concepto de derecho a la vida privada en el derecho anglosajón y europeo", en *Revista de Derecho* (Valdivia), Vol. XI, diciembre 2000.

Warren, S.D. and Brandeis, L.D., "The Right to Privacy", *Harvard Law Review*, vol. IV, num. 5, December 15, 1890.

Juan Carlos I, Rey de España

y en su nombre

el Rector de la Universidad de Salamanca

Considerando que, conforme a las disposiciones y circunstancias prevenidas por la legislación vigente,

Doña María Solange Maqueo Ramírez

nacida el día 7 de octubre de 1974 en México D.F. (México), de nacionalidad mexicana,

ha superado los estudios de Doctorado en el Departamento de Derecho Público General, dentro del Programa de Derecho, Economía y Sociedad en la Unión Europea, en las condiciones establecidas por la legislación vigente para los poseedores de títulos extranjeros no homologados a un título español de segundo ciclo, y ha hecho constar su suficiencia en esta Universidad, con la calificación de SOBRESALIENTE "CUM LAUDE", el día 11 de julio de 2011, expide el presente título de

Doctora por la Universidad de Salamanca

con carácter oficial y validez en todo el territorio nacional, que faculta a la interesada para disfrutar los derechos que a este título otorgan las disposiciones vigentes.

Dado en Salamanca, a 20 de septiembre de 2011

[redacted]

Registro Nacional de Títulos | Código de CENTRO | Registro Universitario de Títulos

1-BD-475031 [redacted]

S.A.

MECM-FNN

FE PÚBLICA
NOTARIAL

CONSEJO GE
NOTARIAL
EUROPA
UNIÓN LATINA
NOTARIADO

0183760

D. JULIO RODRIGUEZ C
ARIO DE SALAMANCA,
EGIO DE CASTILLA Y LE
OY FE de que la presenti
oncuerda fielmente con su
ne ha sido
Salamanca,

[redacted]

[redacted]

Reverso del título universitario oficial del proceso

Por la Universidad de Salamanca se expide el título de Graduado en [redacted]

de septiembre de 2011 a favor de Doña María Solange Maqueo Ramírez que superó el día 10 de [redacted]

[redacted]

M.R.C.M-F.N.M.T Mod. 41/00

El Rector

de la

UNIVERSIDAD DE SALAMANCA

considerando que

DOÑA MARÍA SOLANGE MAQUEO RAMÍREZ

ha superado los cursos y trabajos de investigación del Programa de doctorado de esta Universidad* *Derecho, economía y sociedad en la Unión Europea,* conforme a lo previsto en el R.D. 778/98 de 30 de abril, habiendo obtenido la correspondiente suficiencia investigadora, vinculada al área de conocimiento *Economía Aplicada,* expide el presente

DIPLOMA DE ESTUDIOS AVANZADOS

con carácter de Título Propio de la Universidad de Salamanca (Art. 34.3 de L.O.U.)

Salamanca, 6 de febrero de 2004

LA INTERESADA

[redacted]

EL JEFE DE LA SECCIÓN

** sin previa homologación de su título de Licenciado/a*

Registro Universitario de Diplomas y Títulos Propios 04/111

UNIVERSIDAD DE SALAMANCA
FACULTAD DE DERECHO
Departamento de Economía Aplicada

Campus "Miguel de Unamuno"
37007 Salamanca – Tfno.: 923 294441

En cumplimiento de lo establecido en el art. 5.4 del "Reglamento de Grado de Salamanca", le comunico que el Consejo del Departamento de Economía Aplicada, en sesión celebrada el día 22 de septiembre, acordó, por unanimidad, admitir para su defensa el Trabajo de Grado presentado por usted, bajo la dirección del Dr. D. Fernando Rodríguez López, con el título "Derecho Economía y Sociedad en la Unión Europea", y proponer como integrantes de la Comisión evaluadora correspondiente a los siguientes profesores:

i. Presidente: Prof. Dr. D. José Ignacio Sánchez Macias (Suplente: Profa. Dra. Dña. Victoria Muriel Patino)
ii. Vocal 1: Prof. Dr. D. Rafael Bustos Gisbert (Suplente: Prof. Dr. D. Agustín Sánchez de Vega)

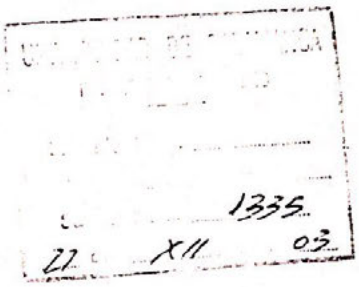
Salamanca, 23 de septiembre de 2003

El Director del Departamento

[redacted]

Fdo.: Rafael Muñoz de Bustillo Llorente

UNIVERSIDAD DE SALAMANCA
FACULTAD DE DERECHO



La Junta de la Facultad de Derecho de la Universidad de Salamanca, en su sesión de 3 de diciembre de 2003, acordó por unanimidad que constase en Acta la felicitación de la Junta de Facultad a. Dª Mª SOLANGE MAQUEO, por su reciente obtención del Grado Salamanca.

De lo cual como Secretario doy fe.

Salamanca, 4 de Diciembre de 2003
EL SECRETARIO,

[redacted]

Universidad de Salamanca
Servicio de Cursos Extraordinarios
y Formación Continua

Certificado

Unión Europea
Cátedra Jean Monnet
de Derecho Comunitario

D./Dña. **Mª SOLANGE MAQUEO RAMIREZ** *con D.N.I./nº Pas.* .....

Ha asistido al **XI** *Curso organizado por la Cátedra Jean Monnet de Derecho Comunitario de la Universidad de Salamanca sobre*

Derecho Comunitario

con un valor académico de 9 créditos (conforme al acuerdo de la Comisión de Docencia, delegada de la Junta de Gobierno, de **15 de julio de 2002**...), *que se desarrolló en la Facultad de Derecho de la Universidad de Salamanca, desde el mes de octubre de* **2002** *al mes de febrero de* **2003** *y en el examen realizado ha obtenido la calificación de* [redacted].....

[redacted]

Dirección de Cursos Extraordinarios

Jus neque inflecti gratia neque
perfringi potentia neque adulterari
pecunia debet

La Escuela Libre de Derec
bajo el patronato del Ilustre y Nacion
Colegio de Abogados de México,

[redacted]

consideración, a que terminó en ella sus
tudios y sustentó examen profesional el día
14 de diciembre de 1999 la Srita.
María Solange Maqueo Ramírez
expide este Título que acredita su compete
para ejercer en el Foro Mexicano la profe
n de Abogado.

México, D. F., a 22 de diciembre de

La Junta Directiva

[redacted]

Secretario General

Título de Abogado expedido a favor de la
Srita. María Solange Maqueo Ramírez
de conformidad con los artículos 2º, 8º, 9º y 10º de la Ley de 30 de diciembre de 1944 y 11º del Reglamento
de la misma, siendo los estudios a que se refiere, todos los necesarios para la carrera de Licenciado en Derecho,
conforme a la mencionada Ley, al Decreto de 17 de enero de 1930 y al Plan de Estudios respectivo.