REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

NÚMERO 3 - octubre, 2018

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

10 AÑOS
DE LA LEY DE PROTECCIÓN
DE DATOS PERSONALES

SUMARIO

PRÓLOGO

Tengo el gusto de presentar el tercer número de la *"Revista Uruguaya de Protección de Datos Personales"* que publica la Unidad Reguladora y de Control de Datos Personales.

Tal como en los dos números anteriores, correspondientes a 2016 y 2017, en esta oportunidad la Revista recoge trabajos que enfocan temas de sumo interés y actualidad, realizados por expertos de diverso origen, fallos jurisprudenciales, y decisiones administrativas y, acorde con el plan inicial, también una entrevista.

La materia de protección de datos dice relación con las personas en cuestiones de toda índole (salud, trabajo, solvencia patrimonial y un interminable etcétera) y, a la vez, con la innovación incesante que hace competitivas las empresas, la necesidad de flujos transfonterizos y, entonces, el rol de organizaciones estatales, supranacionales, internacionales y globales, públicas y privadas.

En el sentido antes indicado el Reglamento (UE) 2016/679 del Parlamento Europeo y de *Consejo* que entró a regir el 25 de mayo de 2018, en su propia denominación, refiere *"a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".*

De manera similar los Estándares aprobados por la Red Iberoamericana de Protección de Datos en junio 2017 atienden el derecho fundamental al debido tratamiento de los datos personales y pretenden contribuir a la circulación de aquellos, con garantías, lo que es base de una integración económica y social.

Con esta perspectiva, este Nº 3 de la Revista incluye, sin duda, contenido de calidad en la línea trazada por la Unidad.

Es que importan sí los procesos, los productos, las aplicaciones, etc. pero antes que nada las personas y el respeto de la dignidad que les es inherente, lo cual constituye una cuestión cultural que se abre a todas las dimensiones humanas.

Dr. Felipe Rotondo

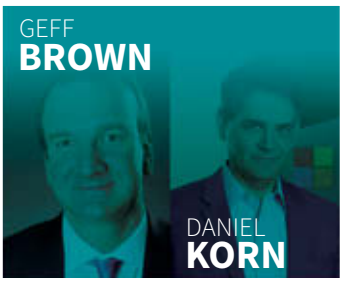
Presidente

Consejo Ejecutivo – URCDP

DOCTRINA


MARTIN
ABRAMS


CARLOS ALBERTO
BONNIN ERALES


GEFF
BROWN
DANIEL
KORN


EDUARDO
CIMATO

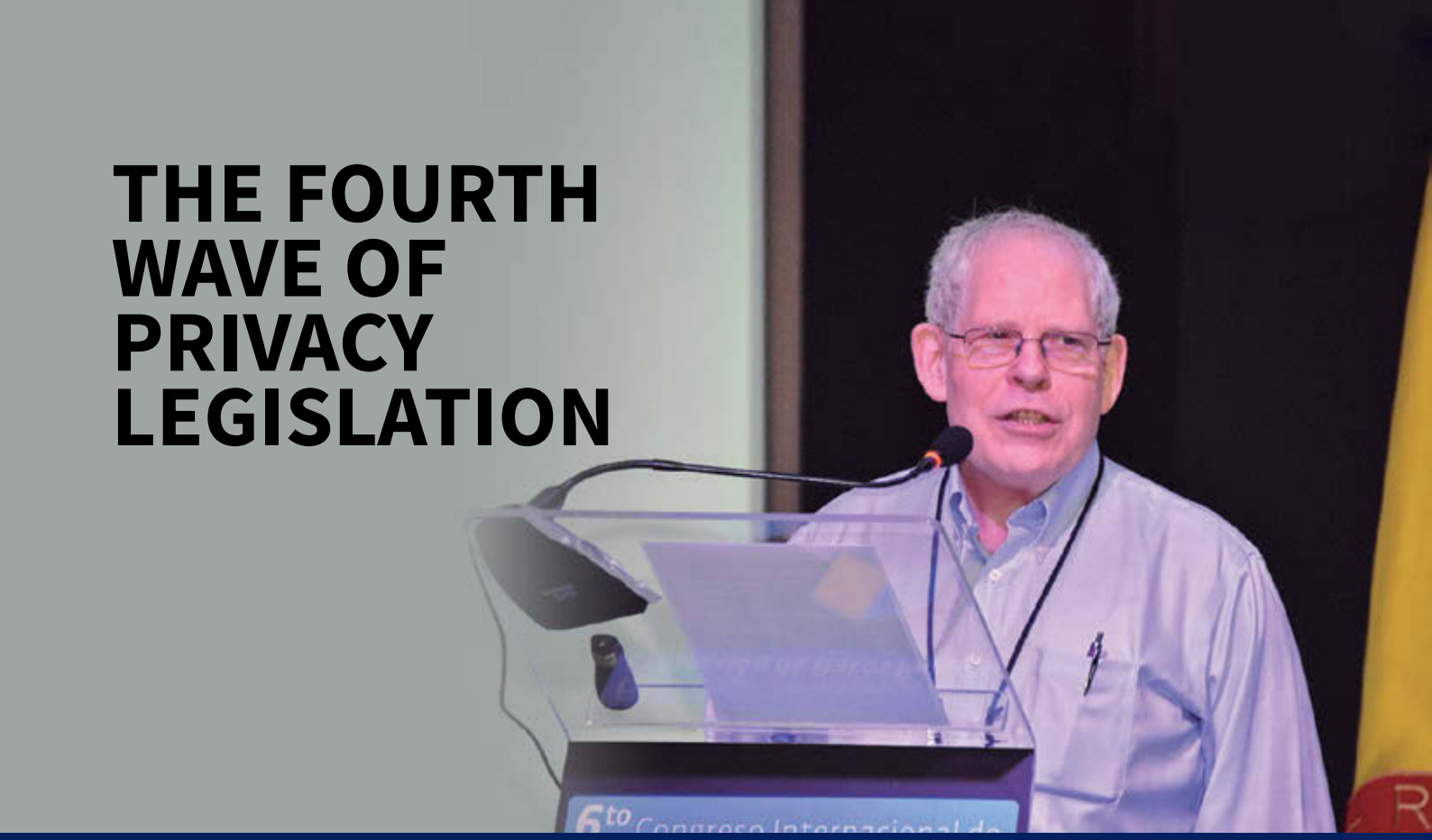

ISABELLE
FALQUE-PIERROTIN


PAULA
VARGAS
LAURA
JUANES MICA


JOHN
PÉREZ BRIGNANI


JESÚS
RUBÍ NAVARRETE

THE FOURTH WAVE OF PRIVACY LEGISLATION



MARTIN
ABRAMS

Es Director Ejecutivo y Jefe Estratégico de la "Information Accountability Foundation" –organización sin fines de lucro para la investigación y educación-. Abrams posee 40 años de experiencia como innovador en políticas de información y consumidores. Ha sido un actor relevante en el desarrollo de conceptos vinculados a la protección de datos como los de "accountability", aproximaciones de dos fases ante big data, y asesoramientos éticos. Ha organizado conferencias y seminarios en todos los continentes.

Fue co-fundador del "Centre for Information Policy Leadership" en "Huntington & Williams LLP", que dirigió durante 13 años. Previamente fue Vicepresidente de Políticas de Información en Experian y Director de Políticas de Información en TRW Information Systems, dónde diseñó una de las primeras herramientas para las evaluaciones de impacto de privacidad. Abrams comenzó su trabajo en políticas de consumidores en el Banco de la Reserva Federal de Cleveland, en el cargo de Vicepresidente adjunto y Oficial de Asuntos Comunitarios.

SUMARIO

RESUMEN

En el artículo los autores analizan cómo los avances de la protección de datos personales en un mundo en que la información es un motor del Desarrollo económico, conjuntamente con las nuevas regulaciones -entre las que se encuentra el Reglamento General de Protección de Datos- generarán una cuarta ola de legislaciones en materia de privacidad. Se desarrollan los principios de esta cuarta ola y su impacto en las legislaciones actuales, todo en base al trabajo de la Information Accountability Foundation (IAF).

INTRODUCTION

The European Union (EU) enacted the General Data Protection Regulation (GDPR) in 2016 and it went into effect in May 2018. The European legislative process began in 2012. The GDPR prohibits data transfers to other jurisdictions unless those jurisdictions have adequate data protection regimes. The GDPR is very different from the Directive it replaced. Countries that had achieved adequacy, such as Uruguay, will have their adequacy revisited by the European Commission by 2022. Other countries, such as Japan, that never achieved adequacy are now trying to obtain that status. For many countries, achieving and maintaining adequacy will require an update to laws that match the detail in the GDPR, which has 99 articles and over 100 recitals, and still meet their own domestic legal, social and economic demands.

At the same time, ministries in most countries are driving economic growth through the data driven fourth industrial revolution. The elements of that revolution are sensor driven technologies that create the raw material for advanced analytics and artificial intelligence (AI). The great leaps forward in AI have taken place since the GDPR was passed. These technological developments have led to a push for building ethics into the data protection process. Ethics fill the gap between what business wants technology to do and a privacy law that is showing stress from the technological benefits that society desires.

Wikipedia Description of Fourth Industrial Revolution. The **Fourth Industrial Revolution (4IR)** is the fourth major industrial era since the initial Industrial Revolution of the 18th century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres, collectively referred to as cyber-physical systems. It is marked by emerging technology breakthroughs in a number of fields, including robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, the Internet of Things, the Industrial Internet of Things (IIoT), fifth-generation wireless technologies (5G), additive manufacturing/3D printing and fully autonomous vehicles.

This reconciliation between improved personal protections in an increasingly data driven era, the need to be interoperable with the GDPR, and the creation of the means to think and learn with data to drive economic growth will precipitate the fourth wave of privacy legislation. This paper reviews how legislation has developed thus far and suggests principles for this fourth wave. The paper is based on the work of the Information Accountability Foundation (IAF) on data ethics, data stewardship and accountability.[1]

BACKGROUND

People everywhere live in a sensor rich environment. Even aboriginals in the deepest Amazonian rain forest are observed by drones. For those people that live in cities, there are CCTV cameras, the Internet, mobile ecosystems, sensors on medical devices and wearables, connected cars, and the Internet of Things (IoT). This sensor rich data fuels powerful technologies that stop the cars people drive, regulate the medicines people use, improve the products people buy, and guide people to the right location. They also define the credit worthiness of people, the products people are likely to buy, how people will most likely vote, and whether people are a threat to their neighbors.

Observation is critical to economic development, safety, education, and health outcomes. The observational world will only continue to accelerate. Societies have some room for limiting where observation takes place and whether observation leads to digital data. However, observation becomes increasingly difficult for people to control.

Observation, if recorded, is a processing, and it drives further processing. Data protection law sets

1 *The IAF is a United States not-for-profit research and education organisation. The IAF has conducted projects and education fora in the Americas, Europe, Asia, Africa and Australia.*

boundaries around that processing. The processing needs to be specified and within the bounds of what is specified. Increasingly, even what is specified is beyond what the typical responsible person understands.

Privacy law has always encompassed two distinct functions. The first is assisting people control the data that is identifiable to them. This is autonomy and is accomplished through informed consent. The second is processing data fairly and for fair outcomes. Fair processing has typically been accomplished through specifications for societally beneficial processing, such as credit referencing, or through accountability provisions. Over time, as observation has become more ubiquitous, accountability provisions have become more important. This shift has happened as the marketplace has made privacy notices longer and more complex and has stretched the concept of compatible use. Much of this change has been driven by privacy enforcement agencies that have created explicit accountability guidance. Examples are the EU Article 29 Working Party accountability opinion in 2010 and the Canadian, Hong Kong and Colombian accountability guidance in 2012.

LEGISLATIVE WAVES AND TECHNOLOGY

Physical privacy issues have existed as long as the human species has had eyes, ears, and a curiosity about others. Societies have evolved rules about how to create private spaces for individuals, so they may conduct parts of their lives beyond the gaze of others. Information privacy started to become an issue as soon as man created the technology to write and record impressions. Information and communications technology evolved slowly over thousands of years until the invention of digital computing took place during World War II. One can chart the development of technology against law for the past fifty years.

Technology/Privacy and Data Protection Law

Year	Technology	Law
1970	Introduction of relational data bases	Hessen Privacy Law - *beginning of wave one*
1971		U.S. Fair Credit Reporting Act
1977	Apple II (distributed processing power)	
1980		OECD Guidelines
1989	FICO credit score (statistical profiling and automated decision-making)	
1990	First web browser	
1993	First consumer web browser – created highly granular transaction data and the ability to track over time and space	
1995		EU Directive enacted - *beginning of wave two*
2000	Adoption of common programming modules in response to Y2K crisis – created the means for cloud computing	
2004 - 2010	Means for conducting analytics with unstructured data - beginning of big data	
2007	iPhone introduced – created the means for constant consumer interaction and tracking	
2012		GDPR legislative process began
2010 - 2015	Continual adoption of big data technologies, early introduction of IoT	
2016		GDPR enacted – *wave three*
2015 - 2018	AI becoming more common, testing of autonomous vehicles, smart devices track health, smart homes applications use, IoT technologies	
2018 - ?		Digital legal infrastructure discussions begin in many jurisdictions – *wave four*

As the chart above shows, there has been a continual evolution of digital technologies over the past 50 years. Technology continually gets faster, cheaper and more capable of looking at trends within data that go beyond unaided human abilities. The first privacy law in 1970 in the German state Hessen was a reaction to mainframe computers. The initial mainframe computers were capable of doing specific tasks with specific data records. The Hessen law was enacted before IBM published a paper that explained relational databases. Relational databases, which sparked a revolution in data utility that has been accelerating ever since, made it possible for data to be easily reused for new purposes. So, before the ink on the first privacy law was dry, the basic legal structural theory: specified use plus specified processing equals individual control, was defined.

Wave one: The first wave began with privacy legislation at the German state Hessen, Sweden and the U.S. Fair Credit Reporting Act. The wave continued with the OECD Privacy Guidelines, sector specific laws in the United States, and privacy laws that predate the EU Directive. The laws were designed to create controls for individuals related to their data or to fix specific risks of harm related to a particular data use, such as drivers' license information.

The EU began a process in 1990 to make sure that disparities between the different privacy laws within the 14 states in the economic union would not impact the single market. The solution was a directive drafted by Directorate General Internal Market that would harmonize data protection at the higher level found in Germany and France. The drafters added protection for data that might flow outside the EU by prohibiting such transfers unless the data importer had equivalent privacy protections. By the time the Directive was passed in 1995, the term had transitioned from "equivalent" to "adequate" privacy protection.

When the Directive drafting process began, data transfers were accomplished by copying data onto a magnetic medium, loading them on an airplane, and mounting them on a new computer at the new location. By the time the Directive was enacted in 1995, businesses in remote locations were already using the Internet to collect data in Europe and to transfer the data collected there to locations outside the EU. The underlying structure of the consumer driven Internet, ubiquitous observation and instant transfers, created challenges for the new wave two privacy laws.

Wave two: Wave two began with the EU Data Protection Directive which required each of the EU states to enact conforming legislation. The adequacy provisions in the Directive had the effect of encouraging privacy legislation in trading partner states. While the Directive established the requirement that all processing be conducted under one of six legal bases, with consent being one of those legal bases, the conforming laws were mostly consent based. Most legislation adopted outside Europe also required consent. Accountability, for the most part, was inferred rather than being explicit. The exceptions were Canada and Mexico where accountability was an express provision of the privacy law. As advanced analytics and communications technologies, such as smart phones, emerged, the drive to add accountable practices, such as privacy by design, became increasingly encouraged.

During the 1990's, processing power was continually improved, and communications costs decreased while bandwidth increased. These developments made it possible to have ever greater knowledge about individuals and to use that knowledge to create greater economic value. As the technology ecosystem approached the year 2000, huge resources were spent to update systems, so they would not stop when the clock stuck midnight on January 1, 2000. This expenditure had the effect of creating common processing modules that would eventually facilitate the development of cloud computing. By the mid-point of the first decade of the 21st century, scientists had discovered how to process unstructured data. The manner in which predictive sciences were conducted were changed to place greater emphasis on the correlation to big data. Advanced analytics led European policymakers to begin work on a new data protection law that created one, EU-wide regulation, rather than conforming national laws.

Between passage of the 1995 Directive and the beginning of the GDPR process, responsibility for data protection was moved from the Internal Markets Director General to the Justice Director General, placing greater emphasis on data protection as a fundamental right. The 2010 Lisbon Treaty elevated fundamental rights to constitutional rights status. As a backbone of European citizenship, the GDPR's importance was enhanced. So even with similar legal language, the GDPR is differentiated from other legal regimes.

Wave three: The European General Data Protection Regulation is wave three. The GDPR places greater emphasis on six legal bases to process data and limits consent to where it is fully effective. It requires accountability measures, such as privacy by design, data protection officers, and data protection impact assessments. While it broadens use by placing less emphasis on consent, it restricts use by prohibiting profiling with legal effect unless one has consent. The GDPR is intended to drive comparable laws in other regions. However, the size and complexity of the GDPR and its link to European citizenship concepts make duplication difficult.

Just as wave two legislation in other regions was driven and inspired by the EU Directive, the GDPR is expected to drive additional wave three legislation. However, the pace in which new technologies and business processes are adopted are both enhanced and retarded by the GDPR. On the positive side, the GDPR for the first time makes accountable processes, such as privacy by design, data protection officers (as accountable parties) and data impact assessments mandatory. It limits the use of consent as a legal basis to those situations where it is fully effective, requiring organizations to conduct balancing assessments to assure processing is consistent with individuals' fundamental rights and freedoms. This assessment forces organizations to understand the true risks and benefits to impacted persons. It further encourages data driven research by making research a compatible purpose. However, the limitations on profiling and automated decision-making conflict with the way AI and IoT technologies are evolving and driving economic and social development. For example, medical devices, as an IoT technology, could be limited. This tension is already seen in Europe in the growing discussion of data ethics as a means to fill a governance gap.

The IAF believes that new laws that are responsive to both the basic requirements of the GDPR and the increased governance obligations that come with AI and linked devices will be different enough to be a fourth wave of legislation. These new laws, an example is Brazil's new privacy law, will reflect the European concept of legitimate processing explicitly permitted by a variety of legal bases in tune with local law. Flexibility to think and learn from data will be facilitated by rigorous assessment processes that will define both risks and benefits to individuals, groups of individuals and society as whole. Individuals' rights will be truly actionable and enforceable, but they will not force individuals to govern data use that is beyond most individuals' understanding.

Wave four: Wave four privacy laws will take the positive innovations in the GDPR and add processes that let society benefit from the data driven fourth industrial revolution. Organisations that wish to use data beyond common understanding will have to be able to demonstrate mechanisms for data stewardship. Further, they will need to be transparent about their values and have effective governance structures that include ethics by design, comprehensive assessments and independent oversight. Persons will have understandable and actionable individual rights

Over the Spring and Summer of 2018, the IAF has been working with the Hong Kong Privacy Commissioner for Personal Data and approximately 25 Hong Kong businesses to develop a full description of attributes for effective data stewardship. Based on that work and work conducted in Europe and Canada, the IAF has developed a set of twelve draft principles to facilitate the debate on wave four privacy legislation. The principles are divided into two parts: individual rights and accountable data stewardship.

IAF Fair Processing Principles to Facilitate Privacy, Prosperity and Progress

Individual Rights

1. **Transparency** Individuals have the right to be free from secret processing of data that pertains to or will have an impact on them. Organizations should provide understandable statements about their data collection, creation, use and disclosure practices and about their policies and governance. Those statements should be directed at enforcement agencies, but they should also be publicly available. Organizations should also provide summaries and other means that make their data collection, creation, use and disclosure practices understandable to individuals.

2. **Access and Redress** As a validation there is no secret collection, creation, use or disclosure taking place and confirmation of adequate data accuracy, individuals have the right to obtain the data they provided, to understand what observational data is created by the organization that pertains to them, and to be told what types of data are inferred by analytical algorithms. Because intellectual property rights may prevent individuals from having the right the right to request disclosure of inferences made by the organization, and where inferences such as scores potentially have negative consequences

for individuals, organizations should provide relevant explanations about their processing, appropriate opportunities for feedback, and the ability for individuals to dispute such processing.

3. **Engagement and Consent** Individuals have the right to know about data uses that are highly consequential to them, and to control those uses through an appropriate level of consent. Individuals also have the right to know that data is disclosed to third-parties beyond the context of the relationship, to request such disclosure not take place, to prohibit solicitations, and to challenge that a data use is not being undertaken in an accountable manner. Individuals have the right to object if they believe that the data about them is inaccurate or being used out of context, is not being undertaken in an accountable manner, or if they believe that uses of data are not legitimate. The right to object to processing does not pertain where data processing and use are permitted by law. Where highly consequential uses, such as health, financial standing, employment, housing and education, are governed by specific laws, those laws take priority.

4. **Beneficial Purposes** Individuals have the right to expect that organizations will process data that pertains to them in a manner that creates benefits for the individual, or if not for the individual, for a broader community of people. They also have the right to expect that data will not just serve the interests of the organization that collected the data. There may be times when objective processing does not serve the needs of each individual, but such processing does serve the broader needs of society. When this is the case, individuals may request an explanation of how processing is beneficial to the broader group. This explanation should be part of understandable summaries required under the Transparency Principle. Where there are negative consequences to individuals, individuals should expect an explanation of the results and the ability to dispute the findings, as provided in the Access and Redress Principle.

Accountable Data Stewardship

1. **Assessed and Mitigated Impacts** All collection, creating, use and disclosure of data should be compliant with all applicable laws, industry codes, and internal policies and practices, and should be subject to privacy, security and fair processing by design. Employees should receive appropriate training for their specified roles, and accountable employees should be identified to oversee privacy, security and fair processing obligations. Specifically, fair processing assessments should identify individuals and groups of individuals who are impacted, both negatively and positively, by the processing, and should guard against identifiable negative consequences. Where there are negative consequences, organizations should mitigate those consequences to the degree possible. If unacceptable consequences still persist for some individuals or groups, the organization should document why the benefits to other individuals, groups and companies are not outweighed by the unacceptable consequences.

2. **Secure** Data should be kept secure at a level that is appropriate for the data.

3. **In Context** Data should be collected, created, used and disclosed within the context of the relationship between the individuals to whom the data pertains and the organization, based on the reasonable expectations of individuals as a group. Public safety, security and fraud prevention are considered within context.

4. **Legitimate Uses** Data should be processed only for legitimate uses that have been disclosed or are in the context of those uses, and only the data necessary for those uses should be collected, created, used or disclosed. When the data is no longer necessary for these uses, it should not be retained in an identifiable manner.

Legitimate uses include the following:

   a. Where individuals have provided informed consent;

   b. Freely thinking and learning with data by organizations that demonstrate effective accountability, consistent with the societal objective of encouraging data driven innovation, and that honor the Onward Disclosure Responsibility Principle.

   c. Uses that create definable benefits for individuals, groups, organizations and society that are not counterbalanced by negative consequences to others, and that are based on assessments established by external criteria.

   d. Designated public purposes, including public safety and the identification and preven-

tion of fraud, and in response to an appropriate legal request;

e. Organizations that stand ready to demonstrate why they believe other uses not listed here that are based on assessments established by external criteria are legitimate;

f. Where permitted by law.

5. **Accurate** Data should be accurate and appropriate for all legitimate uses, and that level of accuracy should be maintained throughout the life of the data.

6. **Onward Responsibility** Organizations that originate data should be responsible for assuring the obligations initially associated with the data are maintained when the data is disclosed to third parties. All further onward transfers should also maintain those obligations.

7. **Oversight** Organizations should monitor all uses of data to ascertain that the uses are legitimate, the data is processed fairly, the data is accurately used within the context of the relationship with those to whom the data pertains, and processes that support individual rights and accountable data stewardship are effective and tested. The oversight process, whether conducted by an internal body or an external agent, should be separate from and independent of those persons associated with the processing.

8. **Remediation** Organizations should stand ready to demonstrate the effectiveness of policies, practices and internal oversight to those that have external authority for oversight. Organizations should consider rectifying negative consequences where they reach a level of significant impact to individuals.

The IAF has begun sharing these principles with parties in many locations. It is the IAF's hope that this paper will trigger discussion in Uruguay and Latin America. The purposes of these principles and, hopefully, fourth wave privacy legislation are to preserve a private space for individuals, achieve fair processing for individuals and society more generally, facilitate the fourth industrial revolution, and create greater global interoperability.

SERVIDORES PÚBLICOS:
Privacidad, protección de datos y Redes Sociales

CARLOS ALBERTO
BONNIN ERALES

Es licenciado en Derecho por la Universidad Panamericana, y tiene maestría en Derecho Internacional, por el Instituto Tecnológico y de Estudios Superiores de Monterrey.
Se ha desempeñado en la Comisión Interamericana para el Control del Abuso de Drogas de la Organización de los Estados Americanos; en la Secretaría de Hacienda y Crédito Público; en la Suprema Corte de Justicia de la Nación; en la Fiscalía Especializada para la Atención de Delitos Electorales; en la Secretaría de Salud; en la Procuraduría General de la República, y recientemente en el Senado de la República de México.

SUMARIO

RESUMEN

En el presente trabajo, el autor realiza un pormenorizado recuento de antecedentes en materia de uso de redes sociales y mecanismos de comunicación en México y otros países, y analiza, a través de la discusión de casos de uso, el impacto en los derechos a la protección de datos, a la imagen, y otros derechos, haciendo especial énfasis en el ejercicio público.

SERVIDORES PÚBLICOS: PRIVACIDAD, PROTECCIÓN DE DATOS Y REDES SOCIALES

En 2008, México contaba con 27.6 millones de internautas, 11.3 millones de computadoras con acceso a Internet y 73.6 millones de teléfonos celulares.[1] Este año significó también la entrada de *Facebook* a México;[2] una plataforma que busca formar comunidades digitales en donde se comparten fotografías, historias, noticias y conversaciones. Con el paso del tiempo, y de acuerdo al Estudio sobre los Hábitos de los usuarios de Internet en México, ésta Red Social es la preferida por los mexicanos con un porcentaje del 98% de los usuarios.[3]

Fue también en 2008, que en la Cámara de Diputados de México se discutía una de las seis iniciativas[4] de los proyectos por los cuales se solicitaban la expedición de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. En la exposición de motivos, se expresaba la preocupación por el tránsito del flujo de la información. La protección de los datos personales era necesaria, se afirmó, porque éstos no sólo podían circular "indiscriminadamente, sino porque en ocasiones, desafortunadamente, pueden ser conocidos y utilizados por personas con fines ilícitos, para la comisión de delitos, o simplemente de formas no autorizadas, con evidente perjuicio para sus titulares."[5]

También, en la misma exposición de motivos, se afirmaba que la protección de los datos personales de los individuos no debía depender sólo del poder informativo o del empleo de las nuevas tecnologías de la información, ya que la tecnología debía servir sólo como herramienta para el procesamiento de la información, a la cual también debían imponerse medidas de protección adecuadas y positivas, para el debido tratamiento de los datos personales.[6]

Diez años después, encontramos que las Redes Sociales y la tecnología han posibilitado la apertura de canales de información y comunicación inmediatos; viralizando datos, fotografías y noticias en poco tiempo, y con un amplio espectro de audiencia. En 2018, de acuerdo a la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) del INEGI,[7] México cuenta con 71.3 millones de internautas, de los cuales, el 76.6% utiliza Internet para acceder a sus redes sociales.

El Internet y sus distintas plataformas de socialización de la información han convertido a cada persona en un medio, así afirmaron Maldonado y Riorda, en su libro *Gobernautas* y ciudadanos, en ese contexto se han consolidado canales alternativos de expresión de ideas y opiniones, nuevas intermediaciones mediáticas,

1 *Estudio AMIPCI. Asociación Mexicana de Internet. Hábitos de los usuarios de Internet en México. Mayo de 2009. En: http://archivo.eluniversal.com.mx/graficos/pdf09/amipci.pdf (Consulta 04/07/2018)*

2 *Facebook y sus 61 millones de usuarios en México. Nota de Mario Maldonado en El Financiero. Disponible en: http://www.elfinanciero.com.mx/blogs/historias-de-negoceos/facebook-y-sus-61-millones-de-usuarios-en-mexico.html (Consulta 04/07/2018)*

3 *Hábitos de Usuarios de Internet en México 2018. Estudio de la Asociación de Internet México. En: https://webmarketingtips.mx/local/habitos-usuarios-internet-en-mexico-2018-7-417/ (Consulta 04/07/2018)*

4 *Proyectos de Decretos presentados para expedir la Ley Federal de Protección de Datos Personales en Posesión de Particulares: Septiembre de 2001, Grupo Parlamentario del Partido de la Revolución Democrática. Enero 2005, Grupo Parlamentario de Convergencia. Febrero de 2006, Grupo Parlamentario del Partido Revolucionario Institucional. Marzo de 2006, Grupo Parlamentario del Partido de Acción Nacional. Noviembre de 2008, Grupo Parlamentario de Acción Nacional. Diciembre de 2008, Grupo Parlamentario del Partido Revolucionario Institucional esta última iniciativa fue en la que se basa el DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE PROTECCION DE DATOS PERSONALES EN POSESION DE PARTICULARES, aprobada en el año 2010.*

5 *Gaceta Parlamentaria, Cámara de Diputados, número 2653-VII, jueves 11 de diciembre de 2008. Exposición de motivos- Iniciativa que expide la Ley Federal de Protección de Datos Personales, a cargo del diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI. En: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-VII.html#Ini20081211-1 (Consulta 04/07/2018)*

6 *Exposición de motivos- Iniciativa que expide la Ley Federal de Protección de Datos Personales, a cargo del diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI. Gaceta Parlamentaria, Cámara de Diputados, número 2653-VII, jueves 11 de diciembre de 2008. En: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-VII.html#Ini20081211-1 (Consulta 04/07/2018)*

7 *En México 71.3 millones de usuarios de Internet y 17.4 millones de hogares con conexión a este servicio: ENDUTIH 2017. Comunicado de prensa número 105/18 del 20 de febrero de 2018. INEGI, SCT, IFT. En: http://www.beta.inegi.org.mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf. (Consulta 04/07/2018)*

y la promoción de la agenda ciudadana, desde sus medios.[8]

Las Redes Sociales además de ser utilizadas como plataforma para compartir momentos felices con la familia y amigos, para comunicarnos y conocer de otros, se han convertido también en lugar de denuncia, exposición y debate de ideas. En ellas, la acción del gobierno en turno, las actividades de los actores políticos y los sucesos inmediatos son comentados y debatidos. Son espacios para la organización comunitaria, para empujar temas en la agenda pública, y para movilizar e incidir en la configuración de las decisiones públicas.

Para Riorda y Valenti, los medios sociales son una herramienta innovadora que permite el surgimiento de nuevas formas de organización[9]. En ellas, argumentan, se redefinen y expanden los muros que antes limitaban las organizaciones en lo público o en lo privado. Es una caja que amplia y hace resonar lo que está en las comunidades.

No obstante, estos medios de comunicación de coparticipación colectiva, han levantado riesgos y otros peligros para los usuarios e internautas. La invasión a la privacidad, el robo de información personal para la suplantación y robo de identidad, así como engaños, acoso, noticias falsas, fraudes y extorsiones son algunos de los riesgos que hemos atestiguado.

Ejemplo de ello, es la aplicación *Periscope*, llegada a México en 2015, la cual permite que cada individuo con un teléfono inteligente pueda tener su canal de transmisión en vivo. En 2016, un año después de su llegada, alcanzó más de 200 millones de transmisiones, lo que equivaldría a 110 años de video en vivo.[10] En febrero del mismo año, la Comisión de Derechos Humanos del Distrito Federal (CDHDF) informó que se encontraba revisando tres quejas por presuntas violaciones a los Derechos Humanos, a la seguridad jurídica, a la honra y la protección de la imagen mediante esta aplicación.[11]

Dichas quejas versaban sobre la exhibición de un ciudadano que había realizado conductas que probablemente constituían una falta administrativa, las cuales fueron transmitidas en vivo por parte de un funcionario público de una Delegación de la Ciudad de México. La Comisión de Derechos Humanos de la entidad estableció que con la utilización de la aplicación antes citada, se exponía a las personas a quienes se exhiben a una violencia innecesaria que se constituye en una sanción adicional no prevista en ninguna ley o normatividad, por lo que se vulneran derechos humanos. La CDHDF instó a los servidores públicos que hacían uso de este medio, a cancelar la publicidad de la imagen y datos personales de las personas agraviadas, con la finalidad de evitar que fueran víctimas de violencia en las redes sociales.[12]

Por otro lado, desde el servicio público en Redes Sociales hemos visto también como empleados y servidores de la administración pública son grabados por usuarios, para documentar su actuación y difundirla a través de estas redes. Ya sea para felicitarlos sobre el buen desempeño de sus funciones, o por lo contrario, para mostrar su disgusto o descontento por el servicio prestado.

A nivel internacional, encontramos también ejemplos de que las redes y la tecnología se han posicionado como vía para documentar la acción pública y exponer al ojo ciudadano todo aquello que se considera inadecuado. Una muestra de ello es *Whatsapp*, red social con más de 1.5 billones de usuarios activos a nivel mundial.[13]

En España, más de 25 millones de personas están conectadas en alguna Red Social. Facebook es la red social más utilizada por los españoles por un 87% de la población, al igual que el Whatsapp también con el 87% de la población. Ésta última, es la red mejor valorada por los españoles con un

8 *Maldonado Martín y Mario Riorda (2015) Riorda Mario y Pablo Valenti (201-) Los gobernantes latinoamericanos y la gestión de redes sociales. Banco Interamericano de Desarrollo y Laboratorio de Ideas, nuevas plataformas sociales para el desarrollo. Pág. 40 En: http://gobernauta.org/gobernautas_y_ciudadanos_completo.pdf*

9 *Mario Riorda y Pablo Valenti (2015) Los gobernantes latinoamericanos y la gestión de redes sociales. Banco Interamericano de Desarrollo y Laboratorio de Ideas, nuevas plataformas sociales para el desarrollo. Pág. 8 En: http://gobernauta.org/gobernautas_y_ciudadanos_completo.pdf*

10 *Periscope celebra su primer año en México. Nota del 29 de marzo de 2016, en El Economista, de Notimex. En: https://www.eleconomista.com.mx/tecnologia/Periscope-celebra-su-primer-ano-en-Mexico-20160329-0163.html (Consultado el 11/07/2018)*

11 *CDHDF-Boletín 031/2016 "CDHDF documenta tres quejas por presunta violación de DDHH con utilización de Periscope" del 23 de febrero de 2016. En: http://cdhdfbeta.cdhdf.org.mx/2016/02/cdhdf-documenta-tres-quejas-por-presunta-violacion-de-ddhh-con-utilizacion-de-persicope/ (Consultado el 11/07/2018)*

12 *Ibídem*

13 *WhatsApp news we have been waiting for will transform these popular phones. Express UK 10/07/2018 En: https://www.express.co.uk/life-style/science-technology/986492/WhatsApp-update-Nokia-8810-download (Consulta 10/07/2018)*

8.4 de aprobación, y más de 1:33 horas de uso al día.[14]

Ante ese escenario, donde las Tecnologías de la Información y las Redes Sociales han movilizado billones y billones de datos e información personal, como autoridades y ciudadanos preocupados por la protección de datos, debemos establecer líneas de acción conjuntas para proteger nuestros derechos e información en nuestra interacción cotidiana. En los siguientes párrafos, analizaremos casos que exponen la delgada línea entre comunicarnos en el mundo actual; y la protección a la imagen y privacidad, incluyendo la de los que trabajan en el ejercicio público.

En ese sentido, se trae a colación la resolución R/00778/2018 emitida por la Agencia de Protección de Datos de España. En este caso se estableció que los empleados públicos no debían ser grabados o fotografiados, para luego difundir sus actuaciones en Redes, puesto que, de acuerdo a la Ley Orgánica de Protección de Datos Personales, éstos, aunque funcionarios públicos ejerciendo sus actividades y competencias en un espacio público, debían otorgar su consentimiento previo.

En dicha resolución se da cuenta de un hecho suscitado en la vía pública, en donde la policía local en el desarrollo de sus competencias profesionales atendía un llamado por violencia de género. Ante tales agresiones, un ciudadano realizó grabaciones de la respuesta policial y posteriormente las distribuyó a través de la Red Social de Mensajería *WhatsApp*.

De acuerdo con la policía local, el ciudadano fue advertido de no grabar las imágenes, lo que manifiesta la falta de consentimiento de los servidores públicos, ante el uso de su imagen. No obstante, a ello, el particular afirmó en sus alegaciones que nunca fue informado de esta advertencia. Y que la grabación de la actuación policial, no pretendía beneficio particular, sino que la pensó como herramienta para que la víctima de la agresión, pudiera utilizarla en un juicio posterior.

Aunado a lo anterior, el particular manifestó que la grabación se realizó en la vía pública, y que, si bien no se contaba con un consentimiento manifiesto por parte de los agentes públicos, los hechos ocurridos y la actuación de los sujetos grabados se había dado en el espacio público, y que en ellas intervinieron servidores en el ejercicio de sus competencias, las cuales no debían ser protegidas, ni requerir anonimato.

Así mismo, el particular aseveró que, en ejercicio de su derecho a la libertad de expresión e información, la utilización de los datos personales, es decir, la imagen de los servidores públicos era un elemento imprescindible para la crítica y la información, por lo cual su utilización estaba justificada.

En la resolución, se determinó que las fotografías y grabaciones que daban cuenta de la imagen de los servidores públicos, permitían su identificación, y por ende, debía concluirse la existencia de datos de carácter personal y la plena aplicabilidad de los principios y garantías normadas en la Ley Orgánica de Protección de Datos de Carácter Personal. Por ello, era necesario la aplicación de medidas de actuación que constituyeran el tratamiento debido de los datos personales.

Se resolvió que en virtud de que el particular divulgó a través de *WhatsApp* las imágenes de un miembro de la policía, sin consentimiento del mismo, éste infringió el artículo 6.1 de la Ley Orgánica de Protección de Datos de Carácter Personal, el cual establece que el tratamiento de los datos de carácter personal requiere del consentimiento inequívoco del sujeto propietario de sus datos.

En consecuencia, ante la infracción del artículo 6.1 de la ley antes referida, tipificada como grave en su numeral 44.3.b), se determinó sancionar a quien difundió las imágenes con una multa de 2.000 Euros.

La siguiente tabla comparativa ilustra los artículos de la ley y reglamento de protección de datos personales que aplicó la Agencia de Protección de Datos de España para el caso narrado en supralineas; con los numerales que se podrían aplicar en la misma hipótesis de las leyes expedidas en México.

14 *Cómo se utilizan las redes sociales en España. De Manuel Moreno, consultor y profesor de redes sociales y periodismo 2.0. En: https://www.trecebits.com/2018/06/05/como-se-utilizan-las-redes-sociales-en-espana/ (Consulta 10/07/2018)*

Ley Orgánica de Protección de Datos de Carácter Personal	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Artículo 1: Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.	Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.
Artículo 2.1: Será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.	Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales.
Artículo 3a: Concepto de dato personal cualquier información concerniente a personas físicas identificadas o identificables.	Artículo 3.- Fracción V.- Datos personales: Cualquier información concerniente a una persona física identificada o identificable.
Artículo 3i: i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.	Artículo 3.- Fracción XIX.- Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.
Artículo 6.1: El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga de otra cosa.	Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.
Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal	**Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**
Artículo 5.1 f: Definiciones A los efectos previstos en este reglamento, se entenderá por: f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.	Ámbito objetivo de aplicación Artículo 3. El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales, se requieran plazos o actividades desproporcionadas. En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.
Artículo 5.1 o: Definiciones A los efectos previstos en este reglamento, se entenderá por: o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere	Articulo 2.-Definiciones VIII. Persona física identificable: Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas.
Tratamiento de Datos	
Ley Orgánica de Protección de Datos de Carácter Personal	**Ley Federal de Protección de Datos Personales en Posesión de los Particulares**
Articulo 3c: c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.	Artículo 3.- Para los efectos de esta Ley, se entenderá por: XVIII. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

15

15 *Tabla 1 de elaboración propia para comparar la normativa española y mexicana en materia de protección de datos personales.*

En ese mismo sentido, y coincidentemente a lo resuelto en la resolución R/00778/2018, que el tratamiento de los datos de carácter personal requiere del consentimiento inequívoco del titular de los mismos, y que en virtud de que el particular divulgó a través de WhatsApp las imágenes de un miembro de la policía, sin el consentimiento de éste último, infringiendo la normativa española; en México se tiene, como regla general, que el tratamiento de los datos personales siempre debe llevarse bajo los principios de consentimiento y plena protección de éstos, sin embargo, expondremos resoluciones judiciales que en el caso concreto contienen diferentes criterios resolutivos.

El Quinto Tribunal Colegiado en Materia Penal del Primer Circuito determinó en el Amparo en revisión 141/2015, que "la información contenida en páginas de Internet, constituye un adelanto científico que puede resultar útil como medio probatorio, siempre que para su obtención no se utilicen mecanismos para violar la privacidad de las personas"[16]. Así mismo, se indicó en dicha resolución que el "derecho a la vida privada tiene vinculación con otros derechos, como aquellos respecto de los registros personales y los relacionados con la recopilación e inscripción de información personal en bancos de datos y otros dispositivos, que no pueden ser invadidos sin el consentimiento de su titular".[17]

La Suprema Corte de Justicia de la Nación, estableció en la tesis cuyo rubro dice **"LIBERTAD DE EXPRESIÓN Y DERECHO A LA INFORMACIÓN. SU PROTECCIÓN ES ESPECIALMENTE INTENSA EN MATERIA POLÍTICA Y ASUNTOS DE INTERÉS PÚBLICO"**, que las personas con responsabilidades públicas tienen un umbral distinto de protección, el cual les expone más al escrutinio y a la crítica del público, lo cual se justifica por el carácter de interés público de las actividades que realizan, debido a que se han expuesto voluntariamente a un escrutinio colectivo más exigente y a la posición les da una gran capacidad de reaccionar a la información y las opiniones que se vierten sobre los mismos, lo anterior, se determinó haciendo alusión al informe de la Relatoría Especial para la Libertad de Expresión de la Organización de Estados Americanos del año 2008[18].

Como se puede apreciar en esta interpretación judicial, los servidores públicos tienen un umbral distinto de protección al de los ciudadanos, mismo que las autoridades de protección de datos personales al momento de resolver deben valorar en función del interés público de las actividades que realizan. Ahora bien, los servidores públicos, no obstante que tienen un umbral de protección menor al de los ciudadanos, no pierden toda la protección derivada del derecho al honor incluso cuando no estén actuando en carácter de particulares, pero las implicaciones de esta protección deben ser ponderadas con las que derivan del interés en un debate abierto sobre los asuntos públicos.

Pero, ¿De dónde viene el derecho a la vida privada? ¿Qué antecedentes internacionales nos remiten a entender estas decisiones jurisdiccionales en países distintos? A continuación, hablaremos de fundamentos e instrumentos internacionales para comprender como el derecho a la imagen, al honor y a la intimidad; pueden tener raíces en principios normativos muy profundos.

EL DERECHO A LA IMAGEN, AL HONOR Y A LA INTIMIDAD, RECONOCIDO A NIVEL INTERNACIONAL:

La Declaración Universal de los Derechos Humanos establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[19]

En ese mismo sentido, la Convención Americana sobre los Derechos Humanos protege la honra y la dignidad, señalando que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[20]

16 *Amparo en revisión 141/2015. 18 de septiembre de 2015. Unanimidad de votos. Ponente: Juan Wilfrido Gutiérrez Cruz. Secretaria: Gabriela González Lozano. PRUEBA ILÍCITA. NO LA CONSTITUYE LA OBTENCIÓN DE LA IMPRESIÓN FOTOGRÁFICA DEL PERFIL DEL IMPUTADO EN UNA RED SOCIAL (FACEBOOK) EN CUYAS POLÍTICAS DE PRIVACIDAD SE ESTABLECE QUE AQUÉLLA ES PÚBLICA (LEGISLACIÓN PARA EL DISTRITO FEDERAL). En Gaceta del Semanario Judicial de la Federación 24 de noviembre de 2015, Tomo IV. Pág. 3603. En: https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=2010454&Clase=DetalleTesisBL.(Consulta 10/07/2018)*

17 *Ibídem.*

18 *Semanario Judicial de la Federación y su Gaceta, tomo XXX, diciembre 2009, página 287. LIBERTAD DE EXPRESIÓN Y DERECHO A LA INFORMACIÓN. SU PROTECCION ES ESPECIALMENTE INTENSA EN MATERIA POLÍTICA Y ASUNTOS DE INTERÉS PÚBLICO.*

19 *Declaración Universal de los Derechos Humanos. Artículo 12.*

20 *Convención Americana sobre los Derechos Humanos. Artículo 11.*

De igual manera en el Pacto Internacional de Derechos Civiles y Políticos, numeral 17 a la letra dice:

> *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
>
> *2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

Lo anterior da cuenta de un principio normativo fundamental para nosotros, nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación y toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Por otro lado, destacamos que la libertad de expresión, recogida en el artículo 13 de la Convención Americana, es proclive a colisionar con otros derechos fundamentales, como el derecho a la intimidad, al honor, al prestigio, así como con el principio de inocencia. Esta colisión de derechos, posee rasgos particulares cuando la expresión se vale de los medios sociales de comunicación, con el enorme alcance que éstos tienen, el poder que significan y el impacto que pueden tener en la vida de las personas, en la integridad y preservación de sus bienes jurídicos.

Cuando no ha sido posible evitar la colisión de derechos, es preciso proveer un acto de autoridad que corrija este choque, exija la responsabilidad consiguiente e imponga las medidas que deriven de ésta. Es en este ámbito donde surge la necesidad de identificar los intereses merecedores de tutela, valorar su jerarquía en el orden democrático y seleccionar los medios adecuados para protegerlos. [21]

CUANDO LA LIBERTAD DE EXPRESIÓN Y EL DERECHO A LA PROTECCIÓN DE DATOS, SE ENCUENTRAN EN EL EJERCICIO PÚBLICO:

Cuando de libertad de expresión hablamos, resulta indispensable abordar el término "umbral de protección" al honor, reputación, intimidad y vida privada. En ese tenor Muñoz Díaz, en su libro *Libertad de Expresión: Límites y Restricciones* apuntó:

> *"El "umbral de protección" al honor, reputación, intimidad y vida privada, debe ser determinado en razón del titular de los derechos de la personalidad, esto es, si la persona que pretende respeto y protección -y que por ende limitará la libertad de expresión- debe de contar con ellos de manera amplia o debe ser limitado de acuerdo a sus funciones o importancia en la sociedad en que se desarrolla"*[22]

En ese sentido, encontramos que el umbral de protección de un particular no será el mismo que el de un servidor público, debido a la relevancia social que implica la investidura del cargo.

En relación a lo anterior, es importante mencionar que tal como afirma Muñoz Díaz, la libertad de expresión parte fundamental del Derecho a la Información, incluye la difusión de los hechos, sucesos o acontecimientos de la realidad.[23] De tal forma que, en esta prerrogativa, tenemos que las y los ciudadanos tienen derecho a difundir de forma libre la información, a transmitirla y acceder a ella.

Coincidimos con las aseveraciones de Muñoz Díaz en el sentido de que, ante la sociedad los servidores públicos asumen, además de su competencias y atribuciones, una carga adicional a la de conducirse con valores éticos dentro de la sociedad, en gran medida debido a que sus ingresos, son remunerados por el Estado, con la contribución tributaria de los ciudadanos. Dicha carga adicional, se extiende a la conducta y proceder dentro y fuera de su lugar de trabajo. En ese sentido, su actuar debe ser proba y honesta, lo cual se extrapola a su esfera privada[24].

A partir de ello, se estima que el umbral de protección de la vida privada, honor y reputación de los servidores públicos, contará con mayores limitaciones, y contrariamente a la ciudadanía, la protección de los datos de los empleados públicos estará sujeta a ciertas restricciones y principios.

Ante este enunciado, es importante traer a colación, un caso que nos ejemplifica lo anterior. Resuelto por la Convención América sobre los Derechos Humanos, en *Herrera Ulloa Vs. Costa Rica*, emitida el 2 de julio de 2004, se determinó que el límite del derecho a la información es el derecho a la intimidad, el cual únicamente cede frente a la libertad de información, cuando se trate de una figura pública y se refiera a actos públicos de esta figura.

Indudablemente e idealmente, los servidores públicos están sujetos al escrutinio y seguimiento

21 *Corte Interamericana de Derechos Humanos Caso Herrera Ulloa Vs. Costa Rica Sentencia de 2 de julio de 2004 http://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf (Consultada el 11/07/2018)*

22 *Pablo Francisco Muñoz Díaz (2016) Libertad de Expresión: Límites y Restricciones. Pág. 109*

23 *Ibídem Pág. 110*

24 *Ibídem Pág. 110*

del ojo de la ciudadanía. En el contexto actual, es necesario que las y los ciudadanos puedan y deban tener un control completo y eficaz de la forma en que se conducen los asuntos públicos. Por ello, es imprescindible operar con mayor tolerancia a la crítica. No obstante, no puede dejarse de lado el hecho de que la protección de la privacidad y de la reputación de los que ejercen sus competencias en el ejercicio público, difiere a la que se otorga a un ciudadano. Ante ello, se destaca la distinción entre la intimidad y la vida privada, "los actos de los funcionarios públicos vinculados con la vida privada [...] sí [son] objeto de información en razón de que generarían un interés público, los actos de la intimidad no".

Ahora bien, regresando a la normativa española tenemos que el derecho a la imagen es garantizado y protegido por el Estado, cuando ésta podría vulnerar su esfera íntima o familiar. La Constitución de España en su artículo 18° establece que las y los ciudadanos, tienen derecho al honor, a la intimidad personal y familiar, y a la propia imagen. Así mismo, se determina que el Estado limitará el uso de la informática para garantizar el honor de los individuos, su intimidad personal y familiar, así como el pleno ejercicio de sus derechos.[25]

De tal modo, como López Carballo afirma, el uso leal de los datos personales sólo puede alcanzarse a través de la implementación y acatamiento de los principios de transparencia y consentimiento, así como, la creación de procedimientos de tutela y seguridad de la información personal.[26] En ese tenor, en la Constitución Política Mexicana,[27] también se regula lo siguiente: Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

A su vez, la Constitución Mexicana garantiza que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros.

Por otro lado, en México la Suprema Corte de Justicia se ha pronunciado por los derechos del hombre como son los concernientes al honor, a la intimidad y a la propia imagen que constituyen derechos subjetivos del ser humano, en tanto que son inseparables de su titular, quien nace con ellos, y el Estado debe reconocerlos.[28]

Como bien puede pensarse, las redes sociales han sido materia de pronunciamiento de uno de los tres poderes de la Unión del estado Mexicano, (Poder Judicial), en el cual se ha dicho que al afectarse a los derechos de honor y reputación por la divulgación en internet de datos que no fueron autorizados por el afectado, o bien, no se contaba con su consentimiento, debe garantizarse su adecuada protección acudiendo a la aplicación del principio *pro personae* establecido en el artículo 1° de la Constitución Política Mexicana.[29]

---

25 *Constitución Española. Título I. De los derechos y deberes fundamentales. Capítulo segundo. Derechos y libertades. Sección 1.ª De los derechos fundamentales y de las libertades públicas.*
Artículo 18
1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
(...)
2. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
En: http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2 (Consulta 04/07/2018)

26 *López, Carballo Daniel (2014) Protección de datos y habeas data: una visión desde Iberoamérica. En: https://www.researchgate.net/publication/278966698_Proteccion_de_datos_personales_y_habeas_data_Una_vision_desde_Iberoamerica Pág. 15 (Consulta 04/07/2018)*

27 *Constitución Política Mexicana artículo 16, párrafos primero y segundo.*

28 *Semanario Judicial de la Federación y su Gaceta Libro XXI, junio de 2013, Tomo 2 Pág. 1258. Número de Registro 2003844. "DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN. CONSTITUYEN DERECHOS HUMANOS QUE SE PROTEGEN A TRAVÉS DEL ACTUAL MARCO CONSTITUCIONAL.*

29 *Semanario Judicial de la Federación y su Gaceta Tomo XX. Mayo de 2013 Pág.1770. Número de Registro 2003546. "DERECHOS AL HONOR Y A LA REPUTACIÓN. PROTECCIÓN ADECUADA TRATÁNDOSE DE INFORMACIÓN DIVULGADA A TRAVÉS DE INTERNET, QUE CAUSA UN DAÑO MORAL.*

Por lo que respecta a la privacidad de quienes realizan, han realizado o desean realizar responsabilidades públicas, la Corte mexicana se ha pronunciado en el sentido de que sus pretensiones en términos de intimidad, tienen que ser con menos resistencia normativa general que la de los ciudadanos, debido al tipo de actividad que han decidido desempeñar, debiendo estar expuestos al escrutinio público en sus actividades, y no obstante que tienen derecho a la intimidad y al honor, las implicaciones de esta protección deben ser ponderadas con las que derivan del interés en un debate abierto sobre los asuntos públicos.[30]

Ante lo anterior, podemos decir que en los servidores públicos debe aplicarse un umbral diferente de protección respecto de su intimidad. Este umbral de protección si bien es menor al de los ciudadanos ordinarios, no debe olvidarse que mantienen la protección derivada de este derecho, misma que, debe ponderarse en virtud del interés público que conllevan las actividades o actos que realizan ya sea en su esfera pública, como en la privada.

Documentar el buen ejercicio público es fundamental para dar cuenta de la responsabilidad y cumplimiento de atribuciones de los servidores públicos. Sin olvidar, que a pesar de que la ciudadanía puede ejercer su derecho a la libertad de expresión, y que gracias a las tecnologías puede convertirse en un canal emisor de comunicación, estas nuevas dinámicas de involucramiento y transmisión de ideas, deben siempre estar basadas en la protección del derecho propio y ajeno. Saber que, aunque tengamos la mejor intención al publicar, denunciar y exponer conductas que consideramos inadecuadas, siempre debemos dejar espacio para el desarrollo pleno de la individualidad y los derechos del otro, como en el caso español.

Los órganos garantes de protección de datos personales, tienen una gran tarea en sus manos, cuando existe choque de derechos entre la libertad de expresión con el derecho a la vida privada, al honor e imagen, surgirán indudablemente las siguientes interrogantes:

¿Las autoridades tendrían que analizar caso por caso?, ¿Los órganos garantes del derecho de protección de datos personales estarán obligados a identificar los intereses merecedores de tutela?, ¿Se tendría que realizar una valoración de la jerarquía de los derechos en el orden democrático y seleccionar los medios adecuados para protegerlos?

BIBLIOGRAFÍA Y DOCUMENTOS CONSULTADOS:

Muñoz Díaz, Pablo Francisco (2016) Libertad de Expresión: Límites y Restricciones. Pág. 109

López, Carballo Daniel (2014) Protección de datos y habeas data: una visión desde Iberoamérica. En:

https://www.researchgate.net/publication/278966698_Proteccion_de_datos_personales_y_habeas_data_Una_vision_desde_Iberoamerica Pág. 15

Riorda Mario y Pablo Valenti (2015) Los gobernantes latinoamericanos y la gestión de redes sociales. Banco Interamericano de Desarrollo y Laboratorio de Ideas, nuevas plataformas sociales para el desarrollo. En:

http://gobernauta.org/gobernautas_y_ciudadanos_completo.pdf Pág. 8

ESTUDIOS:

Estudio AMIPCI. Asociación Mexicana de Internet. Hábitos de los usuarios de Internet en México. Mayo de 2009. En: http://archivo.eluniversal.com.mx/graficos/pdf09/amipci.pdf

Hábitos de Usuarios de Internet en México 2018. Estudio de la Asociación de Internet México. En: https://webmarketingtips.mx/local/habitos-usuarios-internet-en-mexico-2018-7-417/

COMUNICADOS, BOLETINES Y NOTAS PERIODÍSTICAS:

CDHDF-Boletín 031/2016 "CDHDF documenta tres quejas por presunta violación de DDHH con utilización de Periscope" del 23 de febrero de 2016. En: http://cdhdfbeta.cdhdf.org.mx/2016/02/cdhdf-documenta-tres-quejas-por-presunta-violacion-de-ddhh-con-utilizacion-de-persicope/ (Consultado el 11/07/2018)

En México 71.3 millones de usuarios de Internet y 17.4 millones de hogares con conexión a este servicio: ENDUTIH 2017. Comunicado de prensa número 105/18 del 20 de febrero de 2018. INEGI, SCT, IFT. En: http://www.beta.inegi.org.

30 *Semanario Judicial de la Federación y su Gaceta Tomo XXX. Diciembre de 2009 Pág. 278. Número de Registro 165820 DERECHOS AL HONOR Y A LA PRIVACIDAD. SU RESISTENCIA FRENTE A INSTANCIAS DE EJERCICIO DE LA LIBERTAD DE EXPRESIÓN Y EL DERECHO A LA INFORMACIÓN ES MENOR CUANDO SUS TITULARES TIENEN RESPONSABILIDADES PÚBLICAS. Amparo directo en revisión 2044/2008. 17 de junio de 2009. Cinco votos. Ponente: José Ramón Cossío Díaz. Secretarios: Francisca María Pou Giménez y Roberto Lara Chagoyán.*

mx/contenidos/saladeprensa/boletines/2018/OtrTemEcon/ENDUTIH2018_02.pdf

Facebook y sus 61 millones de usuarios en México. Nota de Mario Maldonado en El Financiero. Disponible en: http://www.elfinanciero.com.mx/blogs/historias-de-negoceos/facebook-y-sus-61-millones-de-usuarios-en-mexico.html

Periscope celebra su primer año en México. Nota del 29 de marzo de 2016, en El Economista, de Notimex. En: https://www.eleconomista.com.mx/tecnologia/Periscope-celebra-su-primer-ano-en-Mexico-20160329-0163.html

WhatsApp news we have been waiting for will transform these popular phones. Express UK 10/07/2018 En: https://www.express.co.uk/life-style/science-technology/986492/WhatsApp-update-Nokia-8810-download

Cómo se utilizan las redes sociales en España. De Manuel Moreno, consultor y profesor de redes sociales y periodismo 2.0. En: https://www.trecebits.com/2018/06/05/como-se-utilizan-las-redes-sociales-en-espana/

LEGISLACIÓN Y JURISPRUDENCIA:

Constitución Política de los Estados Unidos Mexicanos, artículo 16, párrafos primero y segundo.

Constitución Española. Título I. De los derechos y deberes fundamentales. Capítulo segundo. Derechos y libertades.

Convención Americana sobre los Derechos Humanos. Artículo 11.

Corte Interamericana de Derechos Humanos Caso Herrera Ulloa Vs. Costa Rica Sentencia de 2 de julio de 2004 http://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf

Declaración Universal de los Derechos Humanos. Artículo 12.

Gaceta Parlamentaria, Cámara de Diputados, número 2653-VII, jueves 11 de diciembre de 2008. Exposición de motivos- Iniciativa que expide la Ley Federal de Protección de Datos Personales, a cargo del diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI. En: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-VII.html#Ini20081211-1

Exposición de motivos- Iniciativa que expide la Ley Federal de Protección de Datos Personales, a cargo del diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI. Gaceta Parlamentaria, Cámara de Diputados, número 2653-VII, jueves 11 de diciembre de 2008. En: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-VII.html#Ini20081211-1

Amparo en revisión 141/2015. 18 de septiembre de 2015. Unanimidad de votos. Ponente: Juan Wilfrido Gutiérrez Cruz. Secretaria: Gabriela González Lozano. PRUEBA ILÍCITA. NO LA CONSTITUYE LA OBTENCIÓN DE LA IMPRESIÓN FOTOGRÁFICA DEL PERFIL DEL IMPUTADO EN UNA RED SOCIAL (FACEBOOK) EN CUYAS POLÍTICAS DE PRIVACIDAD SE ESTABLECE QUE AQUÉLLA ES PÚBLICA (LEGISLACIÓN PARA EL DISTRITO FEDERAL). En Gaceta del Semanario Judicial de la Federación 24 de noviembre de 2015, Tomo IV. Pág. 3603. En: https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=2010454&Clase=DetalleTesisBL

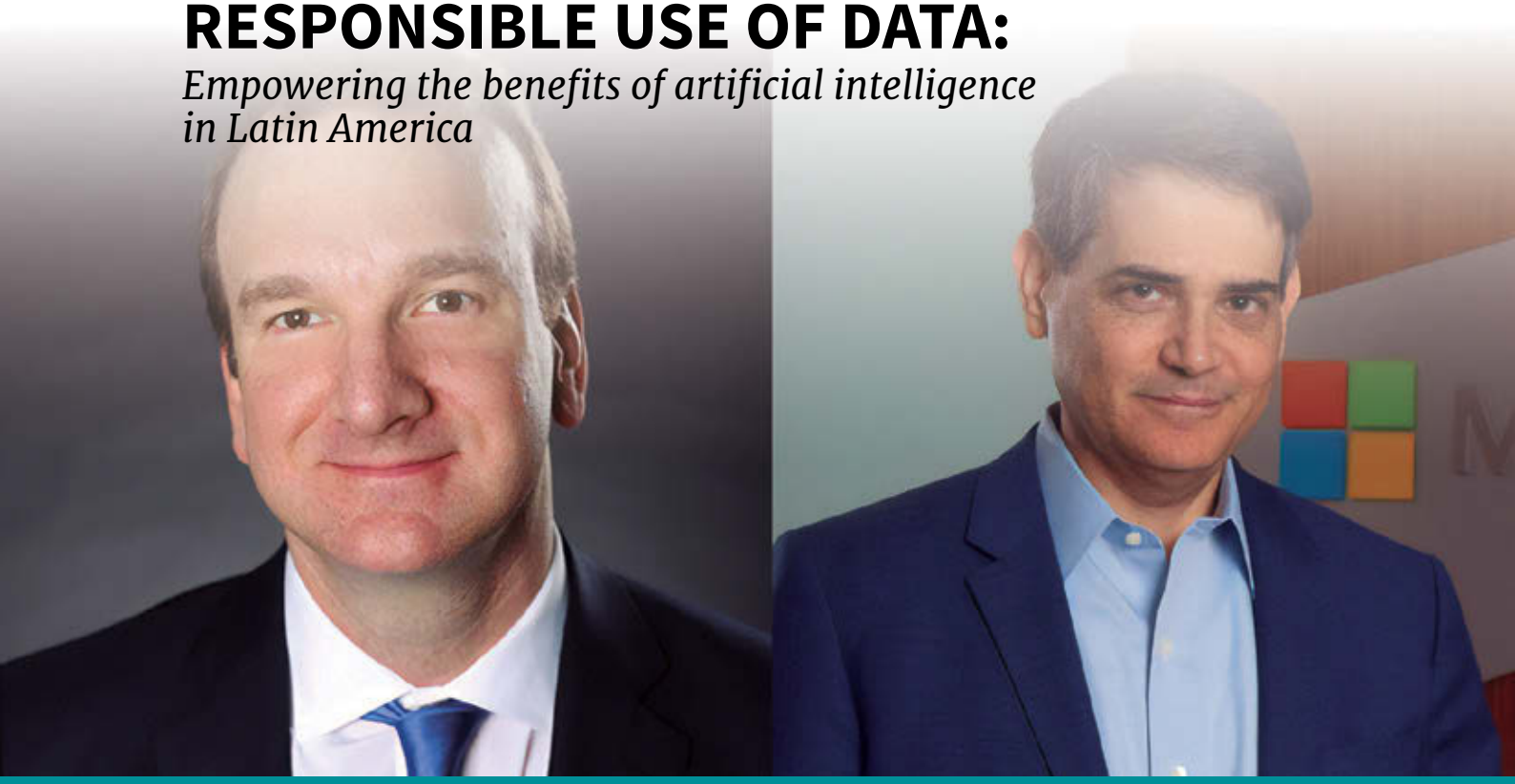
Semanario Judicial de la Federación y su Gaceta Libro XXI, junio de 2013, Tomo 2 Pág. 1258. Número de Registro 2003844. "DERECHOS AL HONOR, A LA INTIMIDAD Y A LA PROPIA IMAGEN. CONSTITUYEN DERECHOS HUMANOS QUE SE PROTEGEN A TRAVÉS DEL ACTUAL MARCO CONSTITUCIONAL.

Semanario Judicial de la Federación y su Gaceta Tomo XX. Mayo de 2013 Pág.1770. Número de Registro 2003546. "DERECHOS AL HONOR Y A LA REPUTACIÓN. PROTECCIÓN ADECUADA TRATÁNDOSE DE INFORMACIÓN DIVULGADA A TRAVÉS DE INTERNET, QUE CAUSA UN DAÑO MORAL.

Semanario Judicial de la Federación y su Gaceta Tomo XXX. Diciembre de 2009 Pág. 278. Número de Registro 165820 DERECHOS AL HONOR Y A LA PRIVACIDAD. SU RESISTENCIA FRENTE A INSTANCIAS DE EJERCICIO DE LA LIBERTAD DE EXPRESIÓN Y EL DERECHO A LA INFORMACIÓN ES MENOR CUANDO SUS TITULARES TIENEN RESPONSABILIDADES PÚBLICAS. Amparo directo en revisión 2044/2008. 17 de junio de 2009. Cinco votos. Ponente: José Ramón Cossío Díaz. Secretarios: Francisca María Pou Giménez y Roberto Lara Chagoyán.

RESPONSIBLE USE OF DATA:

Empowering the benefits of artificial intelligence in Latin America



GEFF
BROWN

Es abogado senior en el equipo de Asuntos Regulatorios de Microsoft en Washington, Estados Unidos. Ha asesorado en cuestiones de privacidad para varios grupos de productos de Microsoft, incluyendo "Business Productivity Online Suite", "Microsoft HealthVault", "Microsoft Office", "Windows 7" y "Xbox". Brinda además apoyo al Grupo de Políticas y Estrategias Avanzadas de Microsoft. Previamente, fue desarrollador de software para la primera versión de "Microsoft Exchange". Es profesional de privacidad certificado y miembro de la Asociación Internacional de Profesionales de la Privacidad (IAPP).

DANIEL
KORN

Es Director de Asuntos Corporativos de Microsoft Latinoamérica. Recibió su B.M. violín de la Escuela Juilliard, B.A. magna cum laude de la Universidad de Yale, Juris Doctor de la "University of Virginia Law School", y abogado (Reválida) de la Universidad de Buenos Aires. Previamente, trabajó como abogado en estudios jurídicos de Estados Unidos y la Argentina. Es co-autor del artículo "Facilitando The Cloud: La Regulación de la Protección de Datos como Motor de la Competitividad Nacional en América Latina," publicado por la Inter-American Law Review de la University of Miami School of Law. También es co-autor del artículo "Computación en Nube: La Reconversión del Espacio en Red" publicado por el Banco Interamericano de Desarrollo (BID) en su revista Integración & Comercio.

SUMARIO

RESUMEN

En el presente artículo los autores analizan distintas legislaciones en las que se regulan distintos aspectos de la protección de datos que impactan en el desarrollo de la inteligencia artificial. Asimismo, se consideran casos de estudio vinculados a la temática y se presentan sus potenciales beneficios.

Farmers are using machines with artificial intelligence (AI) to provide insights which were practically unavailable before to help them improve yields, reduce waste, lower costs, and reduce adverse environmental impacts. Educators are using AI to detect how different individual students learn in order to provide personalized lesson plans for each of them. Cities are using AI to provide better emergency medical care to more people and to improve provision of other citizen services.[1]

But can machines think?

Progress toward thinking machines has picked up dramatically in recent years for several reasons such as massive growth in computing power, the exponential proliferation of digitalized data and digital devices, and advances in the capacity of algorithms capable of processing vast quantities of data. These have all helped fuel the enthusiasm and innovation that characterize AI development today while at the same time requiring more attention about how companies use data.[2]

In fact, macro-economic data also evidences that AI is coming of age. Businesses invested an estimated $26 to $39 billion on AI for their internal use in 2016.[3] By 2021, annual worldwide spending on AI systems is forecast to reach $57.6 billion.[4] *Spending* on AI, however, is easily dwarfed by the expected benefits from the use of AI. Analysts predict that AI usage could drive global economic growth of between $7.1 and $13.17 trillion over the next eight years.[5]

AI could also help drive economic growth in Latin America specifically. Indeed, experts at Accenture predict that by 2035, AI could add $432 billion to the Brazilian economy, $78 billion to the Colombian economy, $63 billion to the Chilean economy, $59 billion to the Argentinian economy, and $43 billion to the Peruvian economy.[6]

Broadly speaking, we must address the need for increased connectivity, the evolution of laws, strong ethical principles, training for new skills and even labor market reforms.[7] In this article, we focus on a key set of questions that involve the use of data in AI systems, and whether such data is being used responsibly. This concept of responsible data use has several dimensions—it includes ensuring that the data which is used to train AI algorithms does not incorporate hidden biases; that AI development and use respects people's privacy and handles data securely; that data-driven AI systems are inclusive; and that people are given sufficient information to understand how AI systems use their data and affect them.

These are complex issues, and it is important that policymakers around the world are thinking about them. As governments in Latin America consider these issues, it will be key to focus on local perspectives and local requirements, such that the policy frameworks policymakers design going forward are especially geared to the unique needs of citizens, economies, and cultures.

To ensure that applicable regulatory frameworks promote responsible data use, while also ensuring that consumers, workers, and organizations reap the full benefits of AI, governments have the opportunity to establish balanced rules that protect personal privacy and data security on the one hand, but that also facilitate socially and economically beneficial uses of data on the other. In connection with this effort, policymakers in Latin America could be guided in their work on these issues by three key principles:

1 *See Microsoft, The Future Computed: Artificial Intelligence and its Role in Society, at 46, 48 (2018), available at https://blogs.microsoft.com/uploads/2018/02/The-Future-Computed_2.8.18.pdf [hereinafter The Future Computed].*

2 *See Steve Guggenheimer, AI and the New Generation of Software Building Blocks, VISUAL STUDIO - STEVE "GUGGS" GUGGENHEIMER'S BLOG (May 7, 2018), available at https://blogs.msdn.microsoft.com/stevengu/2018/05/07/ai-and-the-new-software-building-blocks/.*

3 *See McKinsey Global Institute, Artificial Intelligence: The Next Digital Frontier?, at 9-10 (June 2017), available at (https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.*

4 *See International Data Corporation, IDC Spending Guide Forecasts Worldwide Spending on Cognitive and Artificial Intelligence Systems to Reach $57.6 Billion in 2021 (Sept. 25, 2017), available at https://www.idc.com/getdoc.jsp?containerId=prUS43095417.*

5 *See McKinsey Global Institute, Disruptive technologies: Advances that will transform life, business, and the global economy (May 2013), available at http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.*

6 *See Armen Ovanessoff and Eduardo Plastino, Como A Intêligencia Artificial Pode Acelerado Crescimento Da América Do Sul, at 17-21 (2017) available at https://www.accenture.com/t00010101T000000Z__w__/br-pt/_acnmedia/PDF-49/Accenture-AI-America-do-Sul.pdfla=pt-BR.*

7 *See The Future Computed, supra n. 3, at 90-134.*

- Avoiding rigid rules or one-size-fits-all mandates, especially as regards AI transparency requirements, and instead advance pragmatic, context-aware regulatory regimes for promoting responsible data use in AI,
- Adopting rules that are appropriate for the region's unique context and perspectives and taking care not to reflexively adopt regulatory frameworks from other jurisdictions that might not be compatible with local circumstances, and
- Focusing on the concept of accountability as a cornerstone for regulation in this area.

Part I of this article reflects on the context of digital transformation sweeping the globe and various foundational efforts that governments in Latin America are undertaking in response to this digital transformation. Part II explores various beneficial applications of AI for economic and social advancement. Part III offers recommendations in responsible data use as AI continues to develop and policymakers consider adoption of regulatory frameworks.

DATA PROTECTION IN THE ERA OF DIGITAL TRANSFORMATION

Advancements in the key building blocks of computing in the past few decades—specifically, in computing power, storage, and networks (CSN)—have driven a wave of digital transformation that is impacting every business and industry, from Fortune 1000 organizations to two-person shops.[8] Advances in cloud computing, falling prices for data storage, the surge in connected digital sensors and devices, and increasingly sophisticated data analytics technologies have enabled enterprises across the world, in this so-called "Fourth Industrial Revolution," to capitalize on the benefits of digitization. Analysts estimate that data-enabled efficiency gains could add almost $15 trillion to global GDP by 2030.[9]

Governments across Latin America are responding to this digital transformation by updating laws to encourage the swift and responsible adoption of these technologies, including through data protection laws, adoption of international standards, the promotion of nationwide "digital strategies," and through initiatives prioritizing the use of cloud services in government.

Adoption of Data Protection Laws. This article is written on the 10th Anniversary of Uruguay's Law of Personal Data Protection and Habeas Data Right of Action (No. 18.331/2008) that received an adequacy determination from the European Commission on Aug. 21, 2012. Argentina also adopted an EU-style law and received an adequacy determination from the European Commission in 2003.[10] Argentina's National Directorate for the Protection of Personal Data is now drafting a Personal Data Law that would modify and update the existing legislation,[11] but the initiative is still under development within the Executive branch and has not yet been presented to the National Congress. Since the passage of Uruguay's and Argentina's laws, several governments in Latin America have also passed data protection laws. The substance of these laws varies. While Uruguay and Argentina's laws broadly align with the 1995 European Union (EU) Data Protection Directive[12] —on issues such as the use and cross border transfer of data, requirements for data subject consent before processing, data subject access and correction rights, and data security—the data protection laws of other countries in the region are less aligned with the Directive.[13] Mexico, for example, has in place data privacy legislation that embraces data protection principles of the Asia Pacific Economic Cooperation forum. The Mexican legislation, adopted in 2010, is more flexible with regard to international data transfers and consent requirements as compared to EU-style legislation, although guidelines on privacy notices that went into effect in 2013 require data controllers similar to rules in the EU to provide sufficient notice and obtain consent before personal data is collected using cookies, web beacons, or other automated means.[14] Mexico adopted additional legislation, effective as of January 27, 2017, to regulate the processing of personal information by public institutions (General Law on Protection of Personal Data Held by Public Institutions).[15] Remarkably, this law allows public institutions to process personal information in the cloud (by essentially replicating the provisions of

8 *See Guggenheimer, supra n. 4.*

9 *See BSA, What's the Big Deal With Data?, at 14 (Oct. 2015), available at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf.*

10 *Law No. 25326, Oct. 30, 2000, (Arg.).*

11 *See Anteproyecto de Ley de Datos Personales, www.jus.gob.ar/media/3223892/anteproyecto_mayo2017.pdf*

12 *Horacio E. Gutiérrez and Daniel Korn, Facilitando the Cloud: Data Protection Regulation as Driver of National Competitiveness in Latin America, 45 INTER-AMERICAN LAW REVIEW 33, 36 (2013).*

13 *See id. at 36-37.*

14 *See id. at 38.*

15 *Ley General De Protección de Datos Personales en Posesión de Sujetos Obligados, Camara de Diputados Del H. Congreso de la Unión (Jan. 26, 2017), available at https://www.colmex.mx/assets/pdfs/10-LGPDPPSO_57.pdf?1493134086.*

the Regulations to the data privacy law applicable to private parties). Similarly, the new General Law on Public Archives enacted on June 15, 2018 (which will become effective on June 15, 2019), also allows the processing of public archives in the cloud.[16]

Just this month, Brazil's Senate passed Brazil's first Data Protection Bill, which had already been passed in the House. Among other things, the Bill creates a Data Protection Authority. The President of Brazil, who has line-item veto power over the Bill, must sign it before it can become effective.[17]

Adoption of International Standards. Uruguay's data protection authority, Unidad Reguladora y de Control de Datos Personales (URCDP), is a notable leader in promoting ISO 27018, an international standard for privacy in cloud services. Introduced in 2014, ISO 27018 provides detailed guidance for protecting personal data by requiring cloud service providers to comply with six key principles: control, consent, transparency, communication, disclosure, and compliance. ISO 27018 thereby promotes strong protections for customer data and helps foster trust in cloud services.[18] Within Latin America, Uruguay was the first government in the region to promote the standard on a government website especially to small and medium-sized businesses (SMEs) seeking cloud service providers, by noting that using the standard could lead to greater confidence in providers of cloud services.[19] Chile (2015), Costa Rica (2016), Uruguay (2016), and Mexico (2016) have now formally adopted ISO 27018 as a national standard.[20] Argentina's national standards body, IRAM, lists the adoption of ISO 27018 in its study plan for 2018.[21]

To make digital technologies more accessible to people with disabilities, Mexico's National Standards Bureau of the Ministry of Economy recently announced a public consultation on the adoption of a Mexican accessibility standard.[22] The standard is based on European Accessibility Standard EN 301 549, which establishes public sector procurement requirements for "websites, electronic devices, software, mobile apps and other digital technologies [to be] free of barriers that could prevent people with disabilities from making full use of the technologies."[23]

Adoption of National Digital Strategies. Notwithstanding the advances digitization has brought about thus far, the "digitization of everything" is still only beginning; realizing the potential it holds will still take time.[24] Fortunately, this means that a "window of opportunity" exists for both developed and developing countries, which affords them time to adapt suitable policies and institutions, ideally based on an individualized assessment of structural factors that account for the impact of new technologies different in different countries.[25]

In Latin America, the majority of countries seem to have recognized this potential, with 73% having developed some form of national digital strategy.[26] Uruguay's "Agenda Digital Uruguay 2020"

16 *La Ley General de Archivos (June 15, 2018), available at http://dof.gob.mx/nota_detalle.php?codigo=5526593&fecha=15/06/2018.*

17 *See Pedro Ozores, Brazil congress approves data protection bill, BNA AMERICAS (Jul. 10, 2018), available at https://www.bnamericas.com/en/news/ict/brazil-congress-approves-data-protection-bill/.*

18 *Daniel Korn, First to adopt international security standard for the cloud, TRINIDAD AND TOBAGO NEWSDAY (May 21, 2015), at 5.*

19 *See Informe: Norma ISO/IEC Nº 27.018, Unidad Reguladora y de Control de Datos Personales (June 16, 2015), available at https://datospersonales.gub.uy/inicio/institucional/noticias/informe+norma+iso.*

20 *See Tecnología de la información - Técnicas de seguridad - Código de práctica para la protección de la información personal de identificación (PII) en nubes públicas que desempeñen el rol de procesadores de PII, Instituto Nacional de Normalización, at http://ecommerce.inn.cl/Ficha_Producto/?p=NCh-ISO27018:2015 (regarding Chile's adoption); Tecnología de la información. Técnicas de seguridad. Código de prácticas para la protección de la información de identificación personal (IIP) en nubes públicas en calidad de procesadores IIP, Inteco, at https://www.inteco.org/shop?search=27018 (regarding Costa Rica's adoption); Declaratoria de Vigencia de la Norma Mexicana NMX-I-27018-NYCE-2016, Tecnologías de la Información-Técnicas de Seguridad-Código de Práctica Para la Protección de Datos Personales (DP) Para Proveedores de Servicios de Nubes Públicas, Diario Oficial de la Federación (Aug. 26, 2018), available at http://dof.gob.mx/nota_detalle.php?codigo=5449891&fecha=26/08/2016 (regarding Mexico's adoption); Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de Información para Identificación Personal (IIP) en nubes públicas actuando como procesadores IIP, Instituto Uruguayo de Normas Técnicas (Dec. 2016), at http://www.unit.org.uy/normalizacion/norma/100000820/ (regarding Uruguay's adoption).*

21 *See Plan de Estudio, Instituto Argentino de Normalización y Certificación 93 (2018), available at http://site.iram.org.ar/sites/iram-org-ar/publico/PlanEstudio2018.pdf.*

22 *See publication in Mexico's Diario Oficial de la Federación: www.dof.gob.mx/nota_detalle.php?codigo=5526425&fecha=14/06/2018 http://www.dof.gob.mx/nota_detalle.php?codigo=5526425&fecha=14/06/2018.*

23 *EN 301 549: The Standard for Digital Accessibility in Europe, Essential Accessibility (June 22, 2018), at https://www.essentialaccessibility.com/blog/en-301-549/.*

24 *Antje Uhlig et. al, Technological Innovation and the Future of Work: A View From the South, G20 Policy Brief (June 19, 2018), at http://www.g20-insights.org/policy_briefs/technological-innovation-and-the-future-of-work-a-view-from-the-south/.*

25 *See id.*

26 *See Organization for Economic Cooperation and Development, Government at a Glance: Latin America and the Caribbean 2017, at 126 (2016), available at http://www.oecd.org/gov/government-at-a-glance-latin-america-and-the-caribbean-2017-9789264265554-en.htm.*

(ADU)—a multi-stakeholder agreement among representatives of government, academia, the private sector, and civil society—is one example, which has been heralded as a leading tech success story for Latin America.[27] Broadly, the ADU's objective is to promote an information society focused on development, in which all stakeholders are able to use and share information and knowledge.[28] The ADU focuses on social inclusion, citizen participation, state transformation, and promotion of education.[29] Chile's "Agenda Digital 2020" serves as another model. Launched in 2015, it aims to create a knowledge economy in Chile, expand technology access and use among the population, and pave the way for 10% of the Chilean GDP to be derived from the information and communications technology sector by 2020.[30] As the President of Chile summarized at the III CEO Summit of the Americas in April 2018,

> *"We have a chance we've never had before. We were late for the Industrial Revolution, and that is why we are where we are, but now there is a revolution much more powerful, broad, and which will change our lives and will generate opportunities such as no one suspected until very recently. And this knowledge and information society, this technological revolution, is generous with the countries that embrace it, take it and take advantage of it, but it has proved to be indifferent or even cruel to the countries that turn their backs on it or just let it pass."*[31]

In addition, both Mexico and Brazil have developed national digital strategies. Mexico adopted its digital strategy in 2014 and modified it in 2016[32], while Brazil adopted its digital strategy in 2018.[33] Ecuador is also developing a National Digital Strategy, which is currently in public consultation.[34]

Promoting Cloud Use in Government. Costa Rica, Mexico, Chile, and Argentina have adopted specific "cloud first" policies promoting a preference for the adoption of cloud technologies by their respective public sectors,[35] citing such benefits as cited by Chile's "cloud-first" Presidential Directive dated February 19th, 2018 as follows:

- ***Cost Reduction.*** Initial capital investments are eliminated related to server infrastructure, storage and licenses, as well as maintenance costs (repairs and technical operations staff, among others). These are replaced by variable costs that are paid for based on when and how much service is required.
- ***Scalability.*** Allows for services to be contracted only as required and in the amount required, avoiding the acquisition of infrastructure and licenses and giving the Administration greater adaptability based on its concrete needs.
- ***Flexibility.*** The institution may select public, private or hybrid storage options. It may also select from a menu the tools it needs to implement a project, as well as the level of security (encryption) that its information requires.
- ***Efficiency.*** Allows institutions to develop projects in less time, without having to make major investments in equipment, implementation and configuration.

27 *Digital Agenda in Uruguay, Centre for Public Impact (Mar. 18, 2016), available at https://www.centreforpublicimpact.org/case-study/digital-agenda-uruguay/.*

28 *See id.*

29 *See id.*

30 *See Digital Government in Chile: Strengthening the Institutional and Governance Framework, Organization for Economic Co-operation and Development, at 62 (2016), available at https://chile.gob.cl/ocde/site/artic/20170804/asocfile/20170804210854/estudio_gobierno_digital_en_chile.pdf.*

31 *Free translation from the original Spanish: Presidente Piñera participa del Panel de Clausura de la III Cumbre Empresarial de las Américas, Gobierno de Chile (Apr. 13, 2018), at https://prensa.presidencia.cl/discurso.aspx?id=73235.*

32 *See ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, Diario Oficial de la Federación (Feb. 2, 2016), available at https://www.gob.mx/cms/uploads/attachment/file/59534/MAAGTICSI_compilado_04_02_2016.pdf.*

33 *See Estratégia Brasileira Para a Transformação Digital, E-Digital (2018), at http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf.*

34 *See Ecuador's Plan de la Sociedad de la Información y del Conocimiento, at https://plansociedadinformacion.mintel.gob.ec/*

35 *See Directriz No. 46-H-MICITT, La Presidenta de la República y Los Ministros de Hacienda y el de Ciencia, Tecnología y Telecomunicaciones (Costa Rica cloud first policy); ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, Diario Oficial de la Federación (May 8, 2014) (Mexico cloud first policy); Instructivo Presidencial que Entrega Directrices Sobre la Evaluación y Adopción Preferente de Servicios en la Nube por Parte de los Órganos de la Administración Central del Estado, GAB.PRES No. 001 (Feb. 19, 2018) (Chile cloud first policy); and Decálogo Tecnológico, Versión 1.0.2: Lineamientos y mejores prácticas para elaborar requerimientos de soluciones de tecnologías de la información y comunicación en el Estado, Ministerio de Modernización, available at https://www.argentina.gob.ar/onti-2/decalogo-tecnologico (Argentina cloud-first policy).*

- ***Ubiquity.*** Cloud application users will be able to access applications from any place through a connected device as long as they have Internet access.
- ***Availability of Contingent Environments.*** The cloud is an ideal infrastructure that provides easy access to required backups.[36]

These and other efforts by policymakers in Latin America to respond to transformational advancements in digital technology are a promising sign. They demonstrate an understanding of the linkage between technology adoption and economic growth/improvements in national competitiveness, and the role that pro-innovation regulatory policies can play in achieving these benefits.

ARTIFICIAL INTELLIGENCE: BENEFITS AND CASE STUDIES

Powered by massive growth in the volume of available data, AI is playing an essential role in the digital transformation sweeping the globe. While conceptions of AI vary, at Microsoft, we think of AI as a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do.[37]

As noted in Part I, growth in cloud computing, the availability of data at scale, and advanced algorithms are powering the development of increasingly sophisticated AI technologies.[38] Cloud computing provides developers and researchers with access to the building blocks necessary to create and scale AI tools and models and to process the vast amounts of data needed to improve AI algorithms. Indeed, the rate at which data is produced doubles every two years,[39] and by 2021, global IP traffic will reach 3.3 zettabytes per year—over three trillion gigabytes of data.[40] The quantity of data is increasing exponentially, with no end in sight.

Among the key benefits of AI is that machines can help turn this deluge of raw information and often disparate datasets into insights and knowledge, patterns and connections that would otherwise be invisible to humans, which can then help drive better decision-making and more effective action in support of our communities. The staggering amount of data the world produces today can only advance progress if society has the tools to make sense and use of that data. AI provides society with such tools. The "computational intelligence" that AI provides can assist humans in almost any field where intelligence itself has a role to play.[41]

AI offers incredible opportunities to drive broad economic and social progress. But we must keep humans in the loop. Microsoft aims to develop AI in order to augment human abilities, especially our unique ingenuity. The goal is to combine the capabilities of computers with human capabilities to enable people to achieve more.[42]

Using the building blocks described above, technologists are developing software applications and devices that can see, hear, understand, and reason.[43] The unique capabilities of AI tools are almost infinite, but core AI technologies include:

- ***Vision:*** the ability of computers to "see" by recognizing what is in a picture or video,
- ***Speech:*** the ability of computers to "listen" by understanding the words that people say and to transcribe them into text,
- ***Language:*** the ability of computers to "comprehend" the meaning of the words, taking into account the many nuances and complexities of language, and
- ***Knowledge:*** the ability of computers to "reason" by understanding the relationship between people, things, places, and events.[44]

With these vision, speech, language, and knowledge capabilities in the relatively short timeframe within which AI technologies have evolved, at least four patterns have emerged that illustrate the key ways in which businesses are combining, developing, and applying core AI technologies to improve their operations and become more competitive—through virtual agents, ambient intelligence, assisting professionals, and autonomous systems.[45]

36 *See, e.g., Instructivo Presidencial que Entrega Directrices Sobre la Evaluación y Adopción Preferente de Servicios en la Nube por Parte de los Órganos de la Administración Central del Estado, GAB.PRES No. 001 (Feb. 19, 2018), at 2.*

37 *See The Future Computed, supra n. 3, at 28.*

38 *See Guggenheimer, supra n. 4.*

39 *See BSA, What's the Big Deal With Data?, at 7 (Oct. 2015), available at http://data.bsa.org/wp-content/uploads/2015/10/bsadatastudy_en.pdf.*

40 *Cisco, Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper (May 2015), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.*

41 *See The Future Computed, supra n. 3, at 35.*

42 *See id.*

43 *See id. at 29.*

44 *See id.*

45 *See generally Steve Guggenheimer, Emerging AI Patterns, VISUAL STUDIO - STEVE "GUGGS" GUGGENHEIMER'S*

- ***Virtual Agents:*** This AI can interact with employees, customers, partners, or others on a company's behalf by answering questions, providing support or information and, over time, becoming proactive representatives of the business.[46] Companies such as Hewlett Packard (HP) and Macy's have deployed virtual agents built on core Microsoft AI technologies with significant success. HP, for instance, uses virtual agents to handle approximately 70% of customer support requests; these agents maintain an 85% accurate dialogue rate. Macy's uses virtual agents for functions such as product promotions and alerts, thereby helping Macy's customers receive more relevant and personalized information.[47]
- ***Ambient Intelligence:*** In this case, sensors in physical space are used to create a digital environment where people, objects, and activities can be detected and tracked.[48] A warehouse for example that can detect a person walking in one aisle on a collision course with a forklift driving in another aisle, the AI can prevent the pending accident.[49] In the case of fire emergencies, ambient intelligence can be used to track who is in a building, who has left, and if anyone is still inside.[50] In manufacturing and construction, ambient intelligence can flag when a worker may be going to pick up an item that is too heavy, or to help locate a lost item.[51]
- ***AI Assisting Professionals:*** Since AI can be used to accomplish repetitive and routine tasks, this AI frees up professionals to focus their efforts on non-routine tasks that require uniquely human ingenuity and skills to resolve. For instance, AI can assist attorneys in contract analysis with machine reading tools that review regular contractual provisions and surface potential issues.[52] Researchers at the University of São Paulo in Brazil are developing AI technology that, during outbreaks of dengue, zika, or chikungunya, will identify which disease a patient is most likely to have based on that patient's basic health profile. The AI-developed initial diagnosis in this case will assist overloaded doctors in triaging patients during health crises.[53] As another example, Microsoft's AI solution Project InnerEye uses AI technology originally developed for gameplay to help oncologists increase the number of medical images they can scan, leading to better outcomes in cancer detection and treatment.[54] While the task of "delineating" scans was previously manual, slow, and error prone, InnerEye will accomplish the same task in a fraction of that time while giving oncologists full control over the accuracy of the final delineation.[55]
- ***Autonomous Systems:*** Finally, businesses can extract great value from AI by relying on autonomous systems for purposes such as bolstering cybersecurity.[56] Because machine learning is so effective at detecting patterns in vast amounts of data, it can be used to quickly identify cyberattacks in real-time and then further used to find the most effective approach for stopping and remediating such attacks.[57]

These are just some of the ways in which AI applications are helping organizations become more efficient, productive, and innovative. In other areas, AI tools are helping manufacturers forecast fluctuations in customer demand more accurately, which they can use to run operations and manage supply chains more efficiently and effectively.[58] Manufacturers and logistics firms also are using AI to better identify areas of waste, automate certain processes faster and more easily, maintain equipment more predictably, and dynamically realign production to meet changing customer tastes and needs.[59] In Peru, for instance, Chazki (known as the Peruvian "Uber of Logistics") has used AI to

BLOG (May 7, 2018), at https://blogs.msdn.microsoft.com/stevengu/2018/05/24/emerging-ai-patterns/.

46 *See id.*

47 *See id.*

48 *See id.*

49 *See id.*

50 *See id.*

51 *See id.*

52 *See id.*

53 *See Ovanessoff and Plastino, supra n. 8, at 17.*

54 *See The Future Computed, supra n. 3, at 36.*

55 *See id. at 37. See id. at 37.*

56 *See Guggenheimer, supra n. 47.*

57 *See id.*

58 *U.S. National Science and Technology Council and Networking and Information Technology Research and Development Subcommittee, National Artificial Intelligence Research and Development Strategic Plan, at 8 (Oct. 2016), available at https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.*

59 *Microsoft, The next-generation manufacturer: How to transform into a digital business, at 9 (2017), available at https://enterprise.microsoft.com/en-us/articles/industries/discrete-manufacturing/the-next-generation-manufacturer-how-to-transform-into-a-digital-business/.*

develop new postal maps of hard-to-reach places, opening up new distribution opportunities for electronic retailers.[60] In Chile, copper mining giant Codelco has become a global pioneer in the adoption of autonomous trucks and automated decision-making to streamline operations.[61] AI can also help companies design faster and more environmentally-friendly production processes that increase worker productivity, improve product quality, lower costs, and better protect worker health.[62]

Businesses across the economy are also using AI to improve customer service and engagement. AI technologies can collect and analyze data from multiple sources—including direct customer interactions, product performance monitoring, and social networks—to produce fresh insights into market behavior and customer preferences, which can be used to improve customer satisfaction and deepen customer engagement across the product lifecycle.[63] Argentinian marketing firm Jampp, for instance, uses an AI-based system to generate predictions about customer purchasing behavior, which helps Jampp's enterprise customers empower their online marketing.[64]

AI technologies are also helping businesses expand computing into the physical world, fundamentally transforming how we interact with the space around us. The ambient intelligence discussed above is one manifestation of this; another is autonomous vehicles. Others are using these technologies to generate entirely new services and lines of business. For example ThyssenKrupp Elevator, a leading global elevator provider, worked with Microsoft to create an intelligent monitoring system based on digitally connected sensors that enable technicians to use real-time data to identify a needed repair before a breakdown happens.[65] ThyssenKrupp was able both to revamp its own maintenance operations and to develop a service that it then began offering to other elevator operators.[66]

Organizations across the world have a choice: they either participate fully in this digital transformation, or risk being left behind. Fortunately, many Microsoft customers in Latin America are already taking full advantage of AI and related digital technologies. For example:

- ***inConcert,*** a leading contact center technology company founded in Uruguay and now in more than 25 countries worldwide, uses Microsoft AI to power highly-customizable chatbots that it offers customers. InConcert's chatbot technology relies on Microsoft Azure's Natural Language Understanding, which enables the bot to accurately extract the intention behind a phrase and better understand the customer's requirements, thereby reducing the risk of customer frustration,[67]
- ***Fracttal,*** an IoT provider based in Santiago, Chile, used Microsoft Azure Machine Learning to develop (i) a conversational bot prototype that handles support orders, as well as (ii) modeling software that predicts system failures. After switching to these AI tools and other Microsoft cloud-based services, Fracttal grew tenfold in the span of two years and sees its Microsoft-based AI strategy as an "unquestionable success,"[68]
- ***Fast Shop,*** a Brazilian retailer, implemented a solution based on Microsoft's Cortana Intelligence Suite that provides the company with real-time insights it can use to optimize pricing and customer engagement. For instance, Fast Shop was able to more accurately predict air conditioner sales following a five-degree increase in temperature and the results of a ten-percent discount on products. The company was also able to create new customer service virtual agents,[69] and
- ***Patrus Transportes Urgentes,*** a leading Brazilian cargo transportation firm, recently migrated several aspects of its operations to the Microsoft Azure cloud platform.[70] One result

60 *See Ovanessoff and Plastino, supra n. 8, at 21.*

61 *See id. at 19.*

62 *See Microsoft, supra n. 61, at 5.*

63 *See id.*

64 *See Ovanessoff and Plastino, supra n. 8, at 20.*

65 *See The Internet of Things gives the world's cities a major lift, MICROSOFT CUSTOMER STORIES (Dec. 21, 2014), available at https://customers.microsoft.com/en-us/story/the-internet-of-things-gives-the-worlds-cities-a-major.*

66 *See id.*

67 *See e.g., Omnichannel Contact Center: Chatbot, inConcert, at https://inconcertcc.com/en/products-new/omnichannel-contact-center/chatbot.html.*

68 *See Empresa chilena de IoT reporta crecimiento 10 veces mayor al optimizar manejo de PostgreSQL con soluciones Azure, MICROSOFT CUSTOMER STORIES (Dec. 26, 2017), at http://customers.microsoft.com/en-us/story/fracttal-professional-services-azure-database-postgre-sql-azure-machine-learning-chile.*

69 *See Brazilian retailer stands out from the crowd with data analytics platform, MICROSOFT CUSTOMER STORIES (Jul. 17, 2017), available at https://customers.microsoft.com/en-us/story/fast-shop.*

70 *See Microsoft, Patrus Transportes Case Study (Jan. 26, 2018), available at http://customers.microsoft.com/en-us/story/patrus-azure.*

of this migration was to allow Patrus employees to keep track of hundreds of thousands of cargo shipments using barcode readers on their smartphones, which connected directly to the company's back-office system in the cloud. This also enabled the company to automate its management of bills of lading, thus saving the company significant time and money.[71]

RESPONSIBLE DATA USE AND THE ROLE OF REGULATION

As the preceding case studies reflect, AI and related technologies hold tremendous promise for businesses and communities across Latin America. Realizing their full potential, however, will require more than just innovations in technology. It also will require innovations in policy. A core set of policy questions with regard to AI is ensuring that data is used responsibly. This is an area where governments in Latin America have an opportunity to be global leaders, and indeed innovators, able to adapt new law to the most recent changes in AI technology.

By way of background, there are several dimensions to the responsible use of data in AI. First, AI systems typically require access to enormous amounts of data in order to "train" (i.e., develop) the algorithms that power them. Experience shows that significant care must be taken in selecting this data to ensure that it does not incorporate hidden biases, and that it does not generate results that (unwittingly) discriminate against certain classes of people or otherwise treat people unfairly.[72]

Second, AI services often use or process data that may be personal (e.g., voice commands, emails, photos, etc.), or uniquely sensitive (e.g., about ethnicity, religious affiliation, etc.). It is therefore important that AI systems collect and process such data in ways that respect fundamental notions of privacy, and that they handle such data securely.

Third, depending on how they are developed and deployed, certain AI applications can have important impacts on people's lives. In those cases, people should be given sufficient information to understand how the applications use their data and how the outputs of such applications affect them.

Microsoft is giving a great deal of thought to the use of data in AI systems—in particular, what it means to use data "responsibly" and how we can engineer our processes, systems and tools to promote responsible data use.

Further to discussions both internally and with customers and partners, as well as evaluating AI systems in practice, Microsoft has identified six principles that can be helpful to policymakers looking to promote responsible data use. "It's a start, but it's not the entire answer," as Brad Smith, President of Microsoft has said, since "AI is a journey that the entire world is on" and this will require a global conversation.[73] To that end, we believe data used in connection with the development or deployment of AI systems should be handled in ways that are fair, reliable and safe, private and secure, inclusive, transparent, and accountable, as follows:[74]

- ***Fairness.*** Data should be used in a manner that treats people fairly and does not treat similarly situated groups of people differently. Without careful planning, AI systems can operate unfairly because they are designed by human beings (who have unconscious biases), and the systems are trained using data that reflect the imperfect world we live in.[75]

---

71 *Id.*

72 *Access to AI can present more of a challenge for SMEs. SMEs may not, for example, have access to the large, high-quality datasets required for training AI and can therefore find themselves at a competitive disadvantage with large global technology companies that either can purchase data more easily or are large enough to generate their own data. See Government response to House of Lords Artificial Intelligence Select Committee's Report on AI in the UK: Ready, Willing and Able, UK House of Lords Select Committee on Artificial Intelligence 8 (June 2018), available at https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response.pdf.*
In addition, since approximately half of the region's population still lacks internet connectivity, the related but separate issue of online access to data in Latin America merits close attention. Microsoft has undertaken projects to address this problem by, for example, launching its Airband Initiative which seeks to expand connectivity by leveraging underutilized broadcast spectrum for wireless online connectivity on an unlicensed basis. This issue is also seeing some attention from policymakers. Colombia, for example, was the first country in Latin America to publish spectrum regulations to enable internet connectivity via underutilized broadcast spectrum with pilot programs in the rural areas of Caldas and Mesetas. See Antonio García Zaballos and Enrique Iglesias Rodríguez, Cloud Computing Opportunities and Challenges for Sustainable Economic Development in Latin America and the Caribbean, Inter-American Development Bank, at 9-12 (2018), available at https://publications.iadb.org/bitstream/handle/11319/8864/Cloud-Computing-Opportunities-and-Challenges-for-Sustainable-Economic-Development-in-Latin-America-and-the-Caribbean.pdf?sequence=1&isAllowed=y.

73 *Brad Smith, East meets West: The world must come together to establish ethical standards for AI. LinkedIn (July 13, 2018).*

74 *See The Future Computed, supra n. 3, at 57.*

75 *See id. at 58-59.*

- ***Reliability and Safety.*** Using data responsibly also requires that it be used in technology that performs reliably, safely, and consistently. Securing AI systems requires the ability to identify abnormal behaviors and prevent manipulation of the system by malicious actors.[76]
- ***Privacy and Security.*** Privacy rules for AI should take into account the type of data and the context in which it is used.[77] To help reduce the risk of privacy intrusions, governments should support industry efforts to develop techniques that enable systems to use personal data without accessing or knowing the identities of individuals.[78]
- ***Inclusiveness.*** AI technologies should benefit and empower everyone and address a broad range of human needs and experiences. One dimension of this is that the way data is used in AI systems should account for the context, needs, and expectations of the people who use them.[79]
- ***Transparency.*** Particularly where AI systems significantly impact people's lives – such as the application of sentencing guidelines for criminal defendants[80] and its use in hiring decisions[81] – those impacted by them should be able to understand how they operate. To that end, explanations of how these systems work and interact with data should be made available. Providing this information can make it easier to identify instances of potential bias, errors, or unintended outcomes.[82]
- ***Accountability.*** As described in more detail below, the people who design and implement AI systems must be accountable for how those AI systems operate.[83]

In Microsoft's view, adherence to these principles is critical to building public trust and confidence in AI. We also view them as useful guideposts for governments. As policymakers in Latin America consider how best to promote responsible data use in the context of AI, they could find it empowering to imbue their decision-making and actions with these principles, but also to take into account three specific points that we think have particular significance for the region:

Adopt policies that are context-aware about algorithmic transparency requirements

Retaining an understanding of how AI systems produce results will remain an important objective moving forward. As Henry Kissinger recently observed, if AI's computational power continues to compound rapidly, AI may soon be able to optimize situations that are different from how humans would optimize them, but may not be able to explain why its actions are optimal.[84] Bearing these potential challenges in mind, when considering whether and how to regulate the use of data in AI systems, policymakers will best serve the interests of their community if they take a pragmatic approach that is sensitive to the surrounding context. As the examples throughout this article illustrate, the term "artificial intelligence" covers a diverse array of technologies that can be applied in an almost infinite range of scenarios. These scenarios vary tremendously in their potential impacts on people.

For instance, an AI algorithm that recommends words as a user types text on a phone does not raise the same degree of transparency issues as an AI algorithm that informs employment or criminal sentencing decisions. In the case of employment or criminal sentencing decisions, people will have legitimate interests in an explanation for the AI result i.e. understanding how the AI system processes their data; as opposed to the case of recommended words for a user typing text on a phone, where any such AI transparency interests pale by comparison. Likewise, an AI algorithm that processes an employee's name in a company directory does not raise nearly the same privacy concerns as one that processes such information in the context of adoption records.[85] Furthermore, processing even sensitive information (*e.g.*, health records) will in some cases be appropriate, for instance when seeking to prevent the epidemic spread of contagious diseases.

The UK Government recently acknowledged this reality. Specifically with respect to AI's application to health, the UK government explained that the likely benefits that would accrue to pa-

76 *See id. at 63.*

77 *See id. at 66.*

78 *See id. at 78.*

79 *See id at 69.*

80 *See, e.g., Julia Angwin et al., Machine Bias, ProPublica (May 23, 2016), available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.*

81 *See, e.g., The Future Computed, supra n. 3 at 59.*

82 *See id.*

83 *See id at 73.*

84 *See Henry Kissinger, How the Enlightenment Ends, THE ATLANTIC (June 2018), available at https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.*

85 *See id. at 79.*

tients and providers must be "carefully weigh[ed] against the requirement for transparency,"[86] noting that over-emphasis on transparency could deter the use of AI, and thus deny patients access to an important component of their care. More broadly, the UK government cautioned that an overemphasis on transparency could be a deterrent to improved health outcomes and therefore must be balanced against the positive impacts AI can offer.[87]

In short, context is critical in evaluating the need for transparency in the responsible use of data in AI systems. Rigid, one-size-fits-all transparency requirements that ignore context, by contrast, risk stifling AI innovation and depriving consumers and businesses of the full potential benefits that AI offers. When evaluating issues relating to responsible data use, policymakers in Latin America could be among the first-movers on context-aware transparency requirements.

Incorporate unique national needs and perspectives

An increasing number of jurisdictions across the globe are considering new rules, or adaptations to existing rules, to address the policy issues raised by AI. These efforts are helpful to policymakers in Latin America in that they can provide useful models to be considered. As policymakers in Latin America consider these models, however, it is important that they bring their own perspectives to bear and that they select a path that is appropriate to their nation's own characteristics, economy, and culture.

For instance, as noted in Part I, several governments in Latin America have adopted data protection rules modeled on the 1995 EU Data Protection Directive. For those who may be looking to develop data protection rules to align more closely with the EU's newly issued General Data Protection Regulation (GDPR), it is important to recognize GDPR's original design for an economy, legal culture and society that differs in many respects from those in Latin America. For instance, EU Member States participate in a single market that provides for the free cross-border movement of people, goods, and services. All EU Member States also are subject to the EU political institutions and are governed by several treaties that bind all of them. A detailed, technical regulatory framework for personal data, as embodied in the GDPR, in many ways reflects those EU market characteristics.

Latin America, by contrast, consists of several different markets that, although interdependent, are also governed separately and in which SMEs play a relatively large role. SMEs which employ approximately 67% of the workforce in Latin America,[88] might find it much more burdensome to comply than companies in the EU with a GDPR-like framework that could unduly burden small companies without additional guidance on how to apply such a framework in the context of developing technology. At the same time, the complexity of GDPR's specifics might inadvertently constrain the relatively smaller economies of Latin America by practically representing a greater barrier to growth than in a single, large economy like the EU.

More importantly, to the extent foreign models regulate the use of data, regulatory frameworks from other regions might fail to align with the current economic and social realities in Latin America in ways that could impede AI innovation and use. These may include regulations restricting cross-border transfers of data (either through express prohibitions or mandates to store or process data locally), heightened liability standards for AI, or regulations imposing prescriptive consent requirements since development of modern AI depends on broad access to massive data sets to train algorithms. Even where such regulatory efforts are well-intentioned, they risk stunting the growth of AI if they are not carefully tailored to the region's unique context and needs.

Focus on accountability

Finally, in considering policies for responsible data use, policymakers in Latin America could give special consideration to the concept of accountability. In many cases, the best way to promote responsible data use effectively but flexibly is to hold those who design and deploy AI systems accountable for their effects.[89] Accountability regimes in other contexts—such as healthcare and privacy—can provide useful guidance on how to establish norms for responsible data use in AI. Those who develop and use AI systems should work to adhere to these norms and conduct periodic assessments to determine whether they are working effectively.[90] Such an approach can incentivize AI developers to build privacy or data security safeguards

86 *Government response to House of Lords Artificial Intelligence Select Committee's Report on AI in the UK: Ready, Willing and Able?, UK Secretary of State for Business, Energy and Industrial Strategy 12 (June 2018), available at https://www.parliament.uk/documents/lords-committees/Artificial-Intelligence/AI-Government-Response.pdf.*

87 *See id.*

88 *See Gutiérrez and Korn, supra n. 14, at 39.*

89 *The Future Computed, supra n. 3, at 73.*

90 *See id.*

into their AI systems at the outset in ways that are best suited to the particular product or service being created.

Microsoft's own AI and Ethics in Engineering and Research (AETHER) Committee provides an illuminating example of how organizations can proactively build accountability into their AI development and deployment processes. AETHER is an organization within the company that includes senior leaders from across Microsoft's engineering, research, consulting and legal organizations. Its task is to formulate internal policies and potential responses to specific AI-related issues as they arise. AETHER considers and defines best practices, provides guiding principles to be used in the development and deployment of Microsoft's AI services, and helps resolve questions related to ethical and society implications stemming from Microsoft's AI activities.[91]

As AI develops and its use across society expands, we anticipate that the concept of accountability will play an important part in guiding both private-sector action and public-sector responses to policy challenges.

CONCLUSION

AI technology holds tremendous promise for economies and societies across Latin America. To realize this promise, however, it is critical that innovations in technology are supported by innovations in policy. Policymakers in Latin America have an exciting opportunity to lead on responsible data use while this is still a new frontier; with a good starting point being context-aware transparency requirements, a focus on Latin America's unique market realities, and prioritizing accountability. With this framework, governments in the region could best position their citizens to reap the full benefits of this transformative technology.

91 *See id. at 74.*

ANTEPROYECTO DE REFORMA DE LA LEY

de protección de datos personales en Argentina.

EDUARDO
CIMATO

Es el Director Nacional de Protección de Datos Personales en la Agencia de Acceso a la Información Pública de Argentina. Es abogado de la Universidad de Buenos Aires, con posgrado en el Programa de Especialización en Derecho Bancario y Financiero de la Universidad Austral y maestría en Derecho e Integración Económica en E.P.O.C.A – Universidad del Salvador (tesis pendiente). Fue Asesor Jurídico en la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, Asesor Jurídico del Presidente del Banco de la Provincia de Buenos Aires, Síndico Titular en diferentes empresas del Grupo Banco Provincia y abogado contencioso en el Banco Patagonia S.A. de Argentina.

SUMARIO

RESUMEN

En el presente artículo el autor detalla el proceso llevado adelante para la elaboración del Anteproyecto de reforma de la ley de protección de datos personales de Argentina. Se destaca el proceso de reflexión y de consensos necesarios para dicha elaboración y se realiza además un análisis de los principales cambios que se proponen con respecto a la Ley vigente, en línea con las más modernas tendencias en la materia de protección de datos personales a nivel global.

ANTECEDENTES

La protección de los datos personales se encuentra implícitamente garantizada en Argentina a través de la acción de habeas data prevista en el artículo 43, tercer párrafo de la Constitución Nacional, acción que fuera incorporada en la reforma constitucional del año 1994. Años más tarde, se sancionó la Ley N° 25.326 de protección de datos personales, una norma de orden público que regula los principios aplicables en la materia, así como también el procedimiento de la acción de habeas data.

La Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos, fue la autoridad argentina de protección de datos personales, por consiguiente responsable de garantizar la privacidad de la información a nivel nacional, de conformidad con la Ley Nº 25.326. A partir de septiembre de 2017, la Agencia de Acceso a la Información Pública, entidad autárquica con autonomía funcional y financiera dentro del ámbito de Jefatura de Gabinete de Ministros, se convierte en la autoridad argentina de protección de datos personales (Decreto Nº 746/2017 y Nº 899 / 2017). Como resultado de este cambio legislativo, la autoridad de protección de datos ha ganado independencia, un elemento clave para la protección de los datos personales de acuerdo con los estándares internacionales.

PROYECTO LEY NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.

Resulta una obviedad resaltar los cambios tecnológicos que han tenido lugar durante los últimos diecisiete años a partir de la promulgación de la Ley Argentina de Protección de Datos Personales junto con el nuevo contexto legal internacional, principalmente con la promulgación del Reglamento de Protección de Datos de la UE (GDPR (EU) 2016/679), regulación que recientemente se ha convertido en ejecutable, han llevado a la Autoridad Argentina de Protección de Datos a elaborar en 2016 un proyecto de ley para reformar la ley actual, en el marco del programa "Justicia 2020", creado por el Ministerio de Justicia y Derechos Humanos, en un esquema de elaboración participativa en la que incluyo una amplia aportación federal, se gestó un anteproyecto de reforma a la ley argentina de protección de datos personales. Fue un proceso de reflexión y discusión de los distintos aspectos de la legislación Argentina vigente, que estuvo abierto a todo ciudadano interesado en la materia, donde se realizaron reuniones de trabajo con diferentes actores, provenientes del sector privado, académico y de la sociedad civil[1].

En este proceso de reflexión, se discutieron distintos aspectos de la legislación vigente y se escucharon propuestas de modificaciones a la Ley N° 25.326. Además se debatió acerca de la importancia de adecuar la legislación a los estándares internacionales en materia de protección de datos personales, tanto de los provenientes del Reglamento (UE) 2016/679 como de otros estándares internacionales[2].

En el mencionado proceso, uno de los temas más controvertidos fue el del consentimiento del titular de los datos, destacándose la necesidad de flexibilizar el concepto debido a los avances de la tecnología ya que, actualmente se producen transacciones de datos personales al utilizarse los servicios y productos que brinda internet, tornándose engorroso la necesidad de esperar que las personas reciban y procesen las solicitudes otorgando su consentimiento. Frente a esta evidente problemática, se sugirió ante una eventual reforma de la ley, un consentimiento transparente pero implícito y se restrinja el requerimiento del consentimiento explícito a ciertas situaciones, como ser, cuando se traten datos sensibles.

Un tema en el que hubo consenso generalizado, fue el de la necesidad de que se adopte un sistema de responsabilidad demostrada (o proactiva) a la ley argentina sobre protección de datos, por el cual los responsables que realicen tratamiento de datos se encuentren obligados a demostrar el cumplimiento de la ley, abandonándose de esta manera la registración de bases de datos, conforme tendencia internacional.

Culminado el proceso participativo, la DNPDP elaboro un anteproyecto de ley, en el que no sólo se tomaron en cuenta los comentarios vertidos

1 *https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf*

2 *Se sugirieron seguir los siguientes modelos, entre ellos, el APEC Privacy Framework y el APEC Cross Border Privacy Rules (CBPR) system, Acuerdo Transpacífico de Cooperación Económica.*

en el proceso de reflexión, sino también las regulaciones existentes a nivel internacional específicas en la materia, como el Reglamento (UE) 2016/679, el Convenio del Consejo de Europa para la Protección de la Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y el Convenio sobre Ciberdelincuencia (Convención de Budapest). Se tomó como referencia legislación comparada sancionada en los último años, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, La Ley de Protección de Datos Personales N° 29.733 de Perú, la Ley Estatutaria 1581 de 2012 de Colombia y sus respectivas reglamentaciones y la Ley de Protección de Información Personal y Documentos Electrónicos de Canadá (Personal Information Protection and Electronic Documents Act – PIPEDA), entre otras. Principalmente se tuvo en consideración el Anteproyecto de Estándares de Protección de Datos Personales para los Estados Iberoamericanos (aprobado por la Red Iberoamericana de Protección de Datos Personales –RIPDPP- en junio de 2017) y el informe del Comité Jurídico Interamericano sobre Privacidad y Protección de Datos Personales.

Culminada esta etapa, el anteproyecto fue sometido a discusión pública, nuevamente en el marco de la plataforma "Justicia 2020", recibiéndose comentarios y sugerencias sobre el texto que se había elaborado.

CAMBIOS DESTACABLES DEL ANTEPROYECTO.

Uno de los factores principales que indujeron a la DNPDP a activar el proceso de reforma de la ley vigente, fue la necesidad de que Argentina continúe siendo un país con legislación adecuada conforme los lineamientos del nuevo Reglamento (UE) 2016/679.

El anteproyecto recepta aquellos aspectos que pueden considerarse esenciales del Reglamento, pero presenta ciertas diferencias que responden al contexto argentino. Para ello se tomaron como referencia los 17 años de experiencia de la entonces Dirección Nacional de Protección de Datos Personales, jurisprudencia local en la materia y legislación comparada.

Los principales cambios que se proponen, son:

- El anteproyecto sigue los lineamientos más modernos en materia de protección de datos, entendiendo que la normativa se aplicará en distintos supuestos, aun cuando bajo ciertos supuestos, los responsables de tratar los datos no se encuentren en territorio nacional.
- El eje central pasa a ser el dato personal objeto de tratamiento, y no las bases de datos, como ocurre con la ley vigente.
- Se dispone que la aplicación de la ley no podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión. Específicamente, en relación al derecho de supresión, el anteproyecto aclara que este derecho no procederá cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información.
- Se incorpora el principio de responsabilidad demostrada. Al receptar este principio, se abandona la obligación de registro de bases de datos, imposición que la experiencia de la DNPDP ha demostrado no mejorar la protección de la privacidad de las personas.
- Se incluye la evaluación de impacto y la obligación de notificar incidentes de seguridad, entre las medidas destinadas a garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por ley.
- Se flexibilizan las normas relacionadas al consentimiento, con el fin de estar más acorde a la era digital. El Anteproyecto prevé que el consentimiento puede ser obtenido de forma expresa o tácita. La forma del consentimiento estará sujeta al contexto en el que se recepten los datos personales y al tipo de dato en cuestión.
- El interés legítimo pasa a ser una base legal admitida expresamente para el tratamiento de datos personales.
- Se incorporan parámetros especiales para el tratamiento de datos de niñas, niños y adolescentes, resaltando la importancia que para ello tiene el respeto a la Convención sobre los Derechos del Niño. Particularmente, en torno al consentimiento de los menores de edad para el tratamiento de sus datos, el Anteproyecto dispone que sea válido el consentimiento de una niña, niño o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos. En estos casos, establece que el consentimiento es lícito si el menor de edad es mayor a 13 años, y continúa aclarando que si la niña o niño

es menor de 13 tal tratamiento únicamente se considerará lícito si el consentimiento es otorgado por el titular de la responsabilidad parental o tutela, y sólo en la medida en que se haya otorgado.

- Se amplían las bases legales para realizar transferencias internacionales, incluyendo no sólo el consentimiento del titular de los datos sino también los mecanismos de autorregulación vinculante y las cláusulas contractuales que contengan mecanismos de protección de datos acorde con las disposiciones de ley.
- Se crea la figura del delegado de protección de datos, cuya designación será obligatoria para algunos casos específicamente definidos en la ley: tratamiento de datos por parte de autoridades u organismos públicos, tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento y tratamiento de datos a gran escala.
- Se aumenta el monto máximo de las multas, Asimismo, se contemplan otras sanciones por incumplimiento de la ley, como la suspensión o cierre temporal de actividades relacionadas con el tratamiento de datos e incluso el cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Tanto el anteproyecto como el Reglamento (UE) 2016/679, resaltan la importancia de garantizar el ejercicio de la libertad de expresión. En este sentido se establece que la ley no podrá afectar el tratamiento de datos que realicen los medios de comunicación en ejercicio de la libertad de expresión.

Si bien el proyecto de ley, reconoce el derecho de supresión, aclara especialmente que este derecho no procede cuando el tratamiento de datos persiga un fin público o sea necesario ejercer el derecho de libertad de expresión e información.

Es relevante hacer referencia a los cambios que trae aparejados la normativa proyectada en materia de transferencias internacionales. En la ley vigente, en principio, se prohíbe la transferencia de datos personales a los países que no proporcionen un nivel adecuado de protección[3]. La Ley luego prevé algunas excepciones a esta regla[4], pero en la práctica, ha demostrado que son limitadas y muy pocas aplican al sector privado[5]. Es cierto que la rigidez de estas normas fue flexibilizada por el decreto reglamentario al incluir el consentimiento del titular, pero el anteproyecto estimo conveniente aclarar esta situación.

Para ello, se amplían las bases legales para realizar transferencias internacionales, incluyendo al consentimiento, a los mecanismos de autorregulación vinculante y a las cláusulas contractuales. Cabe aclarar que bajo el modelo que propone el anteproyecto, el carácter de adecuado del país receptor de los datos sigue siendo una base fundamental para la transferencia internacional. La novedad se basa en que permite expresamente la transferencia internacional de datos cuando el responsable del tratamiento transferente y el destinatario adopten mecanismos de autorregulación vinculante o cláusulas contractuales que sean acorde a las disposiciones previstas en la ley, aún si el país receptor no garantice el nivel de protección adecuado[6]. El objetivo que se persigue con este cambio es mayor claridad al sistema, debido a las contradicciones que existen hoy entre la ley y la reglamentación y así crear un escenario más apto para la inversión e innovación en la Argentina.

Debo hacer una especial mención al "Principio de seguridad de los datos personales" y "Notificación de incidentes de seguridad", el anteproyecto lo que pretende es que se refuercen los derechos de los titulares, de modo que tanto el responsable del tratamiento, como el encargado, si existiere, adopten las medidas para garantizar la seguridad de los datos personales que se encuentren en sus bases y la obligatoriedad de informar cuando haya un incidente de seguridad.

Siguiendo la línea del anteproyecto, la Dirección Nacional de Protección de Datos Personales, dependiente de la Agencia de Acceso a la información Pública, consciente de la importancia que reviste el resguardo de la integridad y seguridad de la información en materia de datos personales, actualizó las medidas de seguridad que deben observar quienes hagan tratamientos de datos personales en archivos, registros, bancos y bases de datos públicos y privados, con el objeto de eliminar y/o mitigar los riesgos de dicha información, mediante la Resolución N° 47 del día 25 de julio de 2018, que deroga las Disposiciones de la entonces Dirección Nacional de Protección de Datos Personales del Ministerio

3 *Artículo 12 inc. 1 de la ley N° 25.326*

4 *Artículo 12 inc. 2 de la Ley N° 25.326*

5 *Palazzi, Pablo A. su nota sobre transferencia internacional de datos personales, publicada en Revista Latinoamericana de Protección de datos personales.*

6 *Disposición 60/2016 de la DNPDP, presenta una lista de países que son considerados adecuados bajo la legislación argentina.*

de Justicia y Derechos Humanos N° 11 del 22 de setiembre de 2006 y N° 09 del 3 de septiembre de 2008[7]. Esta Resolución establece una serie de recomendaciones a implementar durante todas las etapas del proceso de recolección y tratamiento de los datos personales, entre las cuales se destaca la notificación de los incidentes de seguridad a la Agencia de Acceso a la Información Pública, supuesto que no se encuentra contemplado en la Ley 25.326. Ello se encuentra en sintonía con el principio de responsabilidad proactiva o accountability que la Agencia tiende a proponer y que se encuentra en línea con el Reglamento General Europeo de Protección de Datos y el hasta aquí mencionado anteproyecto.

Ante el estado actual de evolución de la sociedad, donde las personas nos volvemos cada día más confiados de la tecnología, es necesaria también, la evolución permanente de la normativa. Sea este u otro el modelo que se siga al momento de la aprobación de una nueva ley de protección de datos personales, es imperioso que la República Argentina adecue la normativa al estándar internacional mencionado.

Por último debo mencionar, que mediante el mensaje 147/2018 el día 19 de septiembre de 2018, el Poder Ejecutivo Nacional remitió el proyecto de ley al Honorable Senado de la Nación para someterlo a su consideración.[8]

7 *Resolución N° 47/2018 https://www.boletinoficial.gob.ar/#!DetalleNorma/anexos/188654/20180725*

8 *https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf*

ACADEMIC MAGAZINE ON PERSONAL DATA PROTECTION

URCDP (Uruguay) – Juillet 2018

ISABELLE FALQUE-PIERROTIN

Isabelle Falque-Pierrotin se graduó de la Escuela de Altos Estudios Comerciales (HEC), de la Escuela Nacional de Administración (ENA) y del Instituto Multimedia. Fue relatora del Consejo de Estado, Directora Adjunta del Gabinete del Ministro de la Cultura y de la Francofonía (1993-1995), y es Consejera de Estado desde noviembre de 2001.
Es Presidente de la "Commission nationale de l'informatique et des libertés" (CNIL) desde el año 2011, reelecta en 2014. Fue Presidente del Grupo de Trabajo del Artículo 29 -grupo de las autoridades europeas en la materia-, de febrero de 2014 a febrero de 2018. Desde setiembre de 2017 es además Presidente de la conferencia mundial de autoridades en protección de datos personales.

RESUMEN

Los últimos años han constituido sin lugar a dudas un momento excepcional para la protección de los datos personales, en todo el mundo. Las fallas de seguridad y otros escándalos relativos a la utilización de los datos han provocado un despertar en las conciencias. Luego de las revelaciones de Edward Snowden en 2013 o, más recientemente, aquellas relativas a Cambridge Analytica, nuestras sociedades miden gradualmente hasta que punto los servicios tecnológicos pueden suscitar –mas allá de sus promesas - una serie de consecuencias derivadas de aquellos que trazan, supervisan o manipulan a las personas. En respuesta, las voces se hacen escuchar cada vez más en favor de una regulación más global, más ética, a la altura de la nueva sociedad de la información en la que actualmente vivimos. Es curcial que los próximos años permitan demostrar la credibilidad de los modelos de regulación recientemente consagrados, comenzando por el RGPD.

Les dernières années ont sans aucun doute constitué un moment exceptionnel pour la protection des données personnelles, et cela partout dans le monde. Les failles de sécurité et autres scandales relatifs à l'utilisation des données ont participé à un éveil des consciences. Depuis les révélations d'Edward Snowden en 2013 ou, plus récemment, celles concernant Cambridge Analytica, nos sociétés mesurent progressivement à quel point les services numériques peuvent susciter – au-delà de leurs promesses certaines – une série de dérives dès lors qu'ils tracent, surveillent ou manipulent les personnes. En réponse, des voix se font de plus en plus entendre en faveur d'une régulation plus globale, plus éthique, à la hauteur de la nouvelle société de la donnée dans laquelle nous vivons désormais. Il est crucial que les prochaines années permettent de démontrer la crédibilité des modèles de régulation récemment consacrés, à commencer par le RGPD.

En Europe, l'année 2018 fut celle de la concrétisation d'un choix politique majeur, le Règlement général sur la protection des données personnelles (RGPD), cadre juridique rénové applicable depuis le 25 mai qui vise à répondre aux attentes de chacune des parties-prenantes au sein de cette nouvelle société de la donnée. Attentes de confiance et de maitrise de la part des individus, attentes de fluidité et de simplification administrative de la part des entreprises. L'Europe fait le pari que maintenir un haut niveau de protection des personnes permettra de construire une innovation plus robuste, favorable au développement du numérique. Elle souhaite également renforcer sa souveraineté sur les données des Européens, face à une situation que certains observateurs caractérisaient de « colonie numérique ».

La possibilité d'une telle démarche n'était pas assurée. Il y a quelques années, très peu d'acteurs auraient parié sur un texte commun compte tenu de la variété des intérêts politiques ou économiques européens. Le RGPD a pourtant été adopté en 2016 et est pleinement applicable depuis le 25 mai 2018. C'est donc déjà un succès politique pour l'Europe. Mais ce texte sera vraiment fondateur, inspirant au plan international, s'il apporte des bénéfices opérationnels à tous les acteurs.

D'abord, aux 500 millions de consommateurs européens, qui expriment un appétit réel de maitrise de leur vie numérique, et peuvent se saisir des droits renforcés sur leurs données personnelles que leur offre le nouveau Règlement. Celui-ci met en effet la personne humaine au centre de la régulation, et fournit aux citoyens une « boîte à outils » enrichie, dont certains d'entre eux se sont déjà activement saisi. Les plaintes déposées en l'espace de quelques mois auprès de chacune des autorités de protection de données européennes ont ainsi significativement augmenté ; en France, par exemple, une hausse de 50 % en juin par-rapport à l'année précédente. Des associations ont d'ores et déjà utilisé les possibilités de recours collectif. Il ne s'agit pas ici d'empêcher le partage des données, mais plutôt de renforcer la possibilité – dans un nombre important de cas – de choisir les pratiques auxquelles l'on adhère, de comparer différents produits et services, voire le cas échéant de migrer vers des solutions moins « prédatrices » de données, en récupérant ses données grâce au nouveau droit à la portabilité.

Ensuite, le succès de cette réglementation dépendra de notre capacité en tant qu'autorités de régulation à convaincre l'écosystème de la data – de la grande firme à la startup en passant par la petite ou moyenne entreprise ou la collectivité publique – que la responsabilisation consacrée par le RGPD ne constitue en rien, et pour aucune de ses composantes, un frein à l'innovation. Elle donne au contraire l'opportunité d'intégrer très en amont la protection des données dans les plans de développement, et ainsi d'esquisser les bases du pacte de confiance attendu par les consommateurs, investisseurs ou administrés. Plus de flexibilité dans l'usage de la donnée, plus de garanties en termes de robustesse de l'infrastructure numérique, plus de stabilité dans la relation

client : tels sont les grandes apports du règlement pour ceux qui traitent de la donnée. Par-là, la conformité au règlement peut devenir un véritable argument de différenciation concurrentielle. Trop souvent perçues comme porteuses de lourdeurs administratives inefficientes, nos autorités doivent convaincre les acteurs économiques de l'intérêt stratégique et opérationnel d'une exemplarité en matière de collecte et de traitement des données personnelles. Elles ont un rôle clé à jouer pour accompagner ce changement de culture. C'est le parti qu'a pris la CNIL depuis plusieurs années se positionnant comme une institution « au service » de la conformité des acteurs. Dans cette transition RGPD, elle a renforcé son offre d'accompagnement sur les nouveaux outils, à l'instar de la réalisation d'une analyse d'impact (facilitée par un logiciel libre, traduit en 14 langues, mis à disposition sur le site de la CNIL) ou de la désignation au sein des organisations publiques ou privées d'un délégué à la protection des données (par un téléservice dédié).

Enfin, le RGPD réussira si le nouveau dispositif de coopération entre autorités européennes de protection des données se met efficacement en place. L'Europe s'est mise en capacité de parler d'une seule et même voix non seulement en matière de doctrine mais aussi sur des sujets opérationnels, à travers des décisions ou des sanctions conjointes. Par un dialogue soutenu impliquant chacune des autorités nationales, nos autorités auront pour défi de répondre à l'exigence de cohérence sur le territoire européen. Les premières réunions de l'EDPB (European Data Protection Board), nouvelle institution succédant au groupement des CNIL européennes (G29) ont été en ce sens très encourageantes, en permettant l'adoption de l'ensemble des guidelines relatives au règlement produites par le G29, ainsi que de riches discussions sur les premiers cas opérationnels dont nous avons été saisis. A présent, il est fondamental de démontrer opérationnellement la solidité de ce nouveau modèle de gouvernance, par la production rapide de deux types de résultat : des sanctions d'une part afin de crédibiliser l'arme de dissuasion qu'elles représentent, et des outils satisfaisants de compliance d'autre part, permettant aux entreprises européennes de piloter leur conformité facilement. La CNIL entend se dédier pleinement à cette nouvelle « aventure européenne », notamment en valorisant au-delà de ses frontières le patrimoine normatif très riche qu'elle a constitué depuis plusieurs années auprès des professionnels et citoyens, entre hautes exigences éthiques et accompagnement de l'innovation.

Le RGPD est donc une promesse ambitieuse pour la société numérique européenne mais elle doit, pour être tenue, mobiliser l'ensemble des acteurs européens concernés ; individus, entreprises et régulateurs.

Certains ont critiqué la démarche en considérant que ces exigences avaient une portée territoriale excessive et que l'Europe imposait un modèle au reste du monde. Je ne crois pas que cela soit le cas. Il est vrai que les acteurs mondiaux, même non établis en Europe, sont désormais soumis au droit européen dès lors qu'ils ciblent le marché européen par le déploiement de leurs produits ou services. Mais, ceci est chose courante dans tous les marchés du monde, faire en sorte que la même règle s'applique à tous ceux qui opèrent sur le même marché. Ce qui est sûr, c'est que sur son territoire, l'Europe a posé un cadre qu'elle entend faire respecter. Ce cadre, scruté partout dans le monde, peut devenir un standard global, mais il doit démontrer dans les mois à venir son bénéfice opérationnel.

Dans tous les cas, l'Europe via le RGPD, doit pouvoir s'insérer dans un dispositif mondial, pour répondre au mieux aux besoins des entreprises et aux défis globaux de régulation posés par le numérique. Aucune zone du globe ne peut aujourd'hui prétendre à la suprématie ou à l'isolement ! La présente revue académique annuelle de l'URCDP trouve ainsi toute sa pertinence pour renforcer le dialogue transfrontière nécessaire sur ces sujets. La Conférence Internationale des Commissaires à la Protection des Données et à la Vie Privée (ICDPPC), dont j'assure cette année la présidence, constitue aussi une enceinte privilégiée pour cette discussion féconde. Elle participe à la conversation mondiale indispensable pour partager les visions régionales respectives sur ces sujets, faire valoir des bonnes pratiques pouvant servir d'inspiration à d'autres ; en somme, construire collectivement un meilleur avenir numérique. Le réseau ibéro-américain de protection des données compte sans nul doute parmi les acteurs ayant pris la mesure desdits défis, par l'impulsion depuis plusieurs années d'une dynamique très vertueuse qu'il convient de saluer. L'adoption commune en juin 2017 de standards de protection des données, partagés par l'ensemble des autorités de la région, en constitue l'exemple le plus saillant. L'écosystème ibéro-américain de protection des données peut en outre s'appuyer sur une société civile très active pour la reconnaissance effective de droits à l'ère numérique. Dans le cadre de la récente consultation sur l'avenir de la Conférence Internationale, nous avons pu constater l'investissement énergique dans ces sujets de

plusieurs organisations non-gouvernementales sud-américaines. Avec une culture de la donnée personnelle en réelle maturation, l'espace ibéro-américain démontre ainsi la possibilité d'un développement règlementaire positif et rapide sur ces sujets.

Finalement, au plan national, régional ou mondial, nous sommes tous coresponsables de l'avenir de l'écosystème numérique, et le cadre de régulation de protection des données personnelles apparait de plus en plus comme une hybridation, un métissage de différentes influences. Ce tissage est me semble-t-il éminemment positif.

La régulation des données personnelles, entre éthique et innovation, avancées régionales et standards mondiaux, nous montre peut-être la voie pour une mondialisation plus ouverte, plus diverse.

LA PERSONA EN EL CENTRO:

Enfoque y práctica de la privacidad desde el diseño

LAURA
JUANES MICA

Es Director Global para Políticas de Privacidad de Facebook. Se graduó de Doctor en Derecho de la Universidad Autónoma de Madrid, España. Fue Consejera General Adjunta para Privacidad y Derechos Humanos de Yahoo. Posee certificaciones para profesionales internacionales de privacidad (CIPP) en Estados Unidos y Europa, y ha participado como expositora en foros de privacidad en todo el mundo. Fue miembro del Consejo para la Asociación Latinoamericana de Internet (ALAI) y es co-fundadora y miembro del Consejo para las mujeres en la tecnología de Miami.

PAULA
VARGAS

Es Gerente de Políticas Públicas del Cono Sur en Facebook, Argentina. Es abogada especializada en Derecho y Tecnología, Profesora de Derecho, y Coordinadora del Programa de Derecho de Internet y Tecnología de (DITC) de la Universidad de San Andrés. Obtuvo una Maestría en Derecho en la Universidad de Berkeley y se encuentra certificada como especialista en Gestión de la Privacidad de la Información (CIPM). Actualmente es co-Presidenta de la Asociación Internacional de Profesionales de la Protección de la Vida Privada (IAPP) para el capítulo de Argentina.

SUMARIO

RESUMEN

En el presente artículo las autoras analizan la evolución de las regulaciones con respecto a la "Privacidad desde el diseño" en América Latina, incluyendo el desarrollo de algunos de los proyectos de modificación legislativa que se encuentran a estudio actualmente en algunos países latinoamericanos. Desarrollan además las experiencias de Facebook para incorporar los distintos principios de la "Privacidad desde el diseño" en sus productos.

Las sociedades y los individuos han abrazado masivamente los beneficios del avance tecnológico. La creatividad para encontrar en la tecnología nuevos aportes al progreso no se detiene: las ciudades y el tráfico; la medicina y los diagnósticos; las empresas y su apertura al resto del mundo, y los individuos en todas las dimensiones de sus actividades diarias -desde conectar con sus familias y amigos, trabajar, educarse, informarse, mantenerse activos en sus comunidades y hasta encontrar una pareja- son todos ejemplos de adopción de soluciones innovadoras que los emprendedores inventan a diario.

Estos emprendimientos utilizan datos para ser eficientes y mejorar continuamente; para ello, en algunos casos, el producto o servicio necesita procesar información, incluyendo, cómo no, datos personales. Por ello, los mecanismos para proteger la privacidad de los titulares de esos datos deben ser parte del proceso de innovación y del neto resultante en términos de beneficio social. El progreso implica la innovación cuidadosa de la privacidad.

Un concepto que responde a esta idea es la privacidad desde el diseño, el cual, si bien ha sido parte de la evolución de la práctica y la regulación de la protección de la privacidad desde hace algunos años, en nuestros días se ha vuelto no sólo esencial, sino de facto imprescindible.

Este concepto implica, tal como fue concebido originariamente, incorporar la protección de la privacidad desde la gestación de la idea de un producto y durante todo el ciclo de vida de este. Aplicar la privacidad desde el diseño produce efectos netamente positivos en el individuo, en las empresas u organizaciones y en los reguladores.

Desde el punto de vista del individuo, la privacidad desde el diseño materializa los controles que las personas tendrán sobre sus datos. Así, la persona y el control de ésta sobre sus datos estarán en el centro del diseño del producto o servicio, y el resto de las funcionalidades deberán acompañar y armonizar ese objetivo.

En relación con las empresas u organizaciones, además de influir en los productos, la integración del principio de Privacidad desde el Diseño dentro de los procesos de las organizaciones también puede servir de elemento unificador e inspirador de buenas prácticas corporativas.

En Facebook sabemos que podemos mejorar. Está claro que toda organización, de pequeña a grande, precisa innovar continuamente para garantizar que las personas comprendan como se usan sus datos personales. En esencia, esta es una cuestión de diseño. Pero, además, como decimos en Facebook, no diseñamos para dígitos de ceros y unos, diseñamos para personas. Ello requiere construir y diseñar desde la responsabilidad; creemos que, como empresa de tecnología, tenemos la responsabilidad de explicarle a las personas -de una forma que sea inteligible para ellas- cómo son usados sus datos.

Por su parte, desde el punto de vista regulatorio, el concepto de privacidad desde el diseño es una suerte de "faro" que ilumina o guía tanto la propia redacción de la ley como también la interpretación de su cumplimiento desde el puntapié inicial de un proyecto.

En la práctica, hemos aprendido que alcanzar este objetivo final requiere de un diálogo interdisciplinario en el que todos los involucrados intentarán conciliar posiciones que van desde la complejidad de traducir conceptos legales a herramientas tecnológicas, hasta las propias limitaciones de la tecnología para hacer posible lo deseable, pasando por el factor temporal, que impone un rediseño a veces constante de ciertos productos o servicios, sin descontar los cambios regulatorios que pueden dar lugar a que todo comience otra vez. Todas esas variables, además, deberán responder a lo que los usuarios piden y esperan de un producto en términos funcionales (más información, más relevante o personalizada, con más servicios integrados, etc.).

En una comunidad global como la de Facebook, el desafío que se nos plantea es que cada persona es diferente, y espera diferentes cosas de un modelo de privacidad. La privacidad es un concepto que tiene un significado distinto para cada individuo, en diferentes momentos, y la mejor forma de garantizarla es poniendo a las personas en control de sus datos.

Comprender este desafío es esencial para todos los actores involucrados en la protección de la privacidad: los innovadores, los desarrolladores, los académicos, los reguladores, los defensores de usuarios y los educadores.

En el presente artículo mostraremos por un lado la evolución legislativa y regulatoria en términos de privacidad desde el diseño, y por otro, desarrollaremos algunos ejemplos del impacto de este concepto al momento de llevar a la vida la letra de la ley. La ley elige el diseño como su herramienta y a su vez el diseño tiene leyes propias que deben ser cumplidas para que se alcance el objetivo deseado: que la persona pueda proteger y ver protegida su privacidad.

Cómo comentaremos en la última sección, en Facebook detectamos la necesidad de trabajar en conjunto con el resto de los actores relevantes mencionados más arriba para facilitar más conocimiento sobre buenas prácticas y métodos de implementación de la privacidad desde el diseño. A este fin, motorizamos dos iniciativas de colaboración -Design Jams y TTCLab- de las que participan expertos de varias disciplinas para así potenciar el aprendizaje acumulativo, la transferencia de conocimiento y la minimización de errores. Les invitamos a ingresar a https://www.ttclabs.net para conocer más acerca de esta iniciativa y sacar provecho de esta herramienta.

LA EVOLUCIÓN REGULATORIA DE LA "PRIVACIDAD DESDE EL DISEÑO"

El concepto de "privacidad desde el diseño", fue acuñado y popularizado por la Dra. Ann Cavoukian, entonces a cargo de la Agencia de Protección de Datos Personales de Ontario, Canadá. Con dicho concepto, ella simbolizaba un modelo en virtud del cual se busca proactivamente incorporar la protección de la privacidad en el diseño de las configuraciones de las distintas tecnologías, la infraestructura de las redes y las prácticas comerciales. En su conceptualización, la Privacidad desde el Diseño puede ser segmentada en 7 Principios Fundamentales[1].

Este concepto tiene su primera codificación en octubre del año 2010, cuando es receptado en la Resolución[2] emitida por las Autoridades y Comisionados de Protección de Datos durante su Trigésimo Segunda Conferencia Anual en la ciudad de Jerusalén, reconociendo a la Privacidad desde el Diseño como un componente fundamental de la privacidad. La Conferencia invitó a las autoridades de protección de datos personales a receptar la privacidad desde el diseño en la formulación de sus políticas y de la legislación.

América Latina se presenta como pionera en su adopción, ya que, en el 2015, el Comité Jurídico de la Organización de los Estados Americanos había aprobado los "Principios de la OEA sobre la Privacidad y la Protección de Datos Personales" recomendado *"que los controladores de datos incorporen la protección de la privacidad en el diseño y la arquitectura de sus sistemas de tecnología de la información y en sus prácticas comerciales".*[3]

Europa por su parte incorpora este concepto como estándar legal de cumplimiento obligatorio en el Reglamento General de Protección de Datos Europeo, que explícitamente convierte esta recomendación en un mandato legal, en el Artículo 25.

"Artículo 25

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del

1 *Cavoukian, Ann, Privacy by Design in Law, Policy and Practice, 2011, p. 28. Disponible en: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf*

2 *International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, 2010. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf*

3 *Organización de los Estados Americanos, Comité Jurídico Interamericano, Informe del Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales,*
"Principio Diez: Responsabilidad: Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios. Incorporación de la privacidad en el diseño de sistemas Un enfoque contemporáneo eficaz consiste en requerir que los controladores de datos incorporen la protección de la privacidad en el diseño y la arquitectura de sus sistemas de tecnología de la información y en sus prácticas comerciales. Deben incorporarse consideraciones de privacidad y seguridad en cada etapa del diseño de los productos. Los controladores de datos deben estar preparados para demostrar sus programas de gestión de la privacidad cuando se lo solicite, en particular a petición de una autoridad competente a cargo de la aplicación de la normativa en materia de privacidad o de otra entidad que se encargue de promover la adhesión a un código de conducta. Las autoridades nacionales encargadas de la aplicación de la normativa pueden utilizar mecanismos internos de responsabilización solo si los controladores de datos tienen la disposición y la capacidad para demostrarles en qué consisten esos mecanismos y cuán bien funcionan.", 2015, Disponible en:
http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

presente Reglamento y proteger los derechos de los interesados."

La regulación de la Privacidad desde el Diseño se complementa, en el Reglamento, con una aproximación a la gestión del tratamiento de datos personales basada en el riesgo, la cual se plasma tanto en el Artículo 24, en el cual las organizaciones estiman el nivel de riesgo como en el Artículo 39, que establece las Evaluaciones de Impacto, una herramienta importante para operativizar la responsabilidad demostrada.

Recientemente, el Supervisor Europeo de Protección de Datos publicó la Opinión 5/2018, "Opinión Preliminar sobre la Privacidad desde el Diseño" en la cual brinda algunas precisiones sobre el alcance del concepto. En particular, ensaya una interpretación del estándar que permitiría balancear dos elementos que se presentan al decidir sobre las medidas de seguridad: las herramientas existentes ("estado del arte") y su costo, sopesadas con el riesgo concreto para los individuos. Indica el supervisor que las medidas elegidas deben mitigar en forma suficiente los riesgos existentes, y la protección debe resultar en consecuencia, adecuada.

Finalmente, los Principios Iberoamericanos de Protección de Datos, adoptados por la Red Iberoamericana de Protección de Datos Personales en el año 2017, incorporan la Privacidad desde el Diseño en el Párrafo Capítulo VI de "Medidas Proactivas en el Tratamiento de Datos Personales"[4].

Debe mencionarse que si bien la U.S. Federal Trade Commission, no adoptó este estándar dentro de una regulación específica, sí lo reconoce como una de las 3 prácticas recomendadas para proteger la privacidad en línea[5].

En el futuro, cuál sea el exacto alcance de esta obligación legal (qué tan amplia o enfocada es su interpretación) será determinado por los reguladores de protección de datos alrededor del mundo, quienes se verán balanceando contextos culturales, económicos, estadio de desarrollo, etc.

Aún más, el diseño de la misma ley impactará en las posibilidades reales que tendrá el operador de diseñar productos y servicios que realmente habiliten al titular de los datos a tener el control sobre los mismos. Si la ley no ha sido concebida considerando su aplicabilidad al diseño de servicios y productos, la privacidad desde el diseño corre el riesgo de ser ineficaz.

En efecto, un estudio recientemente publicado por Normally para el Centre for Information Policy Leadership, llamado *"Diseñar para la privacidad"*[6] explica cómo *"Es difícil identificar ejemplos de diseños que hayan abordado la privacidad de forma exitosa. Aún vemos notificaciones sobre cookies intrusivas, avisos de consentimiento repetitivos y densos Términos y Condiciones. Es dudoso que estas experiencias resulten atractivas para los usuarios y que les estén proveyendo algún tipo de elección significativa sobre como sus datos personales son utilizados. Una regulación prescriptiva -y su interpretación contraria al riesgo- está inhibiendo el valor que el Diseño de la Experiencia del Usuario (UX Design) puede aportarle a la privacidad y la protección de datos. El diseño precisa ser flexible y promover un abordaje creativo de los desafíos. Con la transición desde una aproximación basada en prescripciones a una basada en principios, tal vez vea-*

4 *Red Iberoamericana de Protección de Datos, Estándares de Protección de Datos Personales, "Medidas Proactivas 38. Privacidad por diseño y privacidad por defecto 38.1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. 38.2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.", 2017.*
Disponible en: http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo_RIPD.pdf#Testo%20en%20espa%C3%B1ol

5 *U.S. Federal Trade Commission, Protecting Consumer Privacy in an era or rapid change, 2012, p. 22*
Disponible en: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

6 *Normally y Centro for Information Policy Leadership: Design for Privacy How will the ePrivacy Regulation affect the design and user experiences of digital services?, "(Texto original en Inglés) It is difficult to identify examples of design which tackle privacy successfully. We continue to see obtrusive cookie banners, repetitive consent notices and bloated terms and conditions. It is doubtful that these experiences are engaging users and providing them with meaningful choices about how their personal data is used.*
Prescriptive regulation – and risk averse interpretation of it – is inhibiting the value which UX can bring to privacy and data protection. Design needs to be given the flexibility and encouragement to tackle these challenges creatively. With this switch in approach – from prescriptive to principled – we may begin to see the thoughtful innovation in privacy which we've come to expect elsewhere in the products we use", 2018.
Disponible en: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_design-for-privacy_may-2018_2_.pdf

mos una innovación bien pensada en materia de privacidad, lo cual ya se espera de cualquier otro producto que usamos", y concluye abogando por la libertad de crear experiencias basadas en principios y no en reglas prescriptivas, como la mejor opción para generar interacción, aumentar la transparencia y permitir una elección verdaderamente informada.

LA INCORPORACIÓN DE LA PRIVACIDAD DESDE EL DISEÑO EN AMÉRICA LATINA.

Tal como mencionamos en el apartado anterior, tanto el Comité Jurídico de la Organización de los Estados Americanos en los "Principios de la OEA sobre la Privacidad y la Protección de Datos Personales" (2015) como los Principios Iberoamericanos de Protección de Datos, adoptados por la Red Iberoamericana de Protección de Datos Personales (2017) incluyen la Privacidad desde el Diseño como estándar.

En las legislaciones internas de los países de América Latina, la obligación de los Responsables de establecer medidas de seguridad -el antecedente del concepto de Privacidad desde el Diseño- se incorporó en todas las leyes de Protección de Datos Personales que fueron sancionadas con posterioridad a la Directiva Europea 95/46/CE. Sin ir más lejos, Argentina[7], México[8], Uruguay[9] y Colombia[10] contemplan este tipo de medidas en sus leyes de protección de datos personales vigentes.

A medida que se masificó el concepto de Privacidad desde el Diseño, éste comenzó asimismo a aparecer en los proyectos de ley que pretenden actualizar la primera generación de leyes de protección de datos personales o que intentan establecer esta legislación por primera vez.

---

7 *Argentina, Ley 25.326 de Protección de Datos Personales: "ARTICULO 9° — (Seguridad de los datos).1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.".*
Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

8 *México, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, "Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."*
Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

9 *Uruguay, Ley Nº 18.331 Protección de Datos Personales y Acción de Habeas Data, "Artículo 10. Principio de seguridad de los datos.- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad"*
Disponible en:

10 *Colombia, Ley 1581, "Articulo 4 g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*
Disponible en:

Notoriamente, la recientemente aprobada Ley de Datos Personales de Brasil incorpora la privacidad desde el diseño.[11]

Además, todos los proyectos de ley de Protección de Datos Personales existentes en la región incorporan la Privacidad desde el Diseño. En algunos casos, la mención es expresa, en otros, la redacción replica el Reglamento General de Protección de Datos, aunque sin hacer referencia al concepto.

Proyecto de Ley de Datos Personales- Chile

"ARTICULO 14 quater.- Deber de adoptar medidas de seguridad. El responsable de datos debe adoptar las medidas necesarias para resguardar el cumplimiento del principio de seguridad establecido en esta ley, considerando el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados. Las medidas aplicadas por el responsable deben asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de tratamiento de datos.

Si las bases de datos que opera el responsable tienen distintos niveles de criticidad, deberá adoptar las medidas de seguridad que correspondan al nivel más alto."

Anteproyecto de Ley de Datos Personales- Argentina[12]

"ARTÍCULO 38.- Protección de datos desde el diseño y por defecto. El responsable del tratamiento debe aplicar medidas tecnológicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos establecidos en la presente ley. Las medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares. El responsable del tratamiento debe aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento de datos aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas humanas."

Proyecto de Ley de Reforma de la Ley de Datos Personales 18.331- Uruguay

"ARTÍCULO 37.- Sustitúyese el artículo 12 de la Ley Nº 18.331, de 11 de agosto de 2008, por el siguiente:

"ARTÍCULO 12.- Principio de responsabilidad.- El responsable de la base de datos o tratamiento y el encargado, en su caso, serán responsables de la violación de las disposiciones de la presente ley. En ejercicio de una responsabilidad proactiva, deberán adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

La reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización."

La aceptación del estándar de Privacidad desde el Diseño en las nuevas regulaciones de Protección de Datos Personales en la región torna oportuno compartir aprendizajes y experiencias sobre la implementación de este estándar en casos concretos, considerando que el traslado de conceptos jurídicos a la práctica del desarrollo de productos tecnológicos no siempre es intuitivo, sencillo ni necesariamente económico, y requiere un esfuerzo multidisciplinario.

---

11 *Brasil, Ley 13.709, (no disponible en Español, traducción al Inglés no oficial) Article 46 – The treatment agents shall take technical and administrative security measures capable of protecting personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, change, communication, dissemination, or any form of improper or unlawful treatment. Paragraph 2 – The measures mentioned in the head of this Article shall be observed from the product design or service until its implementation.*
Section II Good Practices and Governance Article 50 – The data controllers and data processors, within the scope of their competences, whether individually or by means of associations, may formulate rules of good practice and governance that establish the conditions of organization, the operating regime, procedures, including complaints and petitions, security standards, technical standards, specific obligations for the various parties involved in the treatment, educational actions, internal mechanisms for supervision and mitigation of risks and other aspects related to the treatment of personal data."
Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm

12 *Argentina, Anteproyecto de Ley de Protección de Datos Personales,*
Disponible en: https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pdf

LA EXPERIENCIA DE FACEBOOK EN EL DISEÑO DE HERRAMIENTAS DE PRIVACIDAD

En Facebook, el diseño de productos es crítico para la experiencia de las personas que utilizan la plataforma. Entre los equipos que diseñan productos, se encuentran los que diseñan la privacidad de los productos, aquellas herramientas que permiten a las personas tener control sobre sus datos cuando se conectan y comparten sus publicaciones. Herramientas como las que permiten al usuario "elegir audiencias" son diseñadas por personas que se especializan en comprender el impacto de la plataforma en la privacidad de las personas y cómo incorporar las indicaciones regulatorias.

Pero antes de explicar ejemplos concretos de esta tarea, es buen aclarar, ¿a qué nos referimos con "diseño"?. Como explica Margaret Gould Steward, VP de Diseño de Producto en Facebook, en su publicación -cuya lectura recomendamos- "Navegando la ética de la tecnología moderna"[13], el diseño comienza con la consciencia y la responsabilidad de que no se trata de una cuestión superficial de construir objetos bellos sino de diseñar productos útiles y usables desde la idea inicial hasta su lanzamiento, y durante todas sus etapas. Ella propone que debemos *"obtener aún más habilidades en anticipar efectos del sistema, protegiendo el bienestar de nuestra comunidad y comprendiendo el impacto en la sociedad, cuando una población mucho más grande y más diversa está utilizando nuestros productos"*. Y brinda un ejemplo concreto: la decisión de Facebook de compartir datos anonimizados, en tiempo real, a organizaciones como UNICEF, International Federation of Red Cross, Red Crescent Societies y World Food Program para colaborar con sus esfuerzos de ayuda a la población en el caso de desastres naturales. La construcción de un producto como "Disaster Maps", de enorme beneficio social, implica considerar las preocupaciones sobre la privacidad, y diseñar desde la responsabilidad de cumplir no sólo preceptos legales sino principios éticos.

Cuando estas decisiones éticas y de diseño intersectan con regulaciones, es necesario encontrar una metología que torne estas disciplinas interoperables y que verdaderamente coloquen a la persona en el centro de las decisiones.

En el caso concreto de Facebook, nuestro proceso de revisión de la privacidad de los productos es constante. Comenzamos a discutir y a iterar sobre cómo los productos que construimos impactarían en la privacidad de las personas y no cesamos esas discusiones. A partir de la idea de un producto, establecemos un equipo de revisión que incluye muchos equipos (legales, políticas públicas, marketing, comunicación, seguridad, programas de privacidad, entre otros). Este equipo comienza su proceso de revisión, el cual puede durar desde algunos días hasta meses, dependiendo el tipo de producto. Nuestro objetivo es asegurarnos de que hemos considerado todas las implicancias de privacidad y que todos los involucrados están alineados, al mismo tiempo que nos aseguramos la mejor experiencia para las personas. Este proceso también incluye la búsqueda de opiniones de un círculo más amplio, si fuera necesario. Una vez que acordamos el funcionamiento del producto desde una perspectiva de protección de la privacidad, documentamos esa decisión para nuestra propia referencia y revisión post-lanzamiento. Pero el proceso no termina allí, también discutimos la cancelación y la migración de productos, ya que queremos asegurarnos que la privacidad estará protegida durante todas las etapas del ciclo de vida de un producto.

Además de nuestro proceso interno, hemos contribuido a la creación de experiencias colaborativas de diseño que acercan a la comunidad a la práctica de la privacidad desde el diseño, y facilitan su adopción a gran escala. Siendo la privacidad desde el diseño un concepto que precisa de muchas perspectivas trabajando al unísono, hemos intentado crear y facilitar el espacio para que todas esas partes se reúnan en pos de un objetivo concreto cuyo resultado sea inmediatamente transferible al titular de los datos para tener más control sobre los mismos.

TTCLABS Y DESIGN JAMS

Los mejores conceptos sobre diseño comienzan con la mirada puesta en comprender a las personas: en el caso de los datos, en la forma en que les resulta mejor entender las cuestiones referidas a sus datos y como potenciar su interacción a este respecto. También reconocen la necesidad de una evolución constante: en vez de crear una solución rápida y definitiva, su objetivo es crear procesos que mejoren y se adapten constantemente a los cambios. Asimismo, estos conceptos también reconocen que diferentes soluciones serán aplicables en diferentes contextos.

13 *Stewart, Margaret, Able, Allowed, Should; Navigating Modern Tech Ethics, Disponible en: https://medium.com/facebook-design/able-allowed-should-navigating-modern-tech-ethics-50f54fodf7d6*

Este enfoque resulta sumamente necesario en el contexto actual, en el que las herramientas actualmente disponibles (desde lenguajes rebuscados que es más fácil ignorar que entender, hasta una cantidad de especificaciones técnicas difíciles de encontrar, que obligan a las personas a un esfuerzo grande para controlar el uso de sus datos) se han diseñado exclusivamente desde la necesidad de cumplir con todos los mandatos legales, y están fracasando, es decir, no están acercándonos al objetivo deseado.

Es por eso que estamos intentando expandir nuestro abordaje de cómo generar herramientas de control sobre los datos que puedan seguir el ritmo de la evolución de los productos tecnológicos -cada vez más "inteligentes" e intuitivos-. Facebook colabora con grupos de personas y organizaciones de diferentes áreas y lugares del mundo para comprender las distintas formas de colocar a las personas en el centro de las experiencias de diseño y brindarles más transparencia, control y confianza. Nuestro objetivo es estimular la colaboración en el desarrollo de nuevas soluciones y recursos de Privacidad desde el Diseño, que cualquier persona pueda usar, adaptar y replicar.

A ese fin, en colaboración con más de 60 organizaciones, tanto empresas como organizaciones de la sociedad civil, lanzamos un sitio web que permite a cualquier persona explorar, desarrollar y compartir las mejores prácticas de Privacidad desde el Diseño. El nombre del sitio TTCLabs (representando por sus siglas en Inglés, Trust, Transparency and Control), responde a la idea de que la relación entre las personas y las herramientas que utilizan sus datos para proveerles servicios debe estar guiada por la Confianza, la Transparencia y el Control, (https://www.ttclabs.net).

TTCLabs ha organizado en distintas ciudades del mundo experiencias prácticas llamadas "Design Jams", las que reúnen especialistas de diferentes áreas -incluyendo Economía, Derecho, Desarrollo de Productos, autoridades de protección de datos, activistas, - para resolver dilemas y desafíos de privacidad por medio de soluciones de diseño. El resultado de estas experiencias es práctico, no teórico. Los participantes crean y desarrollan un prototipo de productos, orientados a un público específico, que pueda ser luego aplicado en el mundo real.

Durante los Design Jam se recolectan las opiniones de los usuarios en tiempo real, se desarrollan ideas y se crean modelos de diseño durante una sesión que dura un día entero. Es una experiencia similar a los "Hacks" que desde hace mucho tiempo son un emblema de la cultura de Facebook.

Los resultados obtenidos hasta ahora en Berlín, Bruselas, Dublín, São Paulo, Hong Kong, Paris y Londres se convierten en recursos disponibles en (https://www.ttclabs.net) para que cualquier persona pueda acceder, y a partir de ahí pueda desarrollar y compartir mejores prácticas de Privacidad desde el Diseño. Los recursos que se encuentran en el portal son de código abierto, disponibles con una licencia de creative commons, e incluyen modelos de soluciones de diseño para proteger la privacidad.

Estos modelos surgen de problemas reales y su objetivo es servir de inspiración para las personas que están en busca de ideas concretas, por ejemplo:

- Simplificar las notificaciones sobre cookies[14]
- Educar a las personas sobre como son usados sus datos[15]
- Permitir que las personas elijan sus opciones de privacidad a medida que conocen mejor un determinado servicio[16]

Las experiencias que contamos son sólo un punto de partida. Facebook por sí solo nunca podrá ofrecer todas las respuestas o el consejo perfecto sobre este tema para cada situación o caso hipotético. De lo que se trata es de colaborar y trabajar con diferentes grupos de personas que, cada una a su modo y con base en diferentes experiencias y aprendizajes, están buscando desarrollar herramientas, productos y soluciones que amplíen la transparencia, el control y la confianza de las personas sobre el uso de sus datos, para su propio beneficio y de la sociedad.

14 *https://www.facebook.com/notes/facebook-brussels/cookies-and-jam-in-brussels-experts-come-together-for-a-new-approach-to-trust-an/1448302438549610/*

15 *Educar a las personas sobre como son usados sus datos*

16 *https://www.ttclabs.net/design/building-a-relationship-through-personal-data*

DERECHO AL OLVIDO EN EL REGLAMENTO DE LA UE

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

JOHN
PÉREZ BRIGNANI

Es Ministro de Tribunal de Apelaciones en lo Civil de 2do. Turno, representante del Poder Judicial en el Consejo Consultivo de la Unidad Reguladora y de Control de Datos Personales, e integrante del Grupo de Planificación Estratégica de la Suprema Corte de Justicia.

Es Doctor en Derecho y Ciencias Sociales y Magister en Derecho de la Empresa (IEEM). Ha realizado diversos cursos de especialización en materia judicial en España y Latinoamérica, destacándose la Maestría en Estrategia Nacional, el curso de Técnicas para la Reforma Judicial en la Universidad Complutense de Madrid, y la especialización en Derecho Mercantil en la Universidad de la República.

SUMARIO

RESUMEN

En el presente trabajo se realiza un análisis de los artículos que consagran el derecho al olvido en el nuevo reglamento europeo de protección de datos personales

INTRODUCCIÓN

El avance tecnológico determina la fácil accesibilidad, a todo tipo de información, acerca de cualquier persona o hecho a través de los diversos motores de búsqueda existentes.

Ello conlleva a que no sólo podamos obtener información actual sobre determinada persona, o hecho, sino también más remota en el tiempo, información ésta que quizás a la persona involucrada no le interese que se conozca al tratarse de una etapa superada de su vida, ni que se formen una opinión sobre su persona basada en dicha información.

Tal extremo determina que la persona, cuya información remota o inexacta considera perjudicial a sus intereses, pretenda que no pueda accederse a la misma.

Ahora bien, ¿las personas tienen derecho a obtener la restricción de acceso a tal información? ¿en qué términos? ¿Por qué vías?

Estas son algunas de las interrogantes que nos proponemos modestamente analizar en el presente trabajo

BREVE SÍNTESIS DEL RECONOCIMIENTO DEL DERECHO Y DE LOS INTERESES CONTRAPUESTOS A SU RESPECTO

Para entender el sentido del derecho al olvido y el impacto de su ejercicio, debemos concretar, en primer término el significado de la memoria, concepto clave para una adecuada resolución y comprensión de los temas debatidos.

En ese orden podemos definir la memoria como la capacidad de retener y seguir la información relativa a eventos, imágenes sensaciones ideas, etc. Mediante la misma registramos sucesivamente y llamamos de nuevo la experiencia de vida a nivel individual (memoria privada) y social (memoria colectiva). En términos amplios la memoria colectiva es el conjunto de representaciones sociales, sobre el pasado que cada grupo produce, institucionaliza, conserva y transmite a través de la interacción de sus miembros entre sí.[1]

Ahora bien, con el advenimiento de la informática no sólo podemos archivar inconmensurable cantidad de información, respecto de cualquier tema, sino también interrelacionarlas y acceder a la misma con facilidad, independientemente de la fecha en que se realizó, lo que implica que la memoria colectiva tenga una dimensión pocas veces imaginada con anterioridad.

Como señalan Umberti Ambrosoli y Massimo Sideri "hoy la memoria colectiva de una sociedad pasa a través de la red que para muchos de nosotros es la primera y exclusiva fuente de conocimiento nuestro lugar de archivo y el espacio donde se debate se forma, se alimentan y mueren. Y si bien la tecnología puede ayudar al ser humano, puede ser también un vehículo de problemas.[2]

Otro aspecto importante a tener en cuenta, es que la informática ha modificado claramente nuestro modo de crear y conservar el conocimiento en tres aspectos: 1) reduciendo el tiempo entre la producción y la utilización del conocimiento, 2) promoviendo la cooperación sin límites espaciales, 3) consintiendo una flexibilidad de la arquitectura y en la construcción del contenido de los libros que nosotros conocemos.[3]

Asimismo, y en el orden individual se puede afirmar que la representación online de la identidad personal de un sujeto se forma de: 1) los datos incluidos voluntariamente online, 2) datos que él deja sin saberlo, 3) datos que son introducidos por terceras personas.[4]

Por su parte Internet constituye una red de redes cuya memoria presenta las siguientes características: 1) inmensidad en cuanto a la cantidad de computadores que pueden integrarse, 2) Universalidad porque cualquier persona que pueda acceder puede beneficiarse y convertirse en un creador de contenido, 3) Existen múltiples criterios de organización, creados por el hombre para ordenar dictados por la tecnología que son aplicados desordenadamente sin que exista un orden general, 4) densidad porque existe la posibilidad de concentrar un gran número de información en un espacio físico limitado, 5) Volatilidad por cuanto el dato digital respecto al dato físico es más propenso a expandirse, 6) persistencia o la otra cara de la moneda en comparación con la volatilidad que describe la posibilidad de recuperar información

1 *Martinelli, Silvia Diritto all'oblio e motori di ricerca. Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 27*

2 *Ambrosoli, Umberto - Sideri, Massimo Diritto al oblio dovere della memoria. L'etica nella societa interconnnesa Edit Bompiani 2017 pag 25-29*

3 *Cfm L Floridi La filosofía dell'informzaione e i suoi problema in Iride 2005,18:45 pp 291-312*

4 *Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 46*

inteligible, incluso si se ha borrado e incluso después de un tiempo.[5]

Internet invierte el tema de la memoria, la transmisión del conocimiento y el conocimiento, entendido no sólo como una mera memoria, sino también como una incorporación del pensamiento en la escritura y en un sentido más amplio.

Por lo tanto ejercitar la memoria a través de la información de la red implica la permanencia de los datos y hacerlo con respecto a la memoria colectiva significa escapar de lo que Rodolfo Stefano llamó «ese presente eterno en el que la vida individual y social parece estar oculta, ajena al pasado e incapaz de conciencia del futuro».[6]

El tema de la memoria y de la trasmisión del conocimiento en un documento analógico o digital , cuya finalidad es la difusión de diversos temas entre numerosos sujetos y de la transmisión a la posteridad implica también la relación delicada entre el poder y el conocimiento y el concepto de memoria colectiva, puesto en juego en la lucha por el poder liderado por las fuerzas sociales.

Cabe recordar que como afirmaba Francis Bacon "el conocimiento es poder" y que este concepto está profundamente arraigado en el comportamiento humano: adquirir información sobre lo que nos rodea nos ayuda a sobrevivir.[7]

Otro aspecto importante es que las personas tienden a dar mayor peso a lo que acontece en los próximos 12 a 24 meses a menos que se trate de los hijos o del instinto de supervivencia.

También los indicadores de confianza se basan en el mediano plazo. El largo periodo es considerado generalmente solo por los economistas.[8]

¿Ahora bien, tomando en consideración tales parámetros cabe preguntarnos es posible o no prescindir de determinados datos cuando los mismos causen determinado perjuicio a una persona? ¿Qué derecho tiene a solicitar su cancelación? ¿Bajo qué circunstancias y en qué condiciones?

En este orden el primer aspecto a resaltar es que cuando hablamos de conocimiento, la sociedad necesita tener certezas sobre las cuales formarse opiniones y para ello debe disponer de la mayor cantidad de información posible.

Pero una vez que el público ha sido informado con exhaustividad, cesa el interés público en virtud de que la colectividad ya ha adquirido el hecho. Volver a proponer el evento sería inútil, ya que ya no existiría un interés real en la comunidad para estar satisfecho.

Y no solo es inútil para la comunidad, sino también perjudicial para los protagonistas en lo negativo de la historia. Aquí la reputación de los sujetos sufriría una lesión adicional.[9]

Y si la lesión se justifica inicialmente por la necesidad de informar al público sobre nuevos hechos, ya no es después de que las noticias se adquieren ampliamente. A partir de su adquisición completa, surgen las condiciones del derecho al olvido.

Se trata de un derecho que no pretende borrar el pasado, sino proteger el presente, preservar la reserva y la paz que el sujeto ya conocido, ha encontrado los medios para reconstruir la dimensión social del individuo evitando que la vida pasada puede constituir un obstáculo para la vida presente y se juega en la brecha temporal entre el presente y el pasado.[10]

Pero existen otros hechos serios que se vuelven a proponer precisamente porque no se olvidan, o vicisitudes que se puede decir que han cambiado el curso de los acontecimientos y se convierten en historia y aquí no se puede hablar del derecho al olvido porque los hechos nunca se vuelven privados.

Por el contrario, sería precisamente su no repetición la que se pondría en contacto con el interés público, que siempre prevalece sobre el derecho del individuo a dejar de ser recordado.

Pero a excepción de los casos en que el interés público está destinado a no desvanecerse, el derecho al olvido siempre comienza, desde el momento en que el interés público cesa en torno a un hecho porque ahora se adquiere.

Para el protagonista en el negativo de la historia, ese hecho se vuelve privado y adquiere plena revelación a la confidencialidad.

Cabe destacar que dado que el derecho al olvido depende de la persistencia de la falta de interés público, puede ocurrir que surja un interés público al mismo tiempo que la réplica del hecho mismo.

Pero el derecho al olvido y, en un sentido más amplio, las necesidades individuales de las personas

5 *Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 15*

6 *Ambrosoli, Umberto - Sideri, Massimo Diritto al oblio dovere della memoria . L'etica nella societa interconnnesa Edit Bompiani 2017 pag62*

7 *Mayer-schonberger , Viktor Delete Egea 2016 pág 85*

8 *Cfm Ambrosoli Umberti -Sideri Massimo ob cit pag 36*

9 *A cura dei Giuseppe Cassno, Stalking, atti persecutori, cyberbullismo e tutela dell'oblio Wolters Kluwer2017 pag 263*

10 *Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 89*

a las que se respeta su esfera de intimidad y su identidad personal está correctamente representado, se opone a estas necesidades fundamentales de información y memoria.[11]

Es por ello que como afirma Silvia Martinelli "cuatro aspectos en particular se muestran en el estado actual como un problema que necesita de una amplia reflexión a fin de tutelar los intereses involucrado en un equilibrio justo:

El primero concierne la identificación de los principios generales que deben guiar el equilibrio entre los derechos involucrados a la luz de necesidades subyacentes y que pueden aplicarse a los efectos de decidir sobre el derecho al olvido y la desindexación

El segundo refiere al motor de búsqueda es necesario individualizar los criterios de desindexación para permitir que la referencia al contenido se mantenga donde la investigación no está dirigida al perfil de una persona física

En tercer lugar, se considera que deben proponerse procedimientos para llevar a cabo las solicitudes de desacato y para decidir sobre cuáles son adecuadas para proteger a todos los sujetos afectados por el mismo, para ser individuarse también a través del análisis de otros modelos y verificar la aplicabilidad

Finalmente, en relación al área de implementación territorial de las decisiones sobre olvido y desindexación se plantea la más compleja de las cuestiones, que, más allá de las posibles soluciones técnicas, que solo pueden ser resueltas mediante soluciones de compromiso en el marco de la cooperación y del derecho internacional.[12]

En suma: Existe un derecho fundamental de la persona a mantener el control sobre su propia información y de determinar la modalidad de construcción de la propia esfera privada Tal extremo colide con la información presente atemporal e indiscriminada que existe en Internet.

Por consiguiente para salvaguardar ese derecho debe concederse a las personas la posibilidad de que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos , es decir , cuando el interesado retire su consentimiento al tratamiento de los datos o de que haya expirado el plazo de conservación de los mismos.

Y aquí es justamente donde entrar a operar el derecho al olvido que puede ser definido como aquel derecho fundamental, que tienen las personas a que los enlaces que existen sobre ellas en los buscadores, que les perjudiquen y no sean pertinentes, puedan ser retirados de Internet.

REGULACIÓN EN EL NUEVO ORDENAMIENTO EUROPEO. CAUSALES.

Cabe preguntarnos porque era necesaria la regulación del derecho al olvido.

Por la evolución de las concepciones de derecho de privacidad y protección de datos y la difusión de los mismos debido principalmente a los avances tecnológicos que determinaban la necesidad de que existiera un marco adecuado para el ejercicio del derecho fundamental objeto de estudio.

Es por ello que el nuevo ordenamiento europeo de la protección de datos personales a regulado en su artículo 17 el derecho al olvido en los siguientes términos:

Derecho de supresión ('derecho al olvido')

1. El interesado tendrá derecho a obtener del responsable del tratamiento el borrado de los datos personales que le conciernen sin demora indebida y el responsable del tratamiento tendrá la obligación de borrar los datos personales sin demora indebida cuando concurra alguno de los siguientes motivos:
   a. los datos personales ya no son necesarios en relación con los fines para los que fueron recopilados o procesados;
   b. el interesado retira el consentimiento sobre el que se basa el procesamiento de conformidad con el artículo 6, apartado 1, letra a), o con el artículo 9, apartado 2, letra a), y cuando no haya otro fundamento jurídico para el tratamiento;
   c. el interesado se opone al tratamiento con arreglo al artículo 21, apartado 1, y no existen razones legítimas imperiosas para el tratamiento, o el interesado se opone al tratamiento de conformidad con el artículo 21, apartado 2;
   d. los datos personales han sido procesados ilegalmente;
   e. los datos personales deben borrarse para cumplir con una obligación legal en la legislación de la Unión o del Estado miembro a la que está sujeto el responsable del tratamiento;
   f. los datos personales se han recopilado en relación con la oferta de servicios de la

11 *Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 321*

12 *Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017 pag 323*

sociedad de la información a que se refiere el artículo 8, apartado 1.

2. Cuando el responsable del tratamiento haya hecho públicos los datos personales y se haya obligado de acuerdo con el apartado 1 a borrar los datos personales, el controlador, teniendo en cuenta la tecnología disponible y el coste de la implementación, tomará medidas razonables, incluidas medidas técnicas, para informar a los controladores que están procesando los datos personales que el sujeto de los datos ha solicitado que dichos controladores eliminen de cualquier enlace, copia o reproducción de esos datos personales.
3. Los párrafos 1 y 2 no se aplicarán en la medida en que sea necesario el procesamiento:
   a. por ejercer el derecho a la libertad de expresión e información;
   b. para el cumplimiento de una obligación legal que requiere el procesamiento por la Unión o la legislación del Estado miembro a la que el controlador está sujeto o para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial conferida al controlador;
   c. por razones de interés público en el ámbito de la salud pública, de conformidad con los puntos (h) y (i) del Artículo 9 (2), así como con el Artículo 9 (3);
   d. para fines de archivo con fines de interés público, investigación científica o histórica o con fines estadísticos de conformidad con el artículo 89, apartado 1, en la medida en que los derechos contemplados en el apartado 1 puedan imposibilitar o perjudicar seriamente el logro de los objetivos de ese objetivo. tratamiento; o
   e. para el establecimiento, ejercicio o defensa de reclamos legales.

¿DERECHO AL OLVIDO O DERECHO A LA SUPRESIÓN DE DATOS?

En realidad compartimos con Silvia Martinelli que el reglamento no consagra un derecho al olvido sino un derecho a la cancelación de datos En efecto la cancelación abarca también la revocación del consentimiento previo prestado mientras que el derecho al olvido no Asimismo la cancelación tiene una acepción más estrecha respecto al derecho al olvido, en cuanto el derecho al olvido abarca también el derecho a la no publicación y el derecho a la desindexación, no constituyendo esta ultima una cancelación

El término cancelación es menos preciso, en cuanto engloba seguramente la desindexación, en tanto no se trata en tal caso de cancelación del contenido original sino de datos tratado por el motor de búsqueda.

Cabe señalar que en el proyecto el articulo tenía como título Derecho a ser olvidado y borrado.

Otra diferencia significativa con el proyecto es que en el mismo se preveía la abstención de una mayor difusión de dichos datos y para obtener de terceros el borrado de cualquier enlace, copia o reproducción de esos datos.

En el artículo objeto de estudio se consagra, a favor del titular de los datos el derecho de obtener del responsable del tratamiento el borrado de los datos personales que le conciernan.

Entendemos que como, está redactado el artículo, el titular puede solicitar directamente al responsable la supresión correspondiente, el cual se encuentra obligado a efectuarla si se dan los presupuestos requeridos por la norma

Ahora bien, si el responsable no efectúa la supresión cual es el organismo competente, ¿ante quien debe ocurrir el titular de los datos para el cumplimiento efectivo de la medida?

En ese orden tenemos que el Reglamento asigna la competencia para ordenar dicha rectificación en vía administrativa al organismo de contralor del país respectivo (art 58 2 literal g)

Y en cuanto a las directrices, recomendaciones y buenas prácticas relativas a la supresión de vínculos copias o replicas de los datos personales procedente de servicios de comunicación pública corresponde al Comité europeo de Protección de Datos (art 70 literal d).

Asimismo, sin perjuicio de la acción en vía administrativa el interesado tiene la posibilidad de ejercitar la vía judicial (art 79 nral 2).

En cuanto a la competencia territorial es donde el responsable o encargado tenga un establecimiento o alternativamente ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual salvo el caso que el responsable o encargado actué en ejercicio de sus poderes públicos

Ahora bien, ¿que acontece en caso de que el responsable o encargado del tratamiento no cumpla con la obligación?

En este orden el Reglamento prevé que el mismo puede ser sancionado con una multa de hasta

20.000.000 de Euros o una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio anterior optándose por la de mayor cuantía (art. 83).

En cuanto al periodo de tiempo en que debe efectuarse el borrado la norma dice sin demora indebida ,es decir no establece un lapso especifico y ello es claro que ocurra porque va a depender de la base de datos , el nivel de información y de complejidad de la base entre muchas otras variantes técnicas.

Lo que deja claro la norma es que no debe dilatarse indebidamente, esto es ,sin que exista una justificación técnica o jurídica que impida el cumplimiento de lo peticionado.

Cabe resaltar en este orden que no sólo se establece en el considerando 59 la posibilidad de que la solicitud se efectúe por medios electrónicos sino también la obligación del responsable de dar una respuesta sin dilación indebida y a más tardar en el plazo de un mes y a explicar los motivos por lo que no puede atenderlas.

Tal extremo no condiciona a mi juicio que el plazo máximo referido, esto es un mes, pueda considerarse que es el plazo que dispone el responsable para el borrado de los datos por dos motivos. El primero es que si el legislador entendía que éste debía ser el plazo así pudo haberlo consignado. El segundo y último motivo es que no puede determinarse en cada caso el tiempo que técnicamente puede llevar efectuar la cancelación pretendida.

DATOS QUE PUEDEN SER CANCELADOS

Respecto a que datos pueden ser cancelados tenemos:

a. **los datos personales que no sean necesarios en relación a los fines para los que fueron recogidos o tratados de otro modo**

Los datos son concedidos por el interesado con una finalidad determinada (art 6 literal a) y es claro que si no son necesarios para dicha finalidad deban ser suprimidos. Igual extremo acontece cuando se concedieron para que fueran tratados dentro de determinado ámbito y se pretende darles otro destino no para el que fueron concedidos.

No debemos perder de vista que el interesado es el dueño de los datos y el eje del sistema de protección.

b. **el interesado retira el consentimiento sobre el que se basa el procesamiento de conformidad con el artículo 6, apartado 1, letra a), o con el artículo 9, apartado 2, letra a), y cuando no haya otro fundamento jurídico para el tratamiento;**

En la primera hipótesis el interesado retira el consentimiento específico para el trato de sus datos para uno o varios fines específicos (art 6 1 letra a) y dicho retiro implicará que los datos no puedan ser tratados por el responsable en forma lícita.

En la hipótesis segunda esto es la del art 9 apartado 2 letra a el consentimiento no es especifico sino explicito y para retirar el mismo con uno o mas de los fines especificados, con la excepción de que el Derecho de la unión o de los Estados miembros establezca que la prohibición establecida en el apartado 1 esto es la prohibición del tratamiento de datos personales que revelen el origen étnico o racial , las opiniones políticas, las convicciones religiosas o filosóficas o la de afiliación sindical , datos genéticos , datos biométricos a identificar de manera univoca a una persona , datos relativos a la salud o datos relativos a la vida sexual o a las orientaciones sexuales de una persona física no puedan ser levantadas por el interesado.

Por último, en este inciso se hace referencia a que no exista otro fundamento jurídico distinto a los previstos en los artículos referidos para la solicitud de retiro del consentimiento En este ultimo caso la posible eliminación de los datos deberá ser considerada a la luz de los fundamentos jurídicos que den lugar a la acción.

c. **el interesado se opone al tratamiento con arreglo al artículo 21, apartado 1, y no existen razones legítimas imperiosas para el tratamiento, o el interesado se opone al tratamiento de conformidad con el artículo 21, apartado 2;**

En el caso del apartado 1ero del art 21 la oposición se puede realizar en cualquier momento siempre que los datos sean tratados de conformidad al art 6 apartado 1 letra e o f esto es que el tratamiento es necesario para el cumplimiento de una misión realizada en interés publico o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento siempre que los derechos fundamentales del interesado no prevalezcan o cuando sea un niño.

d. **los datos personales han sido procesados ilegalmente;**

Este inciso no merece mayores comentarios dado que los datos deben ser obtenidos en forma licita y no pueden ser utilizados con finalidades ilícitas por parte del Responsable

e. **los datos personales deben borrarse para cumplir con una obligación legal en la legislación de la Unión o del Estado miembro a la que está sujeto el responsable del tratamiento;**

Si bien en este caso se prevé que sea a solicitud del interesado, creo que en este caso tal solicitud no seria necesaria ya que debería hacerlo directamente sin petición de especie alguna

f. **los datos personales se han recopilado en relación con la oferta de servicios de la sociedad de la información a que se refiere el artículo 8, apartado 1.**

Se trata de datos que fueron obtenidos con relación a la oferta directa a niños.

Se consagra de esa forma el derecho del interesado de ejercer tal derecho independientemente del hecho que no es mas un menor

LÍMITES A LA CANCELACIÓN DE DATOS DE ORDEN TÉCNICO Y ECONÓMICO

Ejecución de las medidas

2. Cuando el responsable del tratamiento haya hecho públicos los datos personales y se haya obligado de acuerdo con el apartado 1 a borrar los datos personales, el controlador, teniendo en cuenta la tecnología disponible y el coste de la implementación, tomará medidas razonables, incluidas medidas técnicas, para informar a los controladores que están procesando los datos personales que el sujeto de los datos ha solicitado que dichos controladores eliminen de cualquier enlace, copia o reproducción de esos datos personales.

El articulo no establece un derecho a la cancelación absoluto, a cualquier precio habla de medidas razonables

Ahora bien ¿que son medidas razonables? ¿ quien cataloga si una medida es razonable o no?

En este orden la norma no trae una definición precisa y es lógico que no la realice ya que la tecnología va evolucionando y los costos también . Creo sí que deberían darse parámetros para determinar cuándo un costo puede considerarse razonable o no .

Tales pautas deberán darse por el Comité europeo de Protección de Datos(art 70 literal d .del Reglamento.)

Lo que si es claro es que la norma no dispone que el borrado deba realizarse sin tomar en cuenta los costos y las tecnologías y que no puede obligarse al responsable de los servicios a realizar el mismo a un coste excesivo , o que sea imposible desde el punto de vista técnico

En cuanto a quien debe catalogar si la medida es o no razonable entendemos que la encargada de determinar tales parámetros será la autoridad de control en el área administrativa , lo que no excluye la competencia judicial para determinar si efectivamente las medidas dispuestas son o no razonables.

DE ORDEN CONSTITUCIONAL Y LEGAL

3. Los párrafos 1 y 2 no se aplicarán en la medida en que sea necesario el procesamiento:

a. **por ejercer el derecho a la libertad de expresión e información;**

Como expresara la CIDH "la libertad de expresión constituye uno de los pilares esenciales de una sociedad democrática y una condición fundamental para su progreso y para el desarrollo personal de cada individuo. Dicha libertad no sólo debe garantizarse en lo que respecta a la difusión de información o ideas que son recibidas favorablemente o consideradas como inofensivas o indiferentes, sino también en lo que toca a las que ofenden, resultan ingratas o perturban al Estado o a cualquier sector de la población Lo anteriormente expuesto, advierte la Corte Europea, tiene una importancia particular cuando se aplica a la prensa. No sólo implica que compete a los medios de comunicación la tarea de transmitir información e ideas relativas a asuntos de interés público, sino también que el público tiene el derecho a recibirla (Cfm CIDH Caso Ivcher Bronstein vs Peru reparaciones y costas Serie C Nro.74 parrá 153-154)

La libertad constituye el principio y las limitaciones son la excepción .Como sugirió alguna vez John Stuart Mill, la protección de la libertad de expresión no se justifica únicamente en el interés autoexpresivo de los sujetos protegidos, sino además en la utilidad de la raza humana. Según este autor "la peculiaridad del mal que consiste en impedir la expresión de una opinión es que se comete un robo a la raza humana."

(Mill, John Stuart: Sobre la libertad. Alianza Editorial. Madrid 1999. P. 77) .

Este derecho constituye uno de los pilares fundamentales de la democracia. no hay desarrollo personal sin libertad de expresión , y no se puede hablar de democracia sin libertad de expresión , es el oxígeno de la democracia.

Es por ello que en la medida que la libertad de expresión se encuentre limitada o se dificulte su ejercicio, mal podremos hablar de que existe una democracia.

Para que ello no ocurra debe darse la mayor amplitud posible al ejercicio de este derecho protegiendo no sólo la forma en que se ejercita ese derecho sino también su posible contenido.

Otro aspecto importante a destacar es que los derechos -o libertades- fundamentales son, además de derechos subjetivos, elementos esenciales de un Ordenamiento objetivo de la comunidad nacional. Por tanto, en su proclamación, efectividad y garantía permanente , reposa el «genio expansivo» del Estado de derecho. En particular, el derecho a la información se ha convertido, junto a la libertad de expresión, su hermana gemela, en piedra de toque de los demás derechos y libertades, porque, según veremos, se configura» como una libertad situada más arriba del cielo de los conceptos jurídicos: una libertad supraconstitucional, incondicionadamente preferente a cualquier otro derecho constitucional, regida por un diferente sistema de frenos y equilibrios, autorregulada, autocontrolada, autotutelada, exenta, en fin, intocable para cualquier otro poder externo».

El mismo concepto de orden público reclama que, dentro de una sociedad democrática, se garanticen las mayores posibilidades de circulación de noticias, ideas y opiniones, así como el más amplio acceso a la información por parte de la sociedad en su conjunto. La libertad de expresión se inserta en el orden público primario y radical de la democracia, que no es concebible sin el debate libre y sin que la disidencia tenga pleno derecho de manifestarse».**(Sentencia de la Comision Interamericana de Derechos Humanos del 6 de febrero de 2001 in re Ivcher Bronstein).**

Por consiguiente la limitación del derecho al olvido respecto de la libertad de expresión y de información se encuentra plenamente justificada.

Es más este articulo está en clara consonancia con lo dispuesto en el art 85 en el cual se establece que los Estados deben conciliar por ley el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información.

Por otra parte no siempre es justo remover del espacio público una información real, verdadera y correcta, cuando esta publicada y existe un claro interés público en su conocimiento en beneficio del interés individual Al interés individual en esos casos se contrapone un interés mayor de carácter publico.[13]

b. **para el cumplimiento de una obligación legal que requiere el procesamiento por la Unión o la legislación del Estado miembro a la que el controlador está sujeto o para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial conferida al controlador;**

Este inciso va en consonancia con lo previsto en el Considerando 73 del Reglamento que dispone que el Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información en La medida que sea necesario y proporcionado en una sociedad democrática.

c. **por razones de interés público en el ámbito de la salud pública, de conformidad con los puntos (h) y (i) del Artículo 9 (2), así como con el Artículo 9 (3);**

Este articulo también está en consonancia con lo expresado en el Considerando 73 antes citado y es una limitación que le da preeminencia a dos aspectos el interés público y el derecho a la salud.

En este orden no debemos perder de vista que en el caso de los asuntos de interés público, se entiende que una democracia exige el mayor ámbito posible de discusión pública sobre el funcionamiento de la sociedad y el Estado en todos sus aspectos , de forma tal que exista la mayor circulación de informes opiniones e ideas sobre asuntos de interés público (Cfm Corte IDH Caso Kimel Vs Argentina sentencia 2 de mayo de 2008 , Serie C Nro. 177 parra 57 y87 , Caso Claude Reyes y otros vs chile Sentencia de 19 de setiembre de 22 de noviembre de 2006 Serie C Nro. 135 par 83).

Ello por cuanto solo con el acceso a la mayor cantidad de opiniones e información posible es que puede ejercerse el contralor de la población respecto de la gestión pública quienes

13 *A cura dei Giuseppe Cassno , Stalking, atti persecutori, cyberbullismo e tutela dell'oblio Wolters Kluwer2017 pag 335*

ejercen funciones publica o pretenden hacerlo se exponen , en ejercicio de su libertad de elección al mayor grado de escrutinio y a la crítica del público y poseen además mayor capacidad de controvertir la información a través de su poder de convocatoria pública, (Cfm Caso Kimel vs Argentina Sentencia de 2 de mayo del 2008 Serie C Nro. 177 parras 86 a 88).

d. **para fines de archivo con fines de interés público, investigación científica o histórica o con fines estadísticos de conformidad con el artículo 89, apartado 1, en la medida en que los derechos contemplados en el apartado 1 puedan imposibilitar o perjudicar seriamente el logro de los objetivos de ese objetivo. tratamiento; o**

El art 89 deja a los Estados miembros un amplio margen de discrecionalidad y al mismo tiempo hacen que la frontera entre el derecho a ser olvidado y otros derechos abra el camino a una amplia diferenciación en su aplicación. en los estados miembros en forma individual.

El reglamento en el considerando 156 sugiere a los estados miembros que pueden disponer las medidas necesarias para garantizar el derecho de los interesados mediante la adopción de medidas técnicas y organizativas tendientes a reducir al mínimo el tratamiento de los datos personales.

CONCLUSIONES

El nuevo Reglamento Europeo en materia del tratamiento de datos personales reconoce, un derecho humano fundamental cual es el derecho al olvido , derecho este intrínsecamente vinculado al tratamiento de datos , en especial los que refieren a los que circulan por internet (considerando 66 del Reglamento)

La regulación en si no sólo no lo define sino que no contempla adecuamente el concepto de derecho al olvido en toda su dimensión.

En puridad nos hallamos ante la concesión de un derecho a la cancelación de datos del interesado con la correspectiva obligación del responsable del tratamiento ,en la cual se contemplan adecuamente el derecho individual del interesado a que se supriman determinados datos con los derechos de información y expresión y el interés publico en los casos previstos en la norma.

Cabe destacar asimismo que el responsable del tratamiento no se encuentra obligado a la cancelación a cualquier precio sino en la medida de lo razonable , concepto éste último sobre el cual deberá fijar pautas el Comité europeo de Protección de Datos.

BIBLIOGRAFIA

Ambrosoli, Umberto Sideri Massimo Diritto all¡oblio dovere della memoria L'etica nella societa interconessa Bompiani editores 2017

A cura dei Giuseppe Cassano , Stalking, atti persecutori, cyberbullismo e tutela dell'oblio Wolters Kluwer2017

A cura di Marco Maglio,Miriam Polini-Nicola Tilli Manuale di diritto alla protezione dei dati personali . La privacy dopo el regolamento UE 2016/679 Maqggioli Editore2017

A cura di Salvatore Sica , Virgilio D'antonio Giovanni Maria Riccio La nuova disciplina dellla privacy Editorial Wolters kluwer Cedam , 2016

Martinelli, Silvia Diritto all'oblio e motori di ricerca . Memoria a privacy nell'era digitale Giuffre Editore 2017

Mayer -Schonberger Viktor Delete Edit Económica Egea2016

Sassano, Francesca Il diritto all¡oblio tra internet e mass media Editore key 2015

Simon Castellano Pere El reconocimiento del derecho al olvido digital en España y en la UE Edit Bosch feb 2015

EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS:

una apuesta para actualizar las garantías a la realidad tecnológica.

JESÚS
RUBÍ NAVARRETE

Es Abogado y Adjunto al Director de la Agencia Española de Protección de Datos. Fue Director del Gabinete de Ministro de Justicia, Secretario General Técnico del Ministerio de Relaciones con las Cortes, Director General de Relaciones con las Cortes, Vocal del Tribunal de Defensa de la Competencia y Subdirector General de Inspección de Datos de la Agencia Española de Protección de Datos.

Es autor de diversas publicaciones en materia de publicidad, derecho de competencia, procedimiento administrativo y protección de datos personales, colaborador en diferentes Universidades de España, participante en reuniones y conferencias internacionales sobre protección de datos personales, en proyectos internacionales de colaboración con otras autoridades de protección de datos de República Checa, Bulgaria, Bosnia y Herzegovina, Israel y Croacia y coordinador de la Red iberoamericana de Protección de Datos.

SUMARIO

RESUMEN

El desarrollo de servicios de la sociedad de la información y de la tecnología han supuesto un cambio profundo de la accesibilidad a la información y al conocimiento con implicaciones en todos los entornos personales, sociales y económicos.

Esta realidad ofrece ventajas muy relevantes para las sociedades y los ciudadanos acompañadas de nuevos riesgos que generan desconfianza sobre el control de la información personal.

El Reglamento actualiza las garantías para la protección de datos personales a la realidad tecnológica extendiendo su ámbito de aplicación territorial, reconociendo nuevos derechos, facilitando los flujos internacionales de datos y estableciendo nuevos modelos de cumplimiento basados en la responsabilidad proactiva que, por su carácter dinámico, permiten una actualización continuada a los desarrollos futuros de la tecnología.

Complementariamente se regulan modelos de supervisión más flexibles, si bien permiten en caso necesario la adopción de medidas disuasorias de tratamientos ilícitos.

EL TRATAMIENTO DE DATOS PERSONALES EN LA SOCIEDAD DIGITAL

Nos encontramos inmersos en una sociedad digital, o sociedad de la información, caracterizada por la existencia de más información sobre las personas y sobre más aspectos de su vida, que puede ser almacenada, intercambiada y procesada para una enorme variedad de fines con gran facilidad y con relativamente bajos costes.

Ese es el escenario en el que actualmente tiene que desenvolverse del derecho fundamental a la protección de datos personales. Ingentes cantidades de información que son constantemente generadas y compartidas por todos los ciudadanos en un contexto altamente tecnificado.

El desarrollo de internet está en la base de este avance. Todos los servicios de la sociedad de la información se apoyan en la red y, al tiempo, han contribuido a su crecimiento y a la universalización de su utilización.

Un factor a destacar es que la presencia de internet se hace patente no solo en los servicios que se prestan íntegra y directamente "on line", sino también en la cada vez más frecuente integración de actividades "off-line" con versiones o utilidades en línea. O dicho de otro modo, la penetración del mundo "on line" en el que tendemos a definir como "mundo real", pese a que ambos lo son, es cada vez más acusada.

Esto es muy evidente en sectores como el financiero o comercial, donde grandes superficies o bancos aúnan la oferta en establecimientos físicos con alternativas en la red que están cobrando cada vez mayor protagonismo.

El futuro inmediato se anuncia también cargado de novedades en este terreno.

Conceptos como "big data", "internet de las cosas" o "inteligencia artificial", y las tecnologías asociadas a ellos y que los hacen posibles, van a tener, están teniendo ya, un impacto enorme en el ámbito de los datos personales.

Las modernas tecnologías y su empleo de la información personal han mejorado nuestra vida, y sin duda lo harán aún más en los próximos años. Son un factor determinante para el cambio y la innovación.

El acceso a la información y a la formación del que disfrutamos actualmente no tiene comparación con el que se nos ofrecía en un pasado no demasiado lejano.

Una información que es, además, más plural y variada. Ya no hay un número limitado de actores en los procesos de comunicación. Es una comunicación abierta y multidireccional.

Internet, y el uso de nuestra información, nos ofrecen mayores posibilidades de relación personal y una enorme diversidad de formas de gestionar nuestro ocio.

No se puede de ninguna manera ignorar su impacto en la actividad económica. Nuevos negocios, nuevos modelos de negocio, una forma diferente de gestionar las relaciones de las empresas con sus clientes son el resultado de la irrupción de las nuevas tecnologías en el entorno empresarial.

Las nuevas tecnologías son un factor fundamental de generación de riqueza en el marco de la economía digital.

Y es necesario aludir también a sus efectos en el terreno de las políticas públicas, incluidas las relacionadas con la seguridad. Las modernas tecnologías y el análisis de la información contribuyen de manera significativa a una mejor identificación de las necesidades de los ciudadanos y a una mejor prestación de los servicios que demandan.

Igual que lo hacen en la lucha contra la delincuencia, especialmente en sus manifestaciones más graves, tanto en la dimensión preventiva como en la de persecución y enjuiciamiento de los responsables.

Es crucial su papel en el desarrollo de la investigación científica en todos los campos, pero en particular en el de la salud. Gracias a estos avances y a la capacidad que ofrecen de procesar grandes cantidades de información se están pudiendo identificar las causas, y también las respuestas, de enfermedades que hasta ahora se resistían al estudio por métodos tradicionales.

Pero si las posibilidades y ventajas son grandes, también lo son los riesgos que se plantean para los ciudadanos.

Algunos de estos riesgos tienen que ver simplemente con una cuestión de cantidad y de estadística. Cuantos más datos hay circulando sobre más aspectos de las vidas de las personas, más probabilidades hay de que algo vaya mal y de que ese problema tenga consecuencias graves para los afectados.

Problemas que no se refieren sólo a cuestiones de seguridad o de confidencialidad de la información.

También, y sobre todo, afecta a usos no previstos, injustos o ilegales de esa información.

Y todo ello a partir de un uso no autorizado de unas informaciones sobre el que sus titulares no tenían ningún conocimiento.

Muchos de estos problemas obedecen a razones que tienen que ver con el modo en que se ha configurado y ha evolucionado la economía en el entorno digital.

Se trata de un sector que ha conocido un intenso proceso de concentración en poco más de una década. Con un grupo reducido de actores en posiciones dominantes que almacenan cantidades ingentes de información.

Al mismo tiempo, el modelo de negocio de muchos, si no de la mayoría, de prestadores de servicios de la sociedad de la información está basado en la monetización de la información personal de sus usuarios.

En principio, esos datos se comercializan con fines de publicidad. Pero también podría hacerse con otro tipo de finalidades. Por ejemplo, con destino a empresas que quieren conocer los perfiles de sus potenciales clientes para determinar los precios a los que van a ofrecerles sus productos o servicios.

En el ámbito público, donde el uso de la información personal no se mueve por incentivos económicos, los riesgos tienen otros orígenes, y también otras manifestaciones.

El natural interés en disponer de información que optimice las decisiones en materias que afectan a los ciudadanos, desde las prestaciones sociales a la protección de su seguridad e integridad física, puede conducir a una concentración en manos de los poderes públicos de cada vez más datos sobre más dimensiones de las vidas de los ciudadanos a los que sirven.

En definitiva, las posibilidades que las nuevas tecnologías ofrecen para la recogida y tratamiento de la información personal se nos presentan como prácticamente ilimitadas.

Las personas, y así lo confirman todos los estudios que se llevan a cabo, tienen percepciones y posiciones hasta cierto punto contradictorias sobre todos estos fenómenos.

Por un lado, desean beneficiarse y seguir disfrutando de las ventajas y los beneficios que las nuevas tecnologías les ofrecen a partir del uso de sus datos.

Muchas de esas personas afirman que están dispuestas a ofrecer sus datos personales a cambio de servicios.

Pero, al mismo tiempo, esas mismas personas nos dicen que desconfían de los servicios digitales y que quieren recuperar el control, o tener un mayor control, sobre la información que les proporcionan.

Uno de los principales obstáculos para el desarrollo de la economía digital es la falta de confianza de los ciudadanos.

Estamos ante los retos que plantea conciliar desarrollo tecnológico e innovación a partir del uso de la información personal con el respeto a los derechos que los ciudadanos tienen a su intimidad, a su privacidad, a controlar qué sucede con datos que, en último extremo, les pertenecen.

Existe, por tanto, una tarea urgente que es restablecer esa confianza de los ciudadanos sobre el control de sus datos personales.

Recuperar esa confianza es una premisa esencial para el desarrollo de la innovación ya que de ella depende la actitud de los consumidores para interactuar en la economía digital.

Pero, garantizando que los derechos fundamentales de la privacidad no se sacrifiquen en nombre de la innovación y sin que el precio que pagamos por la innovación tenga que ser la renuncia a las garantías sobre nuestros datos personales.

Para lograrlo debemos contar con autoridades que garanticen su aplicación y con una posición activa de los ciudadanos en la protección de sus datos personales.

Familiarizarse con sus derechos y obligaciones, interesarse por los fines y los modos en que se tratan sus datos, hacer un uso razonable de sus posibilidades de control, desde ser cuidadosos a la hora de dar su autorización para tratar los datos hasta estar alertas ante posibles excesos en tratamientos con otras bases legales.

De poco sirve que se den más opciones de control de los propios datos si luego esas opciones no se usan.

Esos retos necesitan respuestas. Respuestas que permitan garantizar los derechos de los ciudadanos en un mundo de servicios globalizados que en muchas ocasiones se prestan desde fuera de la Unión Europea.

Respuestas para actualizar los derechos ya reconocidos y para incorporar nuevos derechos adaptados al entorno digital.

Y respuestas para articular un modelo de cumplimiento por parte de responsables y encargados del tratamiento y de supervisión por parte de las autoridades de control, en los que primen la diligencia y la proactividad para garantizar la protección de los datos personales y la disponibilidad de instrumentos que permitan al regulador involucrarse con las empresas y otras entidades en la garantía de este derecho.

Y, al mismo tiempo que permita superar la tradicional afirmación de que "el derecho va siempre por detrás de la realidad".

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: ÁMBITO DE APLICACIÓN

La Unión Europea, partiendo de una amplia tradición y experiencia previa ha abordado estos retos y ha articulado estas respuestas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Reglamento que ha actualizado y completado el modelo europeo de protección de datos al actual entorno tecnológico. Y lo ha hecho partiendo de una premisa básica como es el reconocimiento de la protección de datos personales como un derecho fundamental.

La prestación de servicios globales en Internet desde terceros países hace necesario superar el criterio tradicional sobre el ámbito de aplicación territorial de las normas vinculado al ámbito geográfico de un Estado.

De no superarse esta concepción y articular criterios que permiten la aplicación extraterritorial de las garantías previstas en las normas, la protección de los datos personales quedará restringida de forma progresivamente acelerada.

El Reglamento da respuesta a esta necesidad y permite su aplicación a quienes tratan datos personales de ciudadanos europeos desde terceros países cuando les dirijan específicamente sus servicios o monitoricen su conducta, práctica que se ha generalizado en los servicios de internet.

LOS PRINCIPIOS DE PROTECCIÓN DE DATOS

Los principios de protección de datos se mantienen similares a la Directiva 95/46/CE, con refuerzo en algunos matices, recogiendo los de:

- Licitud, lealtad y transparencia.
- Limitación de finalidad
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva.

La principal novedad es el reconocimiento jurídico del principio de responsabilidad proactiva.

El RGPD, opta por una doble estrategia de prevención y de flexibilización.

La prevención se persigue a partir de la implantación de un principio de responsabilidad y compromiso proactivos de los responsables con la protección de datos.

Quienes tratan datos deben ser conscientes y conocedores de que lo hacen, de cómo lo hacen y del efecto que esos tratamientos tienen sobre los ciudadanos. A partir de ese conocimiento, han de aplicar unas medidas de cumplimiento que buscan colocar a las organizaciones en condiciones de llevar a cabo los tratamientos que desarrollen respetando los principios y derechos que el Reglamento establece.

Posiblemente ahí radica la novedad más destacada del Reglamento. En que no se limita a fijar unos objetivos de cumplimiento, sino que detalla los mecanismos a aplicar para conseguirlo.

En la forma de aplicar estos mecanismos es donde el Reglamento introduce una dimensión de flexibilidad, ya que no todas las organizaciones han de aplicar todas las medidas previstas, ni todas han de hacerlo del mismo modo.

El criterio diferenciador es el riesgo. Las organizaciones que lleven a cabo tratamientos de alto riesgo habrán de implantar medidas que no son necesarias para las organizaciones que tratan datos en situaciones de riesgo bajo o moderado. Al mismo tiempo, la intensidad y el tipo de riesgo determinan cómo aplicar muchas de las medidas que el Reglamento contempla.

Las medidas de responsabilidad activa previstas en el Reglamento exigen a los responsables del tratamiento realizar un análisis sobre el riesgo que va a suponer para los derechos y libertades de los ciudadanos y para la seguridad de la información, el tratamiento de sus datos personales.

Y, en función de dicho análisis, deben adoptar con carácter previo al tratamiento de datos personales las medidas que permitan excluir o minimizar dichos riesgos o, en caso contrario, renunciar al tratamiento de los datos.

Y todos estos análisis y las medidas que se adopten para cumplir con el Reglamento deben estar documentados y a disposición de las autoridades de control para permitir su verificación. Y, lo que es particularmente importante, deben actualizarse a lo largo del tiempo para adaptarlas a los nuevos tratamientos de datos que se realicen. Posteriormente haré una referencia más detallada a estas medidas.

El RGPD exige, por tanto, un cambio de mentalidad para pasar de un sistema de verificación a otro de responsabilidades proactiva.

LA LEGITIMACIÓN PARA EL TRATAMIENTO

En cuanto a la legitimación para el tratamiento de los datos el RGPD introduce una novedad importante, no respecto a la Directiva 95/46/CE, pero sí sobre la Ley Orgánica 15/1999, de 13 de diciembre (LOPD).

En la LOPD, y también en diversas normas de protección de datos en Latinoamérica, se parte del principio de primar el consentimiento de los afectados como base jurídica que legitima el tratamiento de sus datos. Así, se establece como regla general la necesidad de obtener dicho consentimiento y el resto de las bases jurídicas se articulan como excepciones al consentimiento.

El RGPD modifica este criterio y contempla todas las bases jurídicas del tratamiento en términos de igualdad. Las previstas en dicha norma son las siguientes:

- El consentimiento para el tratamiento de sus datos personales para uno o más fines específicos.
- La ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales.
- El cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento.
- Los intereses vitales del interesado o de otra persona física.
- El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Esta modificación, que debe valorarse muy positivamente.

Son numerosos los casos en los que la base jurídica del tratamiento de datos es una relación contractual, que legitima el tratamiento de la información en todo aquello que sea necesario para el adecuado desarrollo del contrato. Confundir esta base jurídica con la obtención del consentimiento de la contraparte no sólo es innecesario sino que, además, puede resultar contraproducente dado que el consentimiento es esencialmente revocable.

Y, también, existen casos en los que no es posible obtener el consentimiento para tratamientos masivos de datos o la exigencia del consentimiento no permite garantizar intereses legítimos del responsable del tratamiento o de terceros, como puede suceder por ejemplo en el tratamiento de datos con fines de evitar el fraude en la contratación de bienes o servicios.

De ahí que deba apreciarse la incorporación de una base jurídica como es la satisfacción del interés legítimo del responsable o de terceros, sin consentimiento.

Sin que ello suponga la prevalencia general del interés legítimo sobre los derechos e intereses de los afectados pues deberá realizarse, caso a caso, una ponderación entre unos y otros y la incorporación de garantías adecuadas que permitan acreditar la prevalencia de aquel interés legítimo.

Para ello, será necesario aplicar, entre otros, el principio de la expectativa razonable derivada de la relación del afectado con el responsable y los supuestos de interés legítimo que citan los Considerandos 47 a 49 del Reglamento.

En cuanto al consentimiento debe ser libre, específico, informado e "inequívoco" y manifestarse a través de declaraciones o "claras acciones afirmativas".

Sobre el consentimiento el Reglamento incorpora algunas aclaraciones adicionales.

Se considera que puede existir un acto afirmativo claro en supuestos como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (Cdo.32).

También puede considerarse un acto afirmativo el marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta. El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento (Cdo. 32).

Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos (Cdo.32).

El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirarlo sin sufrir perjuicio alguno (Cdo.42).

Y, tampoco debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento (Cdo.43).

Respecto de los conocidos como datos sensibles, que el RGPD denomina categorías especiales de datos, las principales novedades son las siguientes:

- Se incluyen los datos genéticos y biométricos.
- Se excluyen los datos de infracciones y sanciones administrativas.

Como regla general queda prohibido su tratamiento. Sin embargo, se contemplan excepciones a la prohibición como son el consentimiento del afectado, la habilitación en el ámbito del derecho laboral y de seguridad o protección social (que puede basarse en un Convenio Colectivo), el tratamiento para la protección de intereses vitales del afectado o de un tercero, los datos hechos manifiestamente públicos por el interesado o el tratamiento necesario por razones de interés público esencial según el derecho de la UE o el derecho nacional, siempre que sea proporcional a la finalidad perseguida.

Sobre el consentimiento de menores el RGPD lo fija en 16 años, pudiendo los Estados Miembro reducirlo hasta los 13 años.

DERECHOS DE PROTECCIÓN DE DATOS

El Reglamento recoge el catálogo tradicional de derechos con tres novedades, a las que se añade la nueva configuración del derecho de información. Los nuevos derechos son el derecho al borrado y al olvido, la limitación del tratamiento y la portabilidad.

El Reglamento configura la información como un derecho del interesado y no como obligación del responsable y amplía la información que habrá de facilitarse cuando los datos se recaban del afectado, incluyendo como novedades, entre otras, los datos de contacto del delegado de protección de datos, los fines y base jurídica del tratamiento, los intereses legítimos del responsable o de un tercero, los destinatarios o las categorías de destinatarios de los datos personales, las transferencias internacionales previstas, el plazo de conservación o los medios para determinarlo y la existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias de las mismas.

Si los datos no se recaban del interesado deberá además informársele de las categorías de datos que se van a tratar y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

En todo caso la información debe facilitarse de forma clara, concisa y accesible.

No obstante, se prevén excepciones al deber de información. Con carácter general se exceptúa, lógicamente, cuando el interesado ya disponga de la información.

Y, si los datos no proceden del interesado, cuando concurra un esfuerzo desproporcionado en el caso de tratamientos con fines de archivo, estadísticos o de investigación científica o histórica; lo exija una previsión legal expresa o una obligación de secreto legal o profesional.

Las condiciones generales sobre el ejercicio de derechos son la obligación de atenderlos a menos que se acredite la imposibilidad de identificar al interesado, la respuesta por medios electrónicos si el derecho se ejercitó por dichos medios salvo que el interesado manifieste lo contrario, y la gratuidad salvo en caso de solicitudes manifiestamente infundadas o excesivas. En cuyo caso será posible

cobrar un canon o negarse a actuar respecto de la solicitud.

El derecho a la limitación del tratamiento puede ejercerse mientras se verifica la exactitud de los datos en casos de impugnación por el interesado; cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales; cuando el interesado necesite que el responsable conserve los datos para la formulación, el ejercicio o la defensa de reclamaciones, y mientras se verifican las circunstancias que se hayan alegado en el ejercicio de la modalidad de derecho de oposición regulado en el artículo 21.1 del RGPD.

El derecho a la portabilidad es el derecho del interesado a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica.

O a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos.

Los requisitos acumulativos para que pueda ejercitarse son que el tratamiento esté basado en el consentimiento o en un contrato y se efectúe por medios automatizados.

En cuanto al modo de ejercicio, podrá implicar la transmisión directa de responsable a responsable a instancia del interesado "cuando sea técnicamente posible".

El derecho a la portabilidad se exceptúa cuando el tratamiento se funde en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

En cuanto al contenido del derecho el Comité Europeo de Protección de Datos ha indicado que será aplicable a los datos facilitados directamente o resultado del funcionamiento, pero no a los datos inducidos (Directrices sobre el derecho a la portabilidad de los datos, adoptadas el 5 de abril de 2017).

El derecho a la supresión sustituye al de cancelación, actualizándolo al entorno de internet cuando el responsable haya hecho públicos los datos. Así, cuando el responsable haya hecho públicos los datos y proceda la supresión tendrá la obligación de informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos, siempre que lo permita la tecnología disponible y el coste de su aplicación. De este modo se pretende garantizar la eficacia del derecho en entornos de gran viralidad como es el de los servicios en internet.

Como excepciones al derecho de supresión se recogen el ejercicio de las libertades de expresión e información, el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, el tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, la concurrencia de razones de interés público en el ámbito de la salud pública o de fines de archivo en interés público, de investigación científica o histórica o fines estadísticos, en la medida en que el derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, así como en caso de tratamientos para la formulación, ejercicio o defensa de reclamaciones.

El derecho de oposición tiene varias modalidades.

La primera (art.21.1) afecta a los tratamientos cuya base jurídica se encuentra en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, o en la satisfacción del interés legítimo del responsable o de terceros.

En estos casos todos los interesados tienen derecho a oponerse en cualquier momento al tratamiento de datos alegando motivos relacionados con su situación particular y el responsable dejará de tratarlos salvo que acredite motivos legítimos imperiosos que prevalezcan sobre los del interesado o para la formulación, el ejercicio a la defensa de reclamaciones.

La segunda recoge el derecho de oposición a la mercadotecnia directa (art.21.2) y dará lugar al cese en el tratamiento de los datos sin necesidad de motivación.

Finalmente, el derecho de oposición puede ejercitarse respecto de los tratamientos con fines de investigación científica o histórica o estadísticos, pudiendo limitarse si son necesarios para el cumplimiento de una misión de interés público (art.21.6).

El RGPD reconoce también el derecho a no ser objeto de una decisión automatizada, incluida la elaboración de perfiles, que produzca efectos sobre el afectado o le afecte significativamente de modo similar.

Se exceptúa cuando sean necesarias para la celebración o ejecución de un contrato, esté autorizada por el derecho nacional o de la UE o se base en el consentimiento explícito.

No obstante, salvo en el caso de la habilitación legal, el interesado tiene derecho a obtener intervención humana en la decisión y a que pueda dar su opinión e impugnar la decisión.

Salvo que exista consentimiento explícito o interés público, no podrá implicar el tratamiento de datos sensibles.

MEDIDAS DE RESPONSABILIDAD PROACTIVA

Anteriormente se hizo referencia a las implicaciones del principio de responsabilidad proactiva; referencia que debe completarse ahora con una descripción sintética de las medidas que implica.

La primera de ellas es la protección de datos desde el diseño que exige adoptar medidas técnicas y organizativas adecuadas (por ejemplo, seudonimización, minimización) para aplicar los principios de protección de datos de forma eficaz y proteger los derechos.

Estas medidas deben adoptarse tanto en el momento de determinar los medios para el tratamiento como en el momento en que éste se lleve a cabo y, deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, los riesgos de diversa probabilidad y gravedad (no sólo el alto riesgo) y el estado de la técnica y el coste.

Asimismo, debe aplicarse la protección de datos por defecto, que implica adoptar medidas técnicas y organizativas apropiadas para que por defecto sólo se traten los datos personales necesarios para cada fin específico. Esta obligación se aplica a la cantidad de datos recopilados, la extensión del tratamiento, el periodo de almacenamiento y a su accesibilidad. En particular, deben garantizar que se evite la accesibilidad a un número indeterminado de personas físicas sin la intervención de la persona.

Cada responsable y encargado tienen la obligación de llevar un registro de actividades de tratamientos que es el punto de partida sobre el que aplicar las restantes medidas de cumplimiento. El registro deberá contener la identificación y datos de contacto de responsable, corresponsable, representante y delegado de protección de datos (DPD), los fines del tratamiento, la descripción de las categorías de interesados y datos personales, las categorías de destinatarios existentes o previstos, las transferencias internacionales de datos a terceros países u organizaciones internacionales y la documentación de garantías para las transferencias exceptuadas sobre base de intereses legítimos imperiosos, así como cuando sea posible, los plazos previstos para la supresión de datos y la descripción general de medidas de seguridad.

Partiendo de las actividades de tratamiento registradas deberá realizarse el análisis de riesgo que se describió anteriormente para analizar si deben adoptarse o no algunas medidas como las evaluaciones de impacto en la protección de datos o la designación obligatoria de un delegado de protección de datos.

En todo caso, el análisis de riesgo debe permitir adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica y los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento y los riesgos para los derechos y libertades de las personas.

La adhesión a un código de conducta o a un mecanismo de certificación podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad.

En relación con la seguridad el Reglamento ha incorporado la obligación de notificar las violaciones de seguridad de los datos.

La notificación debe realizarse a la autoridad de protección de datos sin demora y a más tardar en 72 horas desde que se haya tenido constancia. Si se realiza más tarde debe aportarse justificación motivada. No existirá esta obligación cuando "sea improbable que la violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas".

El Reglamento prevé un contenido mínimo de la notificación y exige documentar todas las violaciones de seguridad.

Específicamente el encargado del tratamiento está obligado a notificar sin dilación indebida las violaciones de seguridad al responsable que le contrató.

Asimismo, se prevé la posible notificación a los interesados cuando es probable que la quiebra entrañe alto riesgo para los derechos y libertades de interesados y sin dilación indebida.

Se exceptúan los casos en que se hayan implementado medidas de protección tecnológica que haga ininteligibles los datos a terceros no autorizados (por ejemplo, datos encriptados) o medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.

La autoridad de protección de datos puede obligar a notificar a interesados.

La evaluación de impacto deberá realizarse cuando sea probable que el tratamiento previsto presente un alto riesgo específico para los derechos y libertades de los interesados, entre otros casos, cuando:

- Se elaboren perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Se realice un tratamiento a gran escala de las categorías especiales de datos.
- Se realice una observación sistemática a gran escala de una zona de acceso público.

Las autoridades de protección de datos deberán establecer listas adicionales de tratamientos de alto riesgo y podrán establecer listas de los que no requieren evaluación de impacto de protección de datos.

El RGPD prevé un contenido mínimo de la evaluación que incluye:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- una evaluación de los riesgos para los derechos y libertades de los interesados.
- las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Como novedad, se prevé que habrá de recabarse "cuando proceda" la opinión de los interesados.

Cuando una evaluación de impacto de protección de datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación, deberá consultarse a la autoridad de protección de datos que podrá asesorar por escrito al responsable, y en su caso al encargado y utilizar cualquiera de sus poderes, incluido prohibir el tratamiento.

Asimismo se contempla la obligación de consulta en la elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que la aplique.

Por su parte, el derecho nacional podrá establecer la obligación de consulta y la petición de autorización previa en tratamientos realizados en el ejercicio de una misión realizada en interés público, en particular, sobre la protección social y la salud pública.

El Reglamento regula la novedosa figura del delegado de protección de datos exigiendo en algunos casos la obligatoriedad de su designación.

El RGPD requiere la designación de un DPD en tres casos específicos:

- Cuando el tratamiento se realice por una autoridad u organismo público (independientemente de los datos que se estén procesando).
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en operaciones de tratamiento que exigen un control periódico y sistemático de los datos a gran escala.
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en procesar a gran escala categorías especiales de datos o datos personales relativos a condenas y delitos penales.

El DPD puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento, o cumplir las tareas sobre la base de un contrato de servicios celebrado con un individuo u organización.

En las Administraciones Públicas puede nombrarse un solo DPD para varias entidades.

Las funciones del DPD son las siguientes:

- Informar y asesorar a responsable y encargado, documentando esa actividad.
- Supervisar la puesta en práctica de las políticas de protección de datos, incluidas la formación y la auditoría.
- Supervisar la aplicación del Reglamento en lo relativo a privacidad desde el diseño y por defecto y a los derechos de los interesados.
- Asegurar la existencia y mantenimiento de documentación obligatoria.
- Supervisar gestión de quiebras de seguridad.

- Supervisar la realización de Evaluaciones de Impacto y la solicitud de autorizaciones o consultas que se requieran.
- Supervisar respuestas a requerimientos de las autoridades de protección de datos.
- Cooperar con la autoridad de protección de datos en el marco de sus tareas.
- Actuar como punto de contacto para la autoridad de protección de datos y los interesados.

Debe comunicarse y ser accesible a los interesados de su identidad al público, así como tener acceso directo a la dirección.

De esta enumeración se desprende que el DPD no es el obligado a cumplir la norma; obligación que recae en el responsable o encargado del tratamiento sino un colaborador cualificado que le ayuda. Y, por tanto, no puede realizar tareas que impliquen un conflicto de intereses con sus funciones.

Por ello, el DPD no puede ocupar un puesto dentro de la organización que lo conduzca a determinar los propósitos y los medios del tratamiento de los datos personales. Debido a la estructura organizativa específica en cada organización, esta situación debe ser considerada caso por caso.

Como regla general, las posiciones conflictivas pueden incluir las de alta dirección, jefe de recursos humanos o jefe de departamentos de tecnologías de la información, pero también otros roles más bajos en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de procesamiento.

En consecuencia, los DPD no son personalmente responsables por el incumplimiento del RGPD. El RGPD deja claro que es el responsable del tratamiento o del procesador quien debe garantizar y demostrar que el tratamiento se realiza de conformidad con el presente Reglamento.

El RGPD exige que el DPD se designe sobre la base de cualidades profesionales y, en particular, conocimientos especializados sobre la legislación y las prácticas en materia de protección de datos y sobre la capacidad para cumplir las tareas a que se refiere el artículo 39.

Estas habilidades y experiencia se refieren a:

- Experiencia en las leyes y prácticas nacionales y europeas en materia de protección de datos, incluida una comprensión en profundidad del RGPD.
- Comprensión de las operaciones de tratamiento realizadas.
- Comprensión de las tecnologías de la información y la seguridad de los datos.
- Conocimiento del sector empresarial y de la organización.
- Capacidad para promover una cultura de protección de datos.

Dependiendo de la naturaleza de las operaciones de procesamiento y las actividades y tamaño de la organización, deben ser proporcionados al DPD los siguientes recursos:

- Apoyo activo de la función del DPD por parte de la alta dirección.
- Tiempo suficiente para que los DPD cumplan sus obligaciones.
- Apoyo adecuado en términos de recursos financieros, infraestructura (locales, instalaciones, equipo) y personal, cuando corresponda.
- Comunicación oficial de la designación del DPD a todo el personal.
- Acceso a otros servicios dentro de la organización para que los DPD puedan recibir apoyo esencial, aportaciones o información de esos otros servicios.
- Entrenamiento continuo.

Las salvaguardias que permiten al DPD realizar sus tareas de manera independiente consisten en que no puede recibir ninguna instrucción de los responsables o encargados sobre el ejercicio de las tareas del DPD y tampoco puede ser despedido o sancionado por el desempeño de las tareas de DPD.

RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

Respecto de los dos principales sujetos obligados, es decir, el responsable y el encargado del tratamiento, el RGPD ha introducido novedades dirigidas a reforzar el régimen de garantías aplicable a las relaciones entre ambos.

La primera de ellas es la exigencia de una obligación general de diligencia por parte del responsable en la selección del encargado del tratamiento.

De este modo, en el momento de seleccionar a un prestador de servicios que va a acceder a los datos personales no bastará con evaluar las condiciones organizativas y tecnológicas o el precio, sino que será necesario evaluar las garantías que ofrece sobre el tratamiento. Diligencia que deberá documentarse para poder acreditar el cumplimiento del RGPD.

Adicionalmente, el Reglamento incorpora una regulación más detallada del contrato entre ambos que debe incluir:

- El objeto, duración, naturaleza y finalidad del tratamiento, el tipo de datos personales, las categorías de interesados afectados, y las obligaciones y derechos del responsable del tratamiento.
- La obligación de tratar los datos únicamente siguiendo instrucciones documentadas del responsable.
- La garantía de confidencialidad de las personas que manejen datos.
- Las medidas de seguridad.
- En caso de contratación de subencargados la autorización previa, general o específica, del responsable, y la posibilidad de rechazar subencargados.
- La asistencia al responsable en el ejercicio de derechos y en el cumplimiento de obligaciones, las de seguridad, notificación de violaciones de seguridad, evaluaciones de impacto y consulta previa a la AEPD.

Finalmente, añade algunas previsiones particulares como la previsión de que el responsable realice auditorías y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable y la obligación de informar al responsable "si, en su opinión, una instrucción infringe el presente Reglamento o las disposiciones nacionales o de la Unión en materia de protección de datos".

CÓDIGOS DE CONDUCTA Y CERTIFICACIÓN

Para facilitar el cumplimiento de sus previsiones el Reglamento promueve la elaboración de códigos de conducta teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

Los códigos de conducta son, por tanto, sistemas de autorregulación que pueden incluir todas o parte de las medidas de cumplimiento.

Sobre ellas cabe destacar que el RGPD promueve la inclusión de procedimientos de mediación y resolución extrajudicial de conflictos y prevé la creación de mecanismos específicos de supervisión, sin perjuicio de las competencias de la autoridad de protección de datos.

Estos organismos de supervisión deben ser acreditados por la APD, incluyendo criterios sobre su independencia y pericia, los procedimientos de evaluación y supervisión, los procedimientos para atender reclamaciones de interesados y garantizar la ausencia de conflicto de intereses.

Los códigos de conducta aprobados por la autoridad de protección de datos garantizan a los responsables adheridos una presunción de cumplimiento del RGPD en las materias que comprenda.

Complementariamente, el Reglamento promueve la creación de mecanismos de certificación y de sellos y marcas de protección de datos con el fin de demostrar el cumplimiento de lo dispuesto en el Reglamento y permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

La Agencia Española de Protección de Datos, en colaboración con la Entidad Nacional de Acreditación (ENAC) ha desarrollado un esquema de certificación para la figura del DPD.

TRANSFERENCIAS INTERNACIONALES DE DATOS

En la regulación de las transferencias internacionales de datos el Reglamento parte del criterio clásico de que los datos objeto de tratamiento en la UE sólo pueden transferirse a países que garanticen un nivel adecuado de protección equiparable al europeo. O que se acompañen de garantías adecuadas.

El Reglamento mantiene la previsión sobre la declaración por parte de la Comisión Europea del nivel adecuado de protección para un tercer país. Pero la flexibiliza admitiendo que puede referirse no sólo a íntegramente a un país, sino también a uno o varios sectores de actividad específicos o a parte del territorio del país tercero, así como a una organización internacional.

Las decisiones de adecuación ya adoptadas se mantienen en vigor hasta que la Comisión proceda a su revisión para su adaptación al RGPD.

Ante esta perspectiva, los estándares de la Red Iberoamericana de Protección de Datos constituyen una herramienta estratégica para la adaptación de la normativa vigente o futura de protección de datos en Latinoamérica al Reglamento, en un lenguaje jurídico propio de la región.

Respecto de las transferencias internacionales basadas en otros instrumentos de garantía también se flexibiliza la regulación admitiendo expresamente que tanto responsables como encargados del tratamiento puedan ser exportadores de datos; regulando detalladamente las normas corporativas vinculantes y admitiendo su aplicación a res-

ponsables y encargados; así como contemplando la posibilidad de que los códigos de conducta y los esquemas de certificación, junto con compromisos vinculantes y ejecutables del responsable o encargado en el tercer país para aplicar las salvaguardas apropiadas, incluidos los derechos del interesado, amparen los flujos internacionales de datos.

Asimismo, se mantienen las cláusulas contractuales estándar aprobadas por la Comisión Europea como garantías adecuadas en esta materia con la muy importante novedad respecto de la LOPD, de que no necesitan ser autorizadas por la Agencia Española de Protección de Datos. Y se admiten las cláusulas contractuales estándar aprobadas por una autoridad nacional y aceptadas por la Comisión.

En conclusión, el Reglamento es consciente de la importancia de facilitar los flujos internacionales de datos, dotando a los instrumentos de garantía aplicables de una mayor flexibilidad.

EL MODELO DE SUPERVISIÓN

El RGPD exige también una conducta proactiva por parte de la Agencia porque, como se ha señalado, el RGPD también modifica el modelo de supervisión por parte de las autoridades de protección de datos.

El Reglamento contempla una obligación de supervisión activa que exige que la Agencia pueda y deba analizar los procesos que ponen en riesgo el derecho a la protección de los datos personales.

Para ello, el RGPD fomenta el establecimiento de medios orientados a agilizar el análisis de las incidencias y su resolución, como los "arreglos amistosos" (Considerando 131), procedimientos de mediación y resolución de conflictos extrajudiciales, los códigos de conducta, la aprobación de mecanismos de certificación o la figura del DPD.

Todo ello, sin perjuicio del derecho de los ciudadanos a presentar reclamación ante la Autoridad de Control, y por supuesto, de su derecho a la tutela judicial efectiva ante los tribunales.

Además el RGPD abre la puerta a proteger los datos desde otro prisma. No sólo se trata de analizar la reclamación del afectado, para dar solución a su problema individual, sino también de valorar la reclamación como fuente de información que arroje luz sobre el origen del problema: es decir, el sistema de gestión de datos del responsable del tratamiento. Por tanto: la reclamación, más allá de una denuncia, es un síntoma del cumplimiento o incumplimiento de la norma.

Las reclamaciones presentadas ante las autoridades de control deben servir para:

- Que la autoridad de control proceda a adoptar las medidas más eficaces para corregir la situación.
- Analizar las causas que originaron esa situación.
- Analizar las medidas adoptadas para evitar que esa situación pueda volver a producirse.

En resumen, la autoridad de control debe:

- Velar por proteger al sujeto lesionado en sus derechos.
- Velar por impedir que otros estén sufriendo o puedan sufrir ese perjuicio.
- Analizar si esa situación responde a una falta de diligencia y, en último término, a un incumplimiento del principio de responsabilidad.

En consecuencia, el régimen sancionador no debe ser siempre la primera opción. Para ser más exactos, tal vez se podría hablar de régimen corrector, puesto que el análisis de esta situación va acompañado de una pluralidad de medidas (poderes correctivos) que las autoridades de control pueden adoptar de modo proporcionado y disuasorio.

Poderes correctivos que incluyen, entre otros, la advertencia o un apercibimiento dotado de gran flexibilidad frente a la rigidez de la actual previsión de la LOPD , que podrán adoptarse en lugar de una sanción económica cuando, pese a producirse un error, se aprecie y documente una adecuada diligencia en el cumplimiento del RGPD.

Ahora bien, junto con estos poderes correctivos el Reglamento incorpora un régimen sancionador con muy importantes multas que pretenden poder ser disuasorias frente al incumplimiento de la norma.

Sanciones que pueden alcanzar hasta 10 o 20 millones de euros o el 2% o 4% de volumen de negocio anual.

Un elemento determinante para decidir sobre la aplicación de acciones correctivas o de sanciones, multas administrativas será sin duda, la diligencia asociada al principio de responsabilidad proactiva que esté adecuadamente documentada para permitir su acreditación: la acreditación documentada de esa diligencia favorecerá la adopción de medidas correctivas y su omisión o su acreditación puramente formal sin adaptación real a los tratamientos de datos personales puede conducir a la imposición de sanciones económicas.

En cuanto a la adopción de medidas disuasorias en caso de incumplimiento, habitualmente se hace hincapié en los umbrales máximos de las sanciones económicas pero quizá esté pasando desapercibido el hecho de las autoridades de control también pueden, en vez de imponer una multa, o además de imponerla, ordenar medidas como por ejemplo la limitación o la suspensión del tratamiento, que impedirían a un responsable continuar llevando a cabo esos tratamientos que constituyen un riesgo para los derechos y libertades de los ciudadanos. Medidas que refuerzan el abanico de opciones para garantizar los derechos de los ciudadanos y que son disuasorios para que ningún modelo de negocio pueda sustentarse sobre un debilitamiento de la defensa de los derechos y libertades de las personas.

EL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

Un objetivo esencial del Reglamento que justifica la propia naturaleza de esta norma es contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica en la Unión Europea.

En la consecución de ese objetivo juegan un papel fundamental los mecanismos de cooperación y coherencia y la actividad del Comité Europeo de Protección de Datos, previstos en el Reglamento.

En este sentido, el Grupo Europeo de Autoridades de Protección de Datos, conocido como Grupo del Artículo 29, ha dedicado la práctica totalidad de su actividad en 2018 a preparar la aplicación del RGPD.

Esta tarea de preparación ha incluido tanto iniciativas dirigidas a ciudadanos, responsables y encargados, como otras más orientadas a ofrecer criterios de actuación a las propias autoridades miembros del Grupo y a hacer posible el establecimiento del actual Comité Europeo de Protección de Datos.

De cara a ciudadanos y responsables, el GT29 ha adoptado una serie de Directrices sobre aspectos centrales del Reglamento, eligiendo temas en los que, por su novedad, o por la falta de concreción de las disposiciones del RGPD, se ha considerado más necesario proporcionar criterios e interpretaciones armonizados.

Entre estas Directrices pueden citarse las relativas al consentimiento, a la transparencia, a las decisiones individuales automatizadas y perfilado, al derecho a la portabilidad o a la notificación de quiebras de seguridad.

También se han aprobado directrices de actualización de la posición del Grupo en relación con los instrumentos para transferencias internacionales, fundamentalmente BCRs, aunque también sobre criterios para la declaración de nivel de protección adecuado de países terceros.

Estos documentos se suman a los adoptados a principios de 2017 sobre delegados de protección de datos, identificación de la autoridad principal y evaluaciones de impacto.

Esta línea de actuación tendrá continuidad, tras el establecimiento del Comité Europeo de Protección de Datos. De hecho, en su primera reunión, el Comité adoptó dos nuevas directrices, unas sobre criterios de certificación y otras sobre la aplicación de las exclusiones para transferencias internacionales previstas por el Reglamento.

BIBLIOGRAFÍA

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

DIC
TÁ
ME
NES

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen Nº	Expediente Nº
1/2017	2015-2-10-0000575

Montevideo, 14 de marzo de 2017

VISTO: La consulta realizada por el Sr. Daniel Mathó, respecto a la procedencia de la publicación de información en internet y su adecuación a la Ley Nº 18.331, de 11 de agosto de 2008.

RESULTANDO:

I) Que el consultante señala que la Caja de Jubilaciones y Pensiones de Profesionales Universitarios (en adelante la Caja) publica en su página web el padrón de afiliados, distinguiendo entre jubilados y quienes no lo están, pero sin indicar en el caso de estos últimos si declararon o no actividad profesional, y en consecuencia si aportan o no a dicha Institución.

II) Que esta aclara en su página web que no brinda información respecto al estado de ejercicio o no de los profesionales no jubilados *"por estar ello vedado por la normativa aplicable al respecto (art. 47 del Código Tributario y art. 9º Ley 18.331)".*

III) Qué, en definitiva, el consultante solicita a esta Unidad si esta interpretación de la Caja es acorde a las normas en materia de protección de datos, o si ésta podría informar quién tiene ejercicio liberal y hace sus aportes y quién no. Ejemplifica con otras situaciones como la puesta a disposición de la información del Banco de Previsión Social, la Dirección General Impositiva, o el Banco Central del Uruguay.

CONSIDERANDO:

I) Que la información sobre el estado de afiliados a la Caja se enmarca en el concepto de comunicación de datos personales según el art. 4 Lit. B) de la Ley N° 18.331, que la define como toda revelación de datos realizada a una persona distinta del titular de los datos.

II) Que dicha comunicación está regida por el art. 17 de la esa Ley, por lo cual al efecto debe existir interés legítimo del emisor y del destinatario de los datos, además de contar con el previo consentimiento informado del titular de estos, sin perjuicio de las excepciones previstas en la misma disposición y en el art. 9.

III) Que esta Unidad ya se ha pronunciado a través del Dictamen Nº 4/2015, de 18 de marzo de 2015 en el sentido de que el dato de si los afiliados a la Caja se encuentran en situación de ejercicio liberal de su profesión requiere del previo consentimiento de los titulares, no estando comprendido en las excepciones previstas en el artículo 17 de la Ley.

IV) Que por otra parte corresponde considerar que el art. 47 del Código Tributario establece que la Administración Tributaria y los funcionarios que de ella dependen, están obligados a guardar secreto de las informaciones que resulten de sus actuaciones administrativas o judiciales, lo que se extiende a la Caja por lo dispuesto en el artículo 1º del mencionado Código.

V) Que asimismo, el hecho de que se obtenga información en línea de los certificados del Banco de Previsión Social y la Dirección General Impositiva a través del número del Registro Único de Contribuyentes no implica que se haya prescindido del consentimiento de los titulares de los datos, en tanto la obtención de dicho número a efectos de la consulta debe haberse realizado por la voluntad expresa del contribuyente o al amparo de alguna de las excepciones previstas en la normativa aplicable.

ATENTO: A lo expuesto, y a lo previsto en la Ley N° 18.331, su decreto reglamentario y demás normas concordantes y complementarias.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que corresponde estar a lo dispuesto por Dictamen Nº 4/2015 de 18 de marzo de 2015, en el sentido de que el "estado" de los afiliados a la Caja de Jubilaciones y Pensiones de Profesionales Universitarios es un dato que requiere del previo consentimiento informado del titular para su comunicación. 2º.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen Nº	Expediente Nº
2/2017	2017-2-10-0000017

Montevideo, 26 de abril de 2017

VISTO: Las preguntas planteadas por la División de Inversión Pública de la Oficina de Planeamiento y Presupuesto de la Presidencia de la República (en adelante OPP) relacionadas al Sistema Nacional de Inversión Pública (en adelante SNIP) creado por el artículo 23 de la Ley Nº 18.996, de 7 de noviembre de 2012.

RESULTANDO:

I) Que dicho organismo plantea en su consulta las siguientes preguntas vinculadas a temas relativos a la competencia de esta Unidad: "¿Es necesario que el Sistema Nacional de Inversión Pública registre el Banco de Proyectos en la Unidad de Protección de Datos Personales, en la medida que utiliza un sistema de usuarios para el ingreso de la información por parte de los organismos públicos alcanzados?, ¿A quién corresponde la propiedad de la información registrada en el Banco de Proyectos; al organismo que la registró o al SNIP?".

CONSIDERANDO:

I) Que los conjuntos de información registrables se identifican en torno a la finalidad para la cual se tratan los datos personales y no en función del soporte que los contiene, sea éste físico o lógico.

II) Que la OPP es responsable de la base de datos que sustenta el SNIP, en tanto conjunto de información cuya titularidad, gestión y administración le es asignada legalmente, continente de datos personales de personas físicas y jurídicas y creada con la finalidad específica de optimizar la asignación de recursos públicos, la cual debe diferenciarse del sistema informático que la soporta.

III) Que asimismo, la OPP es responsable de la base de datos relativa al registro de usuarios para acceder al SNIP.

IV) Que la OPP es titular de una base de datos nutrida por los organismos y tratada con la finalidad específica que le encomienda la Ley Nº 18.996, de optimizar la asignación de recursos públicos, a cuyos efectos se le confieren competencias y atribuciones que implican decidir sobre la finalidad de la información y por ende, ser responsable de este conjunto de información al tenor de lo dispuesto en el literal K) del artículo 4 de la Ley Nº 18.331, de 11 de agosto de 2008.

ATENTO: A lo expuesto e informado, y a lo previsto en los artículos 31 y 34 de la Ley N° 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La Oficina de Planeamiento y Presupuesto es responsable de la base de datos nutrida por los organismos y tratada con la finalidad específica que le encomienda la Ley Nº 18.996, de 7 de noviembre de 2012, de optimizar la asignación de recursos públicos, la cual debe registrarse ante esta Unidad.

2.- Asimismo, la Oficina de Planeamiento y Presupuesto es responsable de la base de datos de registro de usuarios para acceder al Sistema Nacional de Inversión Pública, la cual debe inscribirse ante esta Unidad, salvo que se relacione con un registro previamente realizado.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Dr. Felipe Rotondo

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen Nº	Expediente Nº
3/2017	2017-2-10-0000080

Montevideo, 14 de junio de 2017

VISTO: La consulta formulada por la Dirección General de Registros (en adelante DGR) en relación a la situación planteada ante el Registro de Personas Jurídicas, Sección Asociaciones Civiles y Fundaciones, por la Asociación de Estudios del Cannabis del Uruguay (en adelante la Asociación), en representación de los Clubes Cannábicos.

RESULTANDO:

I) Que la consultante expresa que la Asociación formuló ante el Registro mencionado una petición solicitando que no se brinden a terceros los testimonios de estatutos de los Clubes Cannábicos creados cómo Asociaciones Civiles conforme lo dispuesto por la Ley Nº 19.172, de 20 de diciembre de 2013 y su Decreto reglamentario Nº 120/014, de 6 de mayo de 2014. Ello fundado en que dicha publicidad implicaría conocer datos que a entender de la Asociación tienen la calidad de sensibles, incurriendo en consecuencia en violación de la mencionada Ley, y de la Ley Nº 18.331, de 11 de agosto de 2008.

II) Que solicitada información adicional, la DGR informa que se expiden cuatro clases de certificados en el Registro de Personas Jurídicas, Sección Asociaciones Civiles y Fundaciones. En dos de ellos se expide testimonio de los estatutos de creación de las Asociaciones o Fundaciones al interesado y a terceros, y en los dos restantes solamente se entregan datos que no están referidos por la Ley N° 19.172 como datos sensibles.

CONSIDERANDO:

I) Que no resultan aplicables las normas vinculadas al Registro de Bases de Datos establecidas en la Ley Nº 18.331 a los registros llevados por la DGR, por contar estos con regulación especial (en particular la Ley N° 16.871, de 28 de setiembre de 1997). No obstante, la Ley Nº 19.172 en su artículo 8° establece que la identidad de los miembros de los Clubes Cannábicos se constituye en un dato sensible al amparo de lo dispuesto por el artículo 18 de la primera de las mencionadas.

II) Que por otra parte, los Clubes Cannábicos deben constituirse como Asociaciones Civiles atento a lo dispuesto por el artículo 21 del Decreto 120/014, lo que importa la inscripción de sus estatutos en el Registro de Personas Jurídicas sección Asociaciones Civiles y Fundaciones, y potencialmente la comunicación de la información contenida en éstos a terceros, a través de solicitudes de información registral.

III) Que corresponde en consecuencia armonizar las disposiciones vinculadas a la publicidad registral con las normas en materia de protección de datos personales.

IV) Que en ese sentido, y por tratarse de datos sensibles regulados por el artículo 18 de la Ley N° 18.331 y por una serie de normas especialmente tuitivas explicitadas especialmente en la Ley N° 19.172, cuando se le solicita información por un tercero respecto de Clubes Cannábicos constituidos como Asociaciones Civiles, la DGR no debe entregar información sobre la identidad de los miembros y titulares de estos clubes, sin su consentimiento expreso y escrito, salvo que se empleen mecanismos de anonimización previa de esta información.

ATENTO: A lo expuesto, y a lo previsto en las normas anteriormente citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que la Dirección General de Registros podrá entregar a terceros, cuando se solicite información sobre los Clubes Cannábicos en el Registro de Personas Jurídicas, Sección Asociaciones Civiles y Fundaciones, únicamente las solicitudes de vigencia y las solicitudes de testimonio de la resolución ministerial.

2.- Que la Dirección General de Registros podrá entregar a terceros, cuando se solicite información sobre los Clubes Cannábicos en el Registro de Personas Jurídicas, Sección Asociaciones Civiles y Fundaciones, la solicitud del Primer Testimonio de la última versión del estatuto aprobado y la solicitud de testimonios del estatuto (segundos o ulteriores), debidamente anonimizada, o contando con consentimiento previo, expreso y por escrito de los titulares de los datos.

3.- Notifíquese, publíquese y archívese.

Fdo.: Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen Nº	Expediente Nº
4/2017	2016-2-10-0000567

Montevideo, 12 de julio de 2017

VISTO: La consulta presentada por el Banco de Previsión Social (en adelante BPS), la Caja de Jubilaciones y Pensiones de Profesionales Universitarios (en adelante CJPPU), la Caja de Jubilaciones y Pensiones Bancarias (en adelante CJPB) y la Caja Notarial de Seguridad Social (en adelante CNSS) sobre intercambio de información.

RESULTANDO:

I) Que el intercambio proyectado se funda en la necesidad de cooperación interinstitucional para una correcta aplicación de los respectivos programas de prestaciones económicas de seguridad social. La información a intercambiar consiste en datos identificatorios sobre las personas y sus vínculos, sobre sus prestaciones o beneficios y sobre su actividad amparada por cada una de las entidades consultantes.

II) Que la Ley N° 18.719, de 27 de diciembre de 2010 manda a las entidades públicas estatales y no estatales a adoptar las medidas necesarias e incorporar en sus respectivos ámbitos de actividad las tecnologías requeridas para promover el intercambio de información pública o privada autorizada por su titular, disponible en medios electrónicos, respetando el principio del previo consentimiento informado, a cuyos efectos obliga a recabarlo *"de acuerdo con lo previsto en la Ley N° 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data".*

CONSIDERANDO:

I) Que la puesta a disposición de los datos consultada se enmarca en la definición legal de comunicación de datos personales regulada en el artículo 17 de la Ley N° 18.331.

II) Que aplica respecto de las Instituciones consultantes la excepción prevista en el literal B) del artículo 9 de la citada ley, que dispone que no será necesario el previo consentimiento informado cuando los datos *"se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".*

III) Que el interés legítimo exigido para que proceda la comunicación encuentra fundamento en velar por el goce y efectivo ejercicio del derecho a la seguridad social.

IV) Que las Instituciones consultantes son "Administraciones Tributarias" en función de las contribuciones especiales de seguridad social que recaudan, por lo que se encuentran habilitadas a recibir información de sus similares al tenor de lo dispuesto en los artículos 1º y 47 del Código Tributario, siempre que dicha comunicación se solicite por resolución fundada conforme el inciso segundo del último de los artículos citados.

V) Que la excepción al consentimiento no exime a las entidades consultantes de cumplir con el resto de los principios y derechos consagrados en la Ley Nº 18.331, por lo que deberán cuidar a lo largo del proceso la legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad en relación a los datos personales que intercambian, así como asegurar el cumplimiento de los derechos de información, acceso, rectificación, actualización, inclusión o supresión, en cuanto correspondan.

ATENTO: A lo expuesto e informado, y lo previsto por los arts. 31 y 34 de la Ley N° 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La comunicación de datos no requiere previo consentimiento informado de sus titulares, por resultar aplicables en la especie las excepciones previstas en los literales B) de los artículos 9 y 17 de la Ley N° 18.331, sin perjuicio de resultar aplicable el inciso segundo del artículo 47 del Código Tributario. El interés legítimo encuentra fundamento en velar por el goce y efectivo ejercicio del derecho a la seguridad social.

2.- Las entidades consultantes deberán cuidar la legalidad, veracidad, finalidad, seguridad, reserva y responsabilidad en relación a los datos personales que intercambian, así como asegurar el cumplimiento de los derechos de información, acceso, rectificación, actualización, inclusión o supresión a sus titulares, en cuanto correspondan.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen Nº	Expediente Nº
5/2017	2017-2-10-0000292

Montevideo, 26 de julio de 2017

VISTO: La consulta presentada por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (en adelante AGESIC) sobre intercambio de información.

RESULTANDO:

I) Que el intercambio proyectado se funda en el Acuerdo Específico para el fortalecimiento de áreas TI del Estado entre AGESIC y la OFICINA NACIONAL DEL SERVICIO CIVIL (ONSC), que consiste en el desarrollo de un proyecto de análisis de remuneraciones para perfiles de TI, y la definición de los perfiles necesarios para integrar áreas de TI y de Gobierno Electrónico del Estado, entre otros. La información a intercambiar consiste en datos globales sobre remuneraciones de los perfiles señalados.

II) Que la Ley N° 18.719, de 27 de diciembre de 2010 manda a las entidades públicas estatales y no estatales a adoptar las medidas necesarias e incorporar en sus respectivos ámbitos de actividad las tecnologías requeridas para promover el intercambio de información pública o privada autorizada por su titular, disponible en medios electrónicos, respetando el principio del previo consentimiento informado.

CONSIDERANDO:

I) Que la información de los montos globales de remuneración de los funcionarios del perfil señalado no es información confidencial en los términos de la Ley N° 18.381, de 17 de octubre de 2008, no teniendo esta Unidad objeciones desde el punto de vista de la protección de datos para su comunicación.

II) Que, con respecto a información personal no asociada a la función, se trata de una comunicación de datos personales en los términos del artículo 17 de la Ley N° 18.331, por lo que para dicha comunicación deberá darse cumplimiento a lo dispuesto en ésta, conforme lo establecido en el artículo 158 literal C de la Ley N° 18.719.

ATENTO: A lo expuesto e informado,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- La comunicación de datos referida en el Considerando II del presente Dictamen no requiere previo consentimiento informado de sus titulares.

2.- La comunicación de datos referida en el Considerando III del presente Dictamen requiere del cumplimiento de lo establecido en los artículos 9 y 17° de la Ley N° 18.331, de 11 de agosto de 2008.

3.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
6/2017	2017-2-10-000130

Montevideo, 26 de julio de 2017

VISTO: La consulta presentada por Federico Silva sobre la licitud del tratamiento de ciertos datos publicados por el Ministerio del Interior con fines de seguridad.

RESULTANDO:

I) Que el consultante expresa que se encuentra *"explorando la posibilidad de desarrollar un software a ser ofrecido a los locales comerciales para facilitar la identificación facial de los individuos que hayan sido procesados y cuyos datos identificatorios e imagen hubieren sido publicados por el Ministerios del Interior".*

CONSIDERANDO:

I) Que la presente consulta implica la consideración de dos temas: la publicación de la información sobre personas procesadas por parte del Ministerio del Interior y la utilización de la información publicada por particulares.

II) Que relacionado con la publicación de la información, la comunicación de datos de personas procesadas que realiza el Ministerio del Interior debe considerase conforme con las normas sobre protección de datos vigentes, en virtud de lo dispuesto en los artículos 3, 18 y 25 de la Ley Nº 18.331.

III) Que respecto de la utilización de la información, el tratamiento de datos sobre personas procesadas será lícito siempre que se realice por autoridades públicas en el marco de sus funciones y competencias, específicamente en el caso del Ministerio del Interior, en función de los cometidos atribuidos constitucional y legalmente relativos al orden interno (numeral primero del artículo 168 de la Constitución y artículo 1 de la Ley Nº 19.315, de 18 de febrero de 2015).

IV) Que el sitio web del Ministerio del Interior no califica como fuente pública de información al tenor de lo dispuesto en el artículo 9 bis de la Ley Nº 18.331, desde que no se trata de un diario o publicación oficial, ni de un medio masivo de comunicación, ni de una guía, anuario o similar. Tampoco se trata de un registro o publicación en el cual prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros.

ATENTO: A lo expuesto e informado,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Los datos sobre personas procesadas publicados por el Ministerio del Interior no pueden ser tratados en el ámbito privado por particulares, sin el consentimiento de los titulares de la información.

2.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

Dictamen	Exp.
7/2017	2017-2-10-0000238

Montevideo, 11 de octubre de 2017

VISTO: La consulta presentada por la Dra. María Inés Ferrari, jefa de jurídica del Instituto Nacional de Logística (INALOG) sobre la legitimidad de almacenar en el exterior información proveniente de la Administración Nacional de Puertos, Dirección Nacional de Aduanas, Ministerio de Transporte y Obras Públicas y de un proveedor privado de datos de comercio exterior.

RESULTANDO:

I) Que la consultante expresa que los datos a almacenarse serán: número de Registro Único Tributario (RUT), nombre de despachante, mercadería, estado de la mercadería, el origen, la aduana por la cual ingresó o salió, el depósito y la cantidad en valor y peso de esos movimientos, entre otros datos.

ATENTO: A lo expuesto y a lo informado a fojas 11-13 y a lo previsto en los artículos 23, 31 y 34 de la Ley N° 18.331.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

DICTAMINA:

1.- Que a los efectos de valorar la legitimidad de la transferencia planteada corresponde controlar: el origen de la información, la titularidad de la base de datos o del tratamiento y el destino de los datos.

2.- Que, respecto del origen, reviste especial importancia que la información cuente con el consentimiento de sus titulares o se ampare en alguna de las excepciones legales contenidas en las disposiciones jurídicas internas del país desde el cual se obtienen los datos, sean éstos colectados directamente o a través de un intermediario.

3.- Que, relacionado con la titularidad de la información, se debe determinar el organismo responsable de la base de datos o del tratamiento y por ende exportador y responsable de la inscripción de la base de datos y del cumplimiento de las exigencias legales y reglamentarias para la transferencia internacional de datos.

4.- Que en materia de destino y en tanto los Estados Unidos de América no es un país considerado con niveles adecuados en materia de protección de datos, se debe revisar si la entidad importadora se encuentra adherida al denominado Escudo de Privacidad *(Privacy Shield)* o se ampara en la suscripción de cláusulas contractuales tipo, en cuyo caso debe solicitar autorización para la transferencia internacional de datos ante esta Unidad.

5.- Notifíquese, publíquese y oportunamente archívese.

Fdo. Mag. Federico Monteverde

Consejo Ejecutivo

URCDP

NOTA *de* INTERÉS

INFORME A 10 AÑOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

El presente informe procura otorgar una visión global respecto de la actividad de la Unidad Reguladora y de Control de Datos Personales (URCDP) desde sus orígenes hasta la fecha, haciendo especial hincapié en las actividades desarrolladas no sólo para hacer cumplir la ley sino además para difundir entre la población en general el derecho humano a la protección de datos personales.

Se entendió pertinente proporcionar un panorama general de las razones para la creación de la URCDP y el otorgamiento de las competencias y funciones propias vinculadas a la defensa de dicho derecho, así como de las modificaciones normativas efectivizadas desde sus orígenes para clarificar o evolucionar las disposiciones originalmente sancionadas.

Por otra parte, se ha procurado presentar una visión de la inserción de la URCDP en el ámbito regional e internacional, a través de la participación en instrumentos y organismos internacionales vinculados a la materia, y la adhesión a Convenios internacionales y a estándares que fortalezcan la protección brindada a todas las personas sujetas a las obligaciones y titulares de los derechos que consagran las disposiciones normativas vigentes.

Finalmente, se presentan a modo de ejemplo algunos datos estadísticos de relevancia para comprender el trabajo desarrollado desde el año 2009 a la fecha, sin perjuicio de la información adicional que puede obtenerse de la consulta a las múltiples publicaciones que anualmente realiza la URCDP.

2. UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES (URCDP)

Orígenes

En el marco de la estrategia de Gobierno Electrónico y Sociedad de la Información asociada al desarrollo de infraestructura tecnológica y actualización del marco jurídico nacional, se impulsó en el año 2008 la aprobación de una disposición normativa que se convertiría en la Ley Nº 18.331, de 11 de agosto de 2008, sobre Protección de Datos Personales y Acción de Habeas Data.

La Ley citada reconoce el Derecho a la Protección de los Datos Personales como inherente a la personalidad humana, crea el órgano de control – Unidad Reguladora y de Control de Datos Personales (URCDP) – y establece un proceso jurisdiccional denominado Acción de Habeas Data.

El Decreto Nº 414/009, de 31 de agosto de 2009 reglamentó la Ley en cuanto al ámbito de aplicación, definiciones, consentimiento, seguridad, derecho de acceso, régimen registral, órgano de control, funcionamiento de los Consejos Ejecutivo y Consultivo, además de determinar las normas de actuación.

El régimen jurídico en materia de protección de datos establecido por las normas antes señaladas sigue el modelo de la regulación europea en la materia, que ha sido su fuente inspiradora.

Organización

La Ley N° 18.331 en su artículo 31 dispuso la creación de la Unidad Reguladora y de Control de Datos Personales, dotada de amplia autonomía técnica.

El artículo citado dispone que la URCDP esté dirigida por un Consejo Ejecutivo integrado por tres miembros: el Director Ejecutivo de la Agencia para el Desarrollo de Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento y dos miembros designados por el Poder Ejecutivo entre personas que, por sus antecedentes personales, profesionales y de conocimiento en la materia, aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos, quienes durarán cuatro años en sus funciones, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme con las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico. Uno de estos dos integrantes preside anualmente dicho Consejo.

Los miembros del Consejo Ejecutivo son el Ing. José Clastornik, Director Ejecutivo de AGESIC -quien se encuentra habilitado para delegar sus funciones y lo hizo oportunamente en la Ing. Virginia Pardo-, el Dr. Felipe Rotondo y el Mag. Federico Monteverde.

De acuerdo con lo dispuesto por el artículo 32 de la Ley, el Consejo Ejecutivo de la URCDP funciona asistido por un Consejo Consultivo, integrado por cinco miembros:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser un legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica (de la Facultad de Derecho de la Universidad de la República).
- Un representante del área privada elegido en la forma establecida reglamentariamente (de la Cámara Nacional de Comercio y Servicios).

Dicho Consejo sesiona presidido por el Presidente de la URCDP. Sus integrantes durarán cuatro años en sus cargos y sesionarán a convocatoria del Presidente de la URCDP o de la mayoría de sus miembros. El Consejo Ejecutivo podrá solicitar su opinión sobre cualquier asunto de su competencia y deberá ser consultado por éste cuando ejerza potestades de reglamentación

Competencias

Los cometidos asignados a la URCDP de acuerdo a lo dispuesto por el artículo 34 de la citada Ley son los siguientes:

- Asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.
- Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.
- Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de esas bases.
- Controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.
- Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.
- Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.
- Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.
- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.

3. DESARROLLOS NORMATIVOS

Ley Nº 18.331 y sus modificaciones

La Ley se promulgó el 11 de agosto de 2008 y fue publicada en el Diario Oficial el 18 de agosto de 2008, con el Nº 18.331.

Ha tenido pocas modificaciones tendientes, fundamentalmente, a aclarar algunos puntos relacionados con el procedimiento de clausura de bases de datos, el tratamiento de datos comerciales, y las excepciones al previo consentimiento informado (Ley Nº 18.719, de 27 de diciembre de 2010).

En ese sentido introdujo modificaciones que esencialmente consisten en:

- la sustitución de la referencia del inciso segundo del artículo 9°. En este artículo se sustituyó la referencia errónea que existía en el texto original al artículo 12 de la Ley, por la correcta al artículo 13.
- la modificación del literal e) del inciso tercero del artículo 9º. Se elimina la referencia a las "personas jurídicas, privadas o públicas" ya que el Consejo Ejecutivo ha dictaminado que las personas jurídicas no pueden alegar la excepción de "uso exclusivo personal o doméstico". Se agrega el término "individual" por figurar ya en otros artículos de la Ley.
- la modificación del inciso segundo del artículo 14, relativo al ejercicio del derecho de acceso por parte de los sucesores. Se exige en la redacción actual que la calidad de sucesor se acredite debidamente. En el texto original figuraba el requisito de acreditar la calidad de sucesor universal por sentencia declaratoria de herederos, lo cual constituía una traba innecesaria para el ejercicio de un derecho que no las admite. Se consideró que existen otras formas de probar la calidad de heredero, que en virtud de los intereses en juego, son suficientes.
- la modificación de las causales de eliminación o supresión de datos personales reguladas en el inciso cuarto del artículo 15. En este caso se corrige la redacción del texto original que era confusa al utilizar dos veces consecutivas términos de negación.
- el cambio en la redacción del artículo referido a la impugnación de valoraciones personales regulado en el artículo 16.
- la modificación del literal c) del inciso tercero del artículo 17. Se flexibiliza el requisito de la disociación mediante el agregado "cuando sea pertinente", dejando margen para resolver este tipo de exigencias en cada caso.
- la sustitución del artículo referido a los datos relativos a bases de datos con fines de publicidad, inciso primero del artículo 21. Se incluye a texto expreso la expresión "prospección comercial", la cual había sido objeto de debate en las actividades de fiscalización que venía llevando adelante la URCDP.
- la modificación del inciso primero del artículo 22, referido a la actividad comercial o crediticia.
- la modificación del artículo 28 que regula la creación, modificación o supresión de bases de datos de responsables privados. Se eliminó la expresión "que no sean para uso exclusivamente individual o doméstico" que causara dudas y debates en la práctica.
- la modificación del literal j) del artículo 29 de la Ley. De esta forma se corrige la referencia errónea del texto vigente a "cancelaciones por incumplimiento", sustituyéndola por "cancelaciones por cumplimiento".
- la modificación del literal d) del artículo 34 relativo a tareas de fiscalización. Conforme a la experiencia de la URCDP se desarrolla este cometido con mayor detalle y precisión. Se trata de una norma importante de las competencias de la URCDP porque permite regular las labores indagatorias con la seguridad requerida en estos casos.
- la modificación de las potestades sancionatorias reguladas en el artículo 35, estableciéndose un elenco distinto de sanciones. Se introducen dos figuras sancionatorias nuevas, la observación y la clausura de bases de datos. Se aplican a la clausura los requisitos de forma y procedimiento que originalmente se preveían para la suspensión, recobrando de esta manera coherencia con el régimen legal en el cual se inspiró.

Otra modificación fue realizada por la Ley Nº 18.996, de 7 de noviembre de 2012, que por su artículo 43 agrega un artículo 9 bis a la Ley Nº 18.331 a efectos de definir cuáles son fuentes públicas de información.

Ratificación del Convenio Nº 108 del COE

El 27 de diciembre de 2012 se promulgó la Ley Nº 19.030 que aprueba el Convenio del Consejo de Europa Nº 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos

de Carácter Personal aprobado en Estrasburgo en 1981 y su Protocolo Adicional relativo a las Autoridades de Supervisión y Flujos Internacionales de Datos aprobado en Estrasburgo en 2001.

Esta Ley, que supone un hito en Uruguay, es la culminación de un camino iniciado por la URCDP. El Convenio N° 108 del Consejo de Europa y su Protocolo Adicional N° 181, son instrumentos continentes de los principios rectores en materia de Protección de Datos, fuente de inspiración y consulta de la comunidad internacional.

Obtención del estatus de adecuación

La Decisión de Ejecución de la Comisión Europea de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales (2012/484/UE), que declara a Uruguay país adecuado, fue emitida luego del Dictamen Nº 6/2010 del Grupo de Trabajo de Protección de Datos del Artículo 29 (G29).

La citada Decisión termina por rubricar favorablemente un proceso de examen iniciado tres años antes, habilitando a Uruguay a ingresar en el reducido elenco de Estados, fuera del ámbito europeo, que disponen de tal reconocimiento.

El régimen constitucional, legal y reglamentario uruguayo, así como las competencias y actividades desarrolladas por el Órgano de Control, fueron evaluados positivamente a tales efectos por la Comisión Europea.

Dicho régimen, competencias y actividades se mantienen; precisadas en aquello que -como ya se indicó- se estimó pertinente a los efectos de la protección derecho.

Aplicación de los principios en materia de protección de datos personales

El artículo 3º de la Ley excluye de su aplicación a determinadas bases de datos, a saber:

A. A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

B. Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

C. A las bases de datos creadas y reguladas por leyes especiales.

No obstante ello, el régimen jurídico existente en virtud de los principios y del contexto normativo llevó a que el Consejo Ejecutivo se pronunciara en reiteradas oportunidades, sosteniendo la aplicación de esos principios generales a las bases de datos referidas, y a los tratamientos con ellas asociados, precisamente por tratarse de la defensa de un derecho humano.

A vía de ejemplo se señala el Dictamen Nº 29/013, de 24 de octubre de 2013, en el que el Consejo afirma en el Considerando VIII): *"Que en definitiva, si bien el art. 3° de la Ley N° 18.331, indica que las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado, quedan excluidas de su ámbito de aplicación, corresponde que desde la perspectiva de un derecho humano como lo es la protección de datos personales, se consideren las recomendaciones formuladas por la URCDP".*

En el Dictamen Nº 6/015, de 25 de marzo de 2015 señala el Consejo Ejecutivo, en su Considerando II: *"Que si bien la base de datos se encontraría excluida de la aplicación de la Ley de Protección de Datos Personales, esta Unidad ha sostenido que los principios rectores en la materia deben ser atendidos y resultan aplicables por tratarse de la tutela de un derecho fundamental (artículo 1º Ley Nº 18.331)".*

4. ACTIVIDADES EJECUTADAS EN EL PERÍODO

4.1. PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS

Concurso escolar de la campaña "Tus Datos Valen. CUIDALOS"

Sensibilizar sobre el derecho a la protección de los datos personales es clave y más aún a los niños que se encuentran expuestos a posibles peligros ocasionados por terceros, tanto en las redes virtuales cuanto fuera de ellas. Por esa razón, el objetivo de la campaña iniciada en 2013 fue sensibilizar y capacitar a niños y niñas de 10 a 12 años de escuelas públicas y privadas de todo el país, sus maestros y familias, sobre la importancia que tiene el cuidado y la protección de los datos personales.

A los efectos de orientar a maestros y escolares sobre la temática referida, la URCDP generó un kit de materiales que incluyó un afiche, stickers y folletos para cada niño, una guía para el maestro con una propuesta de actividad didáctica para trabajar la importancia que tienen los datos personales, y material para el uso de las carteleras en clase.

La campaña que cuenta con cinco ediciones ininterrumpidas, ha contado con cinco propuestas de concurso diferentes.

Así:

- En 2013, se realizó el primer concurso denominado "Cómo explicas qué son los datos personales". La consigna implicó la elaboración de un afiche por parte de los escolares, que tuviese como eje la protección de datos personales.
- En 2014, el segundo concurso denominado "Tus datos tu decisión". La consigna implicó la elaboración de un comic (historieta) por parte de los escolares, que tuviese como eje la protección de datos personales.
- En 2015, el tercer concurso denominado "Tus datos. Tu decisión. Animate!. La consigna implicó la elaboración de un audiovisual grabado o filmado por parte de los escolares, que tuviese como eje la protección de datos personales.
- En 2016, el cuarto concurso denominado "Tus datos cuentan". La consigna implicó la elaboración de un cuento por parte de los escolares, que tuviese como eje la protección de datos personales.
- En 2017, el quinto concurso denominado "Me merezco datos protegidos". La consigna implicó la elaboración de un meme por parte de los escolares, que tuviese como eje la protección de datos personales.

Esta campaña, que es una iniciativa de la URCDP, ha contado desde sus inicios con el apoyo de Presidencia de República, el Consejo de Educación Inicial y Primaria (CEIP), el Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia o Plan Ceibal (implementador de la estrategia one laptop per child), la Dirección Nacional de Impresiones y Publicaciones Oficiales (IMPO), y la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

Atento a las estrategias de difusión llevadas adelante desde el inicio del Concurso a la fecha se ha podido llegar con la temática propuesta a todas las escuelas públicas y privadas de la República.

Puede afirmarse que ésta se ha convertido en un aporte fundamental para que los niños, sus familias y los educadores conozcan y aprendan a cuidar adecuadamente tanto sus datos personales, como los de otras personas.

4.2. GOBERNANZA Y FORTALECIMIENTO DE CAPACIDADES

Desarrollo de instancias de capacitación

- *Capacitación a responsables*

La URCDP ha realizado desde su propia constitución una serie de capacitaciones a diversas entidades del Estado y organizaciones sin fines de lucro.

En ese sentido, es posible afirmar que se ha llegado con cuestiones vinculadas a la protección de datos a entidades como la Oficina de Planeamiento y Presupuesto (OPP), el Ministerio de Ganadería, Agricultura y Pesca, el Ministerio del Interior, el Ministerio de Transporte y Obras Publicas, el Ministerio de Turismo y Deporte, el Banco Hipotecario del Uruguay (BHU), el Banco de Previsión Social (BPS), la Administración Nacional de Combustibles, Alcohol y Portland (Ancap), la Administración de las Obras Sanitarias del Estado (OSE), el Plan Ceibal, el Programa APEX de la Universidad de la República (APEX), el Consejo de Educación Inicial y Primaria, la Dirección General de Registros, el Colegio de Contadores del Uruguay, el Colegio de Abogados del Uruguay, la Asociación de Escribanos del Uruguay, la Cámara Uruguaya de Telecomunicaciones, el Colegio de Administradores de Propiedad Horizontal.

- *Capacitación a titulares*

La URCDP ha procurado acercarse a los titulares de datos mediante el empleo de las tecnologías disponibles, elaborando e incentivando el uso de un e-learning, disponible en la página web de la URCDP, en el que se desarrollan en forma sencilla y amena los conceptos más relevantes vinculados al derecho a la protección de datos personales.

Se ha puesto a disposición asimismo desde el año 2014 un Curso de Protección de Datos Personales a través de la plataforma EDUCANTEL de la Administración Nacional de Telecomunicaciones (ANTEL), que ya ha sido realizado por más de 500 participantes de todo el mundo.

Elaboración de guías y marcos de referencia

Una preocupación constante de la URCDP desde su creación ha sido la elaboración de criterios que sirvan de guía o referencia para promover el conocimiento y ejercicio del derecho a la protección de datos personales.

En este sentido, la URCDP ha desarrollado una serie de lineamientos temáticos vinculados con te-

mas tan diversos como la protección de datos en el sector salud, la protección de datos en el sector educación, el manejo de datos personales en operadores de telecomunicaciones, el manejo de datos personales en la Administración Pública.

Recientemente se han publicado una serie de guías aplicativas con recomendaciones vinculadas con la videovigilancia y actualmente se está trabajando, a los efectos de su concreción antes de finales de año en guías vinculadas con Drones, Big data, Byod y Privacy by Design.

Avances en privacidad desde el diseño

En el marco de un acuerdo institucional existente desde 2015, entre AGESIC y el ICT4V (Information and Communication Technologies for Verticals), entidad público – privada orientada a la construcción de capacidades y soluciones en diferentes ámbitos vinculados con la tecnología, se han iniciado una tríada de actividades, vinculadas con la temática de la privacidad desde el diseño. En efecto, a saber:

- Grupo de lectura integrado con profesionales de la ingeniería y el derecho, pertenecientes a entidades públicas y privadas, así como de la academia, en el que se plantean elementos teóricos para la discusión así como su aplicación práctica.
- Desarrollo de documentos tendentes a su presentación en Congresos y Conferencias internacionales, como mecanismo de presentación de resultados de investigación. En una primera instancia se ha presentado el artículo "Privacy by Design: de la abstracción jurídica a la práctica ingenieril" en el XI Congreso Internacional de Seguridad de la Información en 2017, el que fuera aprobado luego de ser sometido a la correspondiente revisión de pares.
- Tutoría a estudiantes de grado de la Facultad de Ingeniería de la Universidad de la República, cuyas tesis de grado se desarrollan en vínculo o directamente sobre este tema.

Organización de la 34º Conferencia Internacional de Autoridades de Privacidad y Protección de Datos

Entre los días 23 y 25 de octubre de 2012 en Punta del Este, se realizó la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, denominada "Privacidad y Tecnología en equilibrio", – por primera vez en América del Sur – con expositores de 50 países y varios cientos de participantes provenientes de los diferentes puntos del planeta.

En este marco se realizaron conferencias magistrales y se trabajó sobre diferentes ejes temáticos que pretendieron abarcar la realidad de la protección de datos personales del momento, lo que trasladado a la fecha, en varios casos es posible afirmar que su vigencia se mantiene, a saber:

- El Impacto de las nuevas tendencias en la Sociedad de la Información
- Protección de Datos Personales y Gobierno Electrónico
- Modelos de Regulación de Privacidad
- La nueva Normativa Europea
- Protección de Datos Personales en América Latina. Ampliando horizontes
- Gobierno abierto
- Geolocalización pública y privada
- E-salud
- Herramientas de Concientización y Difusión: ¿Preparado para una vida 3.0?
- Herramientas forenses: lo que nuestros dispositivos dicen de nosotros
- Herramientas de Cooperación: el camino posible y efectivo
- Marketing comportamental en línea
- Biometría
- Smart Data
- Consentimiento informado ¿Regla o excepción?
- Derechos fundamentales
- Piratería y privacidad: desafíos cruzados
- Explorando caminos: Investigaciones y proyectos

El cierre de la Conferencia estuvo a cargo del Señor Presidente de la República.

Actividades y eventos locales

- *Eventos locales*

La URCDP desde su creación ha participado en diversas actividades y eventos orientadas a la difusión del derecho a la protección de los datos personales.

Año 2009

En el mes de agosto del 2009 la URCDP participó en el evento organizado por AGESIC denomina-

do "Transparencia y privacidad" bajo la consigna Gobierno en Red, que con amplia participación de las áreas legales e informáticas del ámbito público.

En octubre del mismo año, la URCDP participó en el Seminario "Derecho, adolescentes y redes sociales en Internet", evento que contó con el apoyo del Centro Internacional de Investigaciones para el Desarrollo (IDRC) de Canadá, y en el "VII Congreso Uruguayo de Pediatría", en una mesa redonda denominada "Cuidándonos".

En noviembre se participó del "V Congreso Iberoamericano de Seguridad Informática – CIBSI 09", y en una charla sobre Protección de Datos Personales y registro de Bases de Datos en la Asociación de Escribanos del Uruguay.

Finalmente, en diciembre de ese año se realizaron varias sesiones de difusión y capacitación relacionadas con la temática de Protección de Datos Personales y registro de Bases de Datos, las cuales se realizaron en la Bolsa de Valores del Uruguay y el Colegio de Contadores, Economistas y Administradores del Uruguay. El 22 de diciembre ser realizó en Punta del Este, Maldonado, una charla sobre Protección de Datos Personales y Registro de Bases de Datos a solicitud de la Asociación de Inmobiliarias de Punta del Este, el Centro Hotelero de Punta del Este y la Asociación de Abogados de Maldonado.

Año 2010

Entre los días 1º al 4 de junio se realizó en la ciudad de Montevideo el Seminario Regional de Protección de Datos de la Red Iberoamericana de Protección de Datos, evento que contó a la URCDP como anfitrión. El mencionado encuentro fue realizado en los salones del Centro de Formación de la Capacitación Española en Montevideo y contó con la participación de la Agencia Española de Protección de Datos y de AGESIC.

Se trató de una importante instancia de participación y debate de la actualidad en la materia, contando con destacados exponentes de España, Portugal, Chile, Argentina, Ecuador, México, Paraguay, Perú, Brasil, Colombia y Uruguay.

Durante el año se trabajó además en actividades y eventos para difundir el derecho con diferentes actores de la actividad nacional, personas físicas, asociaciones profesionales, empresas, organismos estatales o cualquiera que la solicitara (Centros Comerciales e Industriales de Rosario, Mercedes, Paysandú, Artigas, Rivera, Tacuarembó, Cerro Largo, Dolores, Lavalleja, San José, Cámara Nacional de Comercio y Servicios, Facultad de Ciencias Económicas y de Administración de la Universidad de la República, Asociación de Psicoanalistas del Uruguay, Escuela Nacional de Administración Pública, y Asociación de Escribanos del Uruguay).

Año 2011

En instancia de capacitación y difusión con entidades del Estado se participó de los eventos organizados por el Programa de Gestión Unificada de Registro e Información (GURI) del Consejo de Educación Inicial y Primara en los departamentos de Colonia, Maldonado y Rivera. Los eventos contaron con la concurrencia de inspectores nacionales, regionales y locales, así como docentes y asesores del programa representantes de los departamentos sede y limítrofes.

La URCDP participó de la Primera Sesión Académica del Instituto de Derecho Informático de la Universidad de la República, con la exposición denominada "Central de Riesgos del Banco Central del Uruguay, ventajas y desventajas de su libre acceso".

A su vez se dictaron dos charlas sobre Protección de Datos, una realizada en las instalaciones de Microsoft y otra en la Unidad Reguladora de Servicios de Comunicaciones (URSEC).

Año 2012

En forma concomitante con la organización de la Conferencia Internacional de Autoridades de Privacidad y Protección de Datos, en el año 2012 la URCDP concurrió a diversos medios de prensa escrita, televisiva y radial de forma de promover el derecho y la conferencia que se realizaría en octubre de ese año.

Año 2013

Dentro del marco de eventos nacionales organizados por la URCDP, en el año 2013 se recibió la visita del Prof. Dr. Álvaro Sánchez Bravo de la Universidad de Sevilla, quien brindó una charla sobre la "Nueva normativa de la Unión Europea".

En el mes de abril la URCDP recibió la visita en su sede de la Jefa de la Oficina de Registros Públicos del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires, reunión en la que se trataron diferentes puntos referentes a la protección de datos personales en el Río de la Plata.

Continuando con la visita de expertos extranjeros a la URCDP, se recibió la visita del profesor Dr. Ahti Saarempää, Vicepresidente de la Junta de Protección de Datos de Finlandia, que abordó el tema del vínculo existente entre información y privacidad,

y el desafío de combinar el derecho a la información con la privacidad.

La URCDP participó además como asistente en el Primer Congreso Internacional de Mobbing y Bullying.

El Centro Latinoamericano de Administración para el Desarrollo (CLAD) organizó el XVIII Congreso Internacional sobre la Reforma del Estado y la Administración Pública. A él concurrió por la URCDP, su Presidente Mag. Federico Monteverde, quien participó en el panel denominado "El impacto de la Protección de Datos en la Administración Pública".

Cerrando el ciclo de visitas de expertos extranjeros, en el mes de noviembre se realizó una sesión de trabajo con Jesús Rubí, Adjunto al Director de la Agencia Española de Protección de Datos Personales.

Además de las instancias de capacitación en distintos organismos, la URCDP participó en el seminario organizado por la Jefatura de Policía de Tacuarembó, dentro de su plan de capacitación en seguridad y educación policial, los días 7 y 8 de Junio, denominado "2º Seminario de Seguridad Informática y Educación Policial".

Asimismo, el 11 de setiembre la URCDP comenzó el ciclo de sesiones sectoriales en la Cámara Uruguaya de Telecomunicaciones del Uruguay (CTU), con la presencia de miembros de empresas telefónicas, call centers, proveedores de servicios de Internet y personal de la propia Cámara.

Finalmente, la URCDP participó en el ciclo organizado por AGESIC denominado "Encuentros Regionales de Gobierno Electrónico" en todo el país.

Año 2014

En el año 2014 la URCDP procuró dar prioridad a la generación de redes de replicación para la difusión del derecho, concentrándose los esfuerzos en la realización de capacitaciones, actividades de sensibilización dirigidas a las personas designadas como replicadores y al público en general.

En relación con los primeros es importante mencionar que pertenecen a diferentes entidades públicas, a saber: de la enseñanza (Administración Nacional de Educación Pública -Universidad del Trabajo del Uruguay y Consejo Directivo Central-, Plan Ceibal), políticas de la juventud (Instituto Nacional de la Juventud), Intendencias Departamentales de Canelones y Rocha, entre otros.

Año 2015

A los efectos de continuar avanzando en la aprehensión de conocimiento en la materia por parte de las diferentes entidades, durante el año 2015 se realizaron charlas de sensibilización y capacitación, de acuerdo con los requerimientos y necesidades de cada una de ellas: OPP, Plan Ceibal, Centros de Atención Infantil de Verano, Inspección Departamento de Educación Primaria en Montevideo, Ministerio del Interior (Policía Comunitaria), Universidad del Trabajo del Uruguay (San Ramón, Canelones), Instituto Nacional de la Juventud, Instituto Nacional de Rehabilitación y la Organización No Gubernamental "El Abrojo".

Asimismo, se participó en actividades en todo el país, con el mismo objetivo de capacitación y sensibilización en el marco de las denominadas "Expo EDUCA" organizadas, fundamentalmente, por ANEP-CEIP.

Año 2016

Al igual que en años anteriores se organizaron eventos puntuales en distintas entidades públicas, de forma de difundir el derecho, destacándose las actividades realizadas en la Oficina de Planeamiento y Presupuesto (OPP), el Banco Hipotecario del Uruguay (BHU), el Banco de Previsión Social (BPS), la Administración Nacional de Combustibles, Alcohol y Portland (Ancap), el Centro Ceibal para el Apoyo a la Educación de la Niñez y la Adolescencia (Plan Ceibal), el Programa APEX de la Universidad de la República (APEX) y el Consejo de Educación Inicial y Primaria.

Por otra parte, se realizó una charla de capacitación en el evento denominado "Fortalecimiento de la intervención judicial en la protección y promoción del derecho a la libertad de expresión en el Uruguay", organizado por el Centro de Archivos y Acceso a la Información Pública (CAinfo).

Se organizaron además charlas puntuales con participación de integrantes de la URCDP e invitados extranjeros. Así, el 9 de marzo, el Dr. Juan Antonio Travieso (reconocido especialista de la República Argentina) visitó la URCDP. El 19 y 20 de abril lo hizo la Dra. Mª Verónica Pérez Asinari, jefa de la Unidad de Supervisión y Aplicación de la Ley del Supervisor Europeo de Protección de Datos. El 17 de junio, se recibió la visita del Dr. Pablo Palazzi, abogado, profesor, director del Centro de Tecnología y Sociedad de la Universidad San Andrés de la ciudad de Buenos Aires, República Argentina, y editor e integrante del Comité Académico Interna-

cional de la Revista Latinoamericana de Protección de Datos Personales.

Finalmente, el 10 de noviembre se realizó una reunión entre miembros de la URCDP y del Instituto de Acceso a la Información Pública de la República de El Salvador, con la presencia del comisionado del Instituto de Acceso a la Información Pública, Dr. Jaime Campos, el coordinador de Protección de Datos, Dr. Carlos Calderón, y el magistrado propietario del Tribunal Superior Electoral, Dr. Fernando Argüello Téllez.

Año 2017

En el correr del año 2017, entre otras actividades, la URCDP participó en los talleres "Implementación de la normativa de datos abiertos, transparencia activa y protección de datos personales" realizados en diferentes localidades del interior del país. Los días 5 y 6 de setiembre las actividades se realizaron en Rivera; el 4 y 5 de octubre, en Paysandú; y los días 26 y 27 de octubre, en Tacuarembó.

Dictó además la primera edición del curso de protección de datos personales dirigido a funcionarios públicos de diversas entidades del Estado los días 23, 27 y 30 de octubre y 6 de noviembre. Posteriormente, se realizaron dos ediciones más durante los meses de noviembre y diciembre.

La URCDP participó en el congreso CIBSI 2017, desarrollado en Buenos Aires, Argentina, entre el 1 y el 3 de noviembre, dónde se presentó el documento "Privacy by Design: de la abstracción jurídica a la práctica ingenieril". El texto fue presentado por el grupo de trabajo de ICT4V, en el cual participa la URCDP.

El viernes 8 de setiembre, en el Complejo Torre de las Telecomunicaciones, se realizó una jornada de sensibilización e intercambio sobre protección de datos personales. La actividad fue organizada por ANEP–Codicen, URCDP y Agesic en el marco de un proyecto de cooperación técnica para incorporar esta temática en la labor docente.

La jornada estuvo dirigida a docentes de docencia directa e indirecta de Educación Media y tuvo por objetivo intercambiar ideas y experiencias sobre el tema de la protección de datos personales.

- *Semanas Nacionales de la Protección de Datos*

  I) *Primera Semana Nacional de la Protección de Datos*

En el marco del impulso a la difusión del derecho a la protección de datos que ha caracterizado a la URCDP y con el objetivo de celebrar los ocho años desde la promulgación de la Ley Nº 18.331, de 11 de agosto de 2008, se organizó en la semana comprendida entre el 8 y el 12 de agosto de 2016 la "Primera Semana Nacional de la Protección de Datos Personales", que contó con varias actividades y la participación de múltiples actores sociales.

Actividades académicas

Las actividades académicas realizadas en el marco de la Primera Semana Nacional de Protección de Datos Personales, bajo la consigna: "Retos de la privacidad en la sociedad de la información", se realizaron en Montevideo y Maldonado con el objetivo de reflexionar en torno a los nuevos desafíos del derecho a la protección de datos personales en el contexto de las nuevas realidades operativas y normativas del mundo de las TIC.

Actividades en Montevideo

Además de la entrega de los premios del concurso "Tus Datos Valen", se realizó una Conferencia Internacional en Montevideo los días 9 y 10 de agosto.

En el evento se trataron temas vinculados con la protección de datos en Iberoamérica, como el derecho al olvido, realizándose consideraciones asociadas con la sentencia europea relacionada con dicho derecho y su aplicación a la realidad latinoamericana; las nuevas disposiciones normativas internacionales, destacándose la aprobación del nuevo Reglamento General de Protección de Datos europeo y la modernización del Convenio 108 del Consejo de Europa; la ponderación de derechos fundamentales, analizándose desde una perspectiva global la pertinencia de aplicar el derecho a la protección de datos y su vínculo con otros derechos fundamentales; la elaboración de perfiles desde las perspectivas comercial, estatal, social y económica, considerándose además el tratamiento masivo de información; las perspectivas sobre el tratamiento de información personal desde el punto de vista de la educación, la salud y la actividad comercial; y los desafíos de la protección de datos según las Autoridades de Control.

Se contó con la participación de profesionales, autoridades y académicos de distintos países de América Latina, destacándose la presencia del Dr. Eduardo Bertoni, director de la Dirección de Protección de Datos de la República Argentina, el Mag. Gustavo Parra Noriega, coordinador de Protección de Datos del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos de los Estados Unidos Mexicanos, el Dr. Danilo Doneda, académico de la Universidad de Río de Janeiro, República Federativa del Brasil, y el Dr. Pablo Palazzi, académico de la Universidad San Andrés, de la República Argentina.

Actividades en Maldonado

El 11 de agosto, en el Campus de Maldonado, se efectuó el cierre de la 1ª Semana Nacional de Protección de Datos Personales con la participación del Consejo Ejecutivo de la URCDP y la Intendencia de Maldonado.

La jornada fue la cuarta y última y en ella se desarrollaron mesas y paneles acerca de temas tales como Derechos fundamentales en la Sociedad de la Información, redes sociales y protección de datos e Impacto de la protección de datos en la actividad estatal.

II) Segunda Semana Nacional de la Protección de Datos

En esta segunda edición se celebraron cuatro jornadas contentivas de diferentes actividades:

- Entrega de los premios correspondientes a la 5ta. Edición del concurso para niños de 5tos. y 6tos. años de escuelas públicas y privadas de todo el país, en un evento desarrollado en los salones del Teatro Solís de la ciudad de Montevideo.
- Mesa de discusión a propósito del Handbook on Enforcement Cooperation emanado de la Conferencia Internacional del Autoridades de Privacidad y Protección de Datos, en la que se realizaron intercambios con miembros de la academia, el sector privado, autoridades públicas y miembros de los Consejos Consultivo y Ejecutivo de la URCDP. Esta actividad fue designada como uno de los "Enforcement Cooperation Meeting" del año 2017 por la ICDPPC.
- Taller sobre Privacidad desde el Diseño, en una actividad realizada en coordinación con ICT4V. En éste convocado bajo el título: "Privacidad desde el diseño: estado de situación, desafíos y perspectivas", se contó con la participación de especialistas provenientes del sector privado de Europa, Estados Unidos y América Latina quienes introdujeron la protección de datos en el contexto latinoamericano y explicaron cómo puede contribuir a abordar algunos de los desafíos más urgentes del mundo digital. A través de presentaciones y sesiones interactivas, los participantes aprendieron cómo la protección de datos puede ayudar a resolver algunos de los problemas asociados con la transición digital (ya sean asuntos empresariales, políticos o reglamentarios), así como a mejorar la comprensión de los temas más amplios asociados con la transición digital.
- Foro de protección de datos personales, en el que se debatió acerca de la importancia de la regulación en materia internacional, la privacidad desde el diseño, las transferencias internacionales de datos y las perspectivas y desafíos de la protección de datos en el mundo global, contándose nuevamente con expertos nacionales y extranjeros provenientes de los diferentes ámbitos del quehacer social – académico, empresarial, social, político –

4.3. FORTALECIMIENTO Y POSICIONAMIENTO DE LA URCDP

Edición de la Revista Uruguaya de Protección de Datos Personales

En el "Prólogo" del número inicial de la *Revista Uruguaya de Protección de Datos Personales* – presentado en el marco de la Primera Semana Nacional de la Protección de Datos Personales – se expresa que la publicación constituye una "*iniciativa de la Unidad Reguladora y de Control de Datos Personales de encarar una nueva vía de difundir los derechos que garantiza el régimen de la Ley Nº 18.331, de 11 de agosto de 2008, e incentivar su conocimiento y debida aplicación*".

Se recogen en la revista trabajos doctrinarios de importantes autores nacionales y extranjeros, complementados por jurisprudencia, dictámenes de la URCDP, notas de interés, y entrevistas.

En la sección "Doctrina" se contó con los aportes de Chantal Bernier, ex comisionada de Privacidad Interina y comisionada adjunta de la Oficina del Comisionado de Privacidad de Canadá, Giovanni Buttarelli, supervisor europeo de Protección de Datos, Carlos Delpiazzo, exdecano de la Facultad de Derecho de la Universidad Católica del Uruguay, Mar España Martí, directora de la Agencia Española de Protección de Datos, Pablo Palazzi, profesor de Derecho de la Universidad de San Andrés, Ximena Puente de la Mora, expresidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos de México, y Ahti Saarenpaa, profesor emérito de Derecho Privado en la Universidad de Laponia. Asimismo, se realizó una entrevista a Jacob Kohnstamm, ex presidente de la Autoridad Holandesa de Protección de Datos, y se contó con el aporte a través de una nota de interés por parte de María Verónica Pérez Asinari – jefa de la Unidad Supervisión y Aplicación de la ley, de la oficina del Supervisor Europeo de Protección de Datos –.

La segunda edición de la Revista Uruguaya de Protección de Datos vio la luz en el marco de la Segunda Semana Nacional de la Protección de Datos.

En esta oportunidad nuevamente se contó con aportes doctrinarios, dictámenes de la URCDP, una nota de interés y una entrevista.

En la Sección Doctrina se visualizan los aportes de especialistas y autoridades nacionales y extranjeras, tal el caso de Roberto Balaguer, especialista en el uso de redes por menores; Marcelo Bauzá, académico y miembro del Consejo Consultivo de la URCDP, Ann Cavoukian, especialista en Privacy by Design y excomisionada de la autoridad de protección de datos de Ontario; Areli Cano Guadiana, comisionada del Instituto Federal de Acceso a la Información y Protección de Datos de los Estados Unidos Mexicanos; John Edwards, comisionado y presidente de la Conferencia Internacional de Autoridades de Privacidad y Protección de Datos; Sophie Kwasny, jefa de Protección de Datos del Consejo de Europa; Alvaro Sánchez Bravo, catedrático de la Universidad de Sevilla. Asimismo, se realizó una entrevista a Alessandra Pierucci, presidente del Bureau del Consejo Consultivo (TP-D) del Convenio Nº 108 del Consejo de Europa.

En la nota de interés se presentó la experiencia de inclusión en la educación primaria de la temática de la protección de datos personales, a través del relato de la experiencia vinculada con el Concurso de Protección de Datos reseñado supra.

Índice de criterios administrativos de Protección de Datos de la URCDP – 2009 – 2015

Durante el año 2015 se trabajó en la generación de un documento que recopilara los principales criterios definidos por el Consejo Ejecutivo a través de las resoluciones y dictámenes emitidos desde su creación. Así, se publicó el documento denominado "Criterios administrativos de la URCDP 2009 – 2015".

El objetivo de la publicación es realizar un aporte para el conocimiento y protección del derecho, en el marco de las actividades de promoción que ha venido llevando adelante la URCDP.

Se recopilaron así criterios asociados a transferencias internacionales, comunicación de datos a terceros, tratamiento de datos para publicidad y marketing, tratamiento de datos por entidades públicas, datos personales y fuentes públicas, registro de bases de datos, ejercicio de derechos, tratamiento de datos sensibles, videovigilancia, tratamiento de datos en la nube y sistema de sanciones.

Ciclo "Charlas de Café"

Las Charlas de Café son una iniciativa de la URCDP cuyo comienzo como proyecto piloto, durante el último trimestre del año 2015, se ha extendido exitosamente durante 2016 y 2017.

Se presentaron como una alternativa para discutir temas de vanguardia desde el foco de la protección de datos personales y el impacto que la inclusión de esta visión en los diferentes ámbitos del quehacer cotidiano verifica.

Las charlas son un mecanismo de acercamiento a propósito de una temática especializada y concreta a los distintos grupos de interés, de forma tal de plantear, a través de expertos especialmente convocados, inquietudes, experiencias, consultas y problemáticas de ineludible análisis.

Las charlas iniciales, desarrolladas en 2015 tuvieron como foco privacidad desde el diseño y big data.

Durante el año 2016 se trabajó a propósito de varios temas que convocaron fuertemente a la reflexión en su vínculo con la protección de datos personales, a saber:

- Educación y protección de datos
- Identidad digital y protección de datos
- Innovaciones tecnológicas y protección de datos personales: ciudades inteligentes e internet de las cosas

Y como cierre de año se presentó el Film *Democracy: fiebre de datos (Democracy. Im rausch der daten)*, del director David Bernet, con la participación además de las autoridades de la URCDP de representantes de la Delegación de la Unión Europea en Uruguay y del Goethe-Institut en tanto entidad titular de los derechos de la película. Además, esta instancia sirvió para poner en la discusión al Nuevo Reglamento Europeo de Protección de Datos Personales.

Se continuaron realizando estas actividades, bajo las consignas que se indican:

- ÉTICA: datos, dignidad y tecnología
- El Consejo de Europa como defensor de los Derechos Humanos y el Estado de Derecho: cuál es el interés para Uruguay, con la participación del Sr. Patrick Penninckx, jefe del Departamento de Sociedad de la Información del Consejo de Europa
- Inteligencia artificial y protección de datos.
- Videovigilancia y Privacidad.

4.4. RELACIONAMIENTO INTERNACIONAL

Participación en la Red Iberoamericana de Protección de Datos Personales (RIPD)

Desde la constitución de la URCDP, se ha participado en forma activa en las actividades convocadas por la RIPD.

Así se ha sido parte de todos los encuentros que han sido propuestos desde 2009 a la fecha, sea que éstos impliquen actividades de análisis académico, o reuniones de autoridades.

La URCDP se integró al Consejo Directivo en calidad de vocal en el año 2010.

En noviembre de 2016 Uruguay fue designado para la Presidencia de la Red, por un plazo de dos años, de acuerdo con su Reglamento. En este sentido, se ha patrocinado y se trabaja activamente a los efectos de dar cumplimiento a los compromisos incluidos en el documento denominado RIPD 2020.

Participación en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

Uruguay ha sido un activo participante en la Conferencia Internacional de Autoridades de Protección de Datos, colaborando en la redacción y apoyo de resoluciones emanadas de ella.

Integró además el Comité Ejecutivo de la Conferencia en los años 2012 y 2013.

Desde 2008, se ha concurrido a las reuniones citadas en Francia, España, Israel, México, Holanda, Mauricio, Marruecos, Hong Kong, habiendo a su vez, sido sede en el año 2012, tal como se señalara con anterioridad.

Participación en las reuniones plenarias vinculadas con el Convenio Nº 108 de Protección de Datos Personales

Incluso antes de la promulgación de la Ley Nº 19.030, de 27 de diciembre de 2012, Uruguay participó en calidad de observador de las reuniones plenarias del Convenio Nº 108 del Consejo de Europa.

Se ha participado en las discusiones correspondientes a la modernización del Convenio Nº 108, así como se continúa participando de las reuniones plenarias a los efectos de compartir la toma de decisiones que se entienden fundamentales para la unificación de criterios en la aplicación de las disposiciones vinculadas con éste.

Participación en diferentes ámbitos temáticos

La convocatoria y participación desde diferentes foros, seminarios y actividades de diversa índole han sido permanentes desde la creación de la URCDP.

Solo a los efectos de citar algunas de las actividades del último bienio, es posible citar:

- Global Privacy Dialogue, en Brasilia.
- Simposio sobre Ciberseguridad y Privacidad en Latinoamérica, en Miami.
- Global Privacy Summit 2016, en Washington.
- IV Reunión del Comité Ad Hoc de Protección de Datos (CAHDATA) y Conferencia Internacional del Convenio 108, en Estrasburgo
- Seminario "Derecho al olvido, tutela integral de la privacidad. Visión Iberoamericana", en México.
- Foro de Autoridades de Privacidad de Asia Pacífico (APPA) en Manzanillo, México.
- 10ª Conferencia Internacional Computers, Privacy & data Protection "The Age of Intelligent Machines", en Bruselas.
- Global Privacy Summit 2017, en Washington.
- Second Annual Latin American Privacy & Cybersecurity Symposium, en México.

5. METAS Y COMPROMISOS DE LA URCDP

La URCDP ha desarrollado desde sus inicios una gestión enfocada en el cumplimiento de metas anuales –y en ocasiones quinquenales- asociadas a proyectos específicos vinculados a la promoción, difusión y evolución del derecho a la protección de datos personales.

Tales metas poseen además consagración normativa en las sucesivas Agendas Digitales aprobadas por el Poder Ejecutivo. A modo de ejemplo, la última Agenda Uruguay Digital 2020 –aprobada por Decreto del Poder Ejecutivo N° 459/016, de 30 de diciembre de 2016- establece dentro de su Objetivo VIII asociado a la Confianza y seguridad en el uso de las tecnologías digitales, la meta 40 (adecuar y actualizar el marco normativo en los aspectos prioritarios para acompasar el desarrollo de la Agenda Uruguay Digital 2020, entre los que se encuentra la protección de datos personales).

Precisamente la "Evolución del Marco de Referencia" es uno de los cuatro grandes proyectos gestionados por la URCDP. Este proyecto tiene como metas la Reforma del Marco Normativo -teniendo en cuenta entre otros, el Reglamento (UE)

2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la modernización del Convenio Nº 108 del Consejo de Europa, y los Estándares aprobados por la RIPD en el XV Encuentro Iberoamericano de Protección de Datos-, la elaboración de un Texto Ordenado de Protección de Datos Personales, y la elaboración de Guías en diversos aspectos vinculados a la materia.

El segundo proyecto está orientado a la elaboración de "Contenidos Educativos y Acciones Directas a la Ciudadanía". Este proyecto tiene por metas la firma de convenios con el ámbito educativo y el concurso para escolares, además de la inclusión de la protección de datos en los planes de estudio de la educación formal y de la formación docente.

El tercer proyecto se vincula a la "Gobernanza y Fortalecimiento de Capacidades". Desde esa perspectiva se han trazado como metas la elaboración de documentos –memoria anual, revista de protección de datos, libro de resoluciones y dictámenes- y la realización de una Semana Nacional de Protección de Datos Personales. También se prevé la continuidad del ciclo Charlas de Café, nuevas ediciones de Curso de Protección de Datos, e instancias de capacitación en el interior, particularmente en los Gobiernos Departamentales.

Finalmente, la URCDP tiene como cuarto proyecto el de "Participación en la Comunidad Internacional", que tiene como metas el trabajo en la Red Iberoamericana de Protección de Datos Personales, y su Posicionamiento Internacional.

ANEXO 1 – ENLACES DE INTERÉS

Se presentan a continuación una serie de enlaces a normas y documentos de interés elaborados por la URCDP, y mencionados en el presente informe.

- Normativa nacional- https://www.datospersonales.gub.uy/inicio/normativa/nacional/
- Resoluciones- https://www.datospersonales.gub.uy/inicio/Resoluciones+y+ dictamenes/ resoluciones/
- Dictamenes- https://www.datospersonales.gub.uy/inicio/Resoluciones+y+ dictamenes/ dictamenes/
- Memorias- https://www.datospersonales.gub.uy/inicio/publicaciones/memorias-nuales/
- Libros y recopilaciones- https://www.datospersonales.gub.uy/inicio/publicaciones/Libros+y+recopilaciones/
- Informes- https://www.datospersonales.gub.uy/inicio/publicaciones/informes/
- Guías- https://www.datospersonales.gub.uy/inicio/publicaciones/Guias+de+ayuda/
- Boletines- https://www.datospersonales.gub.uy/inicio/publicaciones/boletines/
- Revistas de Protección de Datos Personales- https://datospersonales.gub.uy/inicio/publicaciones/Libros+y+recopilaciones/
- Criterios administrativos 2009-2015- https://datospersonales.gub.uy/inicio/publicaciones/Libros+y+recopilaciones/
- Curso en línea- https://www.datospersonales.gub.uy/inicio/Sobre+datos +personales/Ciudadanos/Curso+en+linea/
- Campaña "Tus Datos Valen"- https://www.datospersonales.gub.uy/inicio/ Sobre+datos+personales/Ciudadanos/tusdatosvalen/?WCM_Page.ResetAll=TRUE

ENTREVISTA

BRUNO
GENCARELLI

Es el responsable de la Unidad de flujos internacionales y protección de datos en la Comisión Europea (DG Justicia y Consumidores). Lideró el trabajo de la Comisión en el área de protección de datos en la reforma legislativa y en las negociaciones UE-EE.UU. En ese sentido, tuvo a su cargo la delegación de la Comisión en las negociaciones con el Parlamento y el Consejo de Europa que derivó en la adopción del Reglamento General de Protección de Datos y la Directiva (UE) N° 2016/680, del Parlamento Europeo y del Consejo.

Fue uno de los principales negociadores del "Privacy Shield" entre UE-EE.UU. y recientemente negoció el acuerdo mutuo de adecuación con Japón. Previamente fue miembro de los Servicios Legales de la Comisión Europea y asistente judicial en el Tribunal de Justicia Europeo, habiéndose desempeñado anteriormente en la actividad privada.

Posee títulos en derecho y ciencia política y desarrolla actividad docente en la cátedra de Derecho de la Competencia de la UE en "Sciences Po Paris". Es autor de varias publicaciones en derecho de la UE.

1. COULD YOU SAY SOMETHING ABOUT YOUR ROLE IN DATA PROTECTION? YOU ARE HEAD OF THE INTERNATIONAL DATA FLOWS AND PROTECTION UNIT AT THE EUROPEAN COMMISSION. WHAT ARE THE RESPONSIBILITIES AND DUTIES OF SUCH UNIT?

I am working in this field since 2012. In particular, I was in charge of the European Commission's work in the area of data protection in the decisive years of the legislative reform and the EU-US negotiations. This included heading the Commission's delegation in the interinstitutional negotiations with the European Parliament and the Council (the body that represents the Member States of the EU) that resulted in the adoption of the General Data Protection Regulation (GDPR) and the "Law Enforcement Directive" (Directive 2016/680). I was also one of the lead negotiators of the EU-US Privacy Shield and "Umbrella Agreement".

After the adoption of the EU data protection legislative reform, it was decided to give more emphasis to the international dimension of privacy and develop the synergies between protecting privacy and facilitating data flows, be it to support trade or strengthen cooperation between public authorities. Contrary to what is sometimes said, promoting high standards of data protecting and facilitating such exchanges are complementary objectives, they can – and, actually, they should – go hand in hand. Think about trade: as commercial exchanges in our digital area rely increasingly on personal data flows, the privacy and security of such data has become a central factor of consumer trust and hence of the competitiveness of the goods and services that are being offered on the global marketplace. This is also true for cooperation between public authorities. For example, in an interconnected world where crime rarely stops at national borders, the swift exchange of personal data is essential for an effective response to crime. Convergent data protection safeguards are thus an important element for more efficient and quicker cooperation between law enforcement authorities of different countries, as they notably contribute to build confidence between such authorities and ensure legal certainty when data is exchanged and then used in criminal proceedings.

The unit pursues these objectives and addresses these issues in many ways. Our "roadmap" is described in the Commission's Communication of 10 January 2017 "Exchanging and Protecting Personal Data in a Globalised World" but let me give you just a few examples of our work in the last months. For instance, we negotiated for the EU

1. ¿PODRÍA COMENTARNOS ALGO SOBRE SU ROL EN LA PROTECCIÓN DE DATOS? UD. ES EL DIRECTOR DE LA UNIDAD DE FLUJOS INTERNACIONALES Y PROTECCIÓN DE DATOS EN LA COMISIÓN EUROPEA. ¿CUÁLES SON LAS RESPONSABILIDADES Y TAREAS DE DICHA UNIDAD?

Estoy trabajando en este tema desde el año 2012. En particular, estuve a cargo del trabajo de la Comisión Europea en el área de la protección de datos en los años decisivos de la reforma y de las negociaciones UE-EE.UU. Esto incluyó liderar la delegación de la Comisión en las negociaciones interinstitucionales con el Parlamento Europeo y el Consejo (el cuerpo que representa a los Estados Miembros de la UE), que resultaron en la adopción del Reglamento General de Protección de Datos (RGPD) y la "Directiva para el Cumplimiento de la Ley" (Directiva 2016/680). También fui uno de los negociadores líderes del Escudo de Privacidad UE-EE.UU. y el "Umbrella Agreement".

Luego de la adopción de la reforma en la legislación de protección de datos de la UE, se decidió dar más énfasis a la dimensión internacional de la privacidad y desarrollar sinergias entre la protección de la privacidad y la facilitación de los flujos de datos, de forma de apoyar el comercio o fortalecer la cooperación entre autoridades públicas. Al contrario de lo que en ocasiones se menciona, la promoción de altos estándares en protección de datos y la facilitación de esos intercambios son objetivos complementarios, pueden –y de hecho deberían- ir mano a mano. Pensemos en el comercio: en tanto los intercambios comerciales en nuestra área digital se apoyan cada vez más en los flujos de datos personales, la privacidad y seguridad de tales datos se ha vuelto el factor central de la confianza de los consumidores y por ende de la competitividad de los productos y servicios que se ofrecen en el mercado global. Esto también es así para la cooperación entre autoridades públicos. Por ejemplo, en un mundo interconectado dónde el crimen pocas veces se detiene en las fronteras nacionales, el rápido intercambio de datos personales es esencial para una efectiva respuesta al delito. La convergencia en las salvaguardas para la protección de datos es por ende un elemento importante para una más rápida y eficiente cooperación entre las autoridades de policía en los distintos países, contribuyen notablemente a crear confianza entre dichas autoridades y garantizan la seguridad jurídica cuando los datos son intercambiados y empleados luego en procedimientos criminales.

the modernisation of Convention 108 of the Council of Europe and played an important role in the successful conclusion of such negotiations in May of this year. This is a key achievement as Convention 108 is the only binding international instrument in this area and it is a universal treaty, open to all countries in the world and which has indeed an increasingly universal membership. And as we know, this is also thanks to Uruguay which was the first non-European State to join this convention. Then in the summer we concluded our adequacy talks with Japan, resulting for the first time in a "two-way adequacy" that will create the world's largest area of free and safe data flows. In this way, it will also complement and amplify the benefits of the EU-Japan free trade agreement that was signed in July: a very concrete illustration of the type of synergies I was referring to. Of course, this was also the year of the entry into application of the GDPR on 25th May. We have thus engaged with many international partners, from Latin America to Asia, to explain the GDPR, share our experience with the reform of data protection rules and learn from recent developments in privacy legislation and enforcement in other countries.

As you can see, we are very busy and are looking forward to be even busier in the coming months, in particular with our Latin American partners with whom we share so much common ground.. On the basis of their shared values, Latin American countries and the EU can certainly play a key role in further promoting and building on the developing convergence in privacy standards, to the benefit of their citizens and their economy.

2. WHAT MAKES A COUNTRY "ADEQUATE" IN THE DATA PROTECTION FIELD? HOW HAS THIS CONCEPT EVOLVED FROM DIRECTIVE 45/96/CE TO THE GDPR?

The GDPR has essentially harmonized and modernized the data protection rules that have been place in Europe for more than 20 years under Directive 45/96. While it has introduced some important novelties, it is thus characterized by a great deal of continuity with the previously applicable rules, including in the area of international transfers of data. As regards specifically adequacy and following the Schrems judgment of the European Court of Justice, the GDPR has mainly clarified the test to be applied by the European Commission when making an adequacy finding. It is required to assess whether a third country ensures a level of protection "essentially equivalent" to the one guaranteed in the EU. This involves a comprehensive assessment, that is not limited

La Unidad persigue estos objetivos y se enfoca en estos temas de distintas maneras. Nuestra "hoja de ruta" se describe en la Comunicación de la Comisión de 10 de enero de 2017 "Exchanging and Protecting Personal Data in a Globalised World", pero déjenme darles algunos ejemplos de nuestro trabajo en los últimos meses. Por ejemplo, negociamos con la UE la modernización del Convenio 108 del Consejo de Europa y jugamos un rol importante en la finalización exitosa de esas negociaciones en mayo de este año. Este es un hito fundamental ya que el Convenio 108 es el único instrumento vinculante internacional en esta área, y es un tratado internacional, abierto a todos los países del mundo, y que de hecho ha efectivamente aumentado su membresía universal. Y, como sabemos, esto también es gracias a Uruguay, que fue el primer país no europeo en adherirse a este convenio. Luego en el verano concluimos nuestras conversaciones para la adecuación con Japón, resultando por primera vez en una "adecuación bilateral", que creará el área de intercambios libres y seguros de datos, más grande del mundo. En este sentido, también complementa y amplifica los beneficios del acuerdo de libre comercio UE-Japón firmado en julio: una muy concreta muestra de los tipos de sinergias a los que me estaba refiriendo. Por supuesto, este fue el año de la entrada en vigencia del RGPD, el 25 de mayo. Nos encontramos por ende vinculados con muchos socios internacionales de América Latina y Asia, para explicar el RGPD, compartir nuestras experiencias con la reforma de las reglas de protección de datos y aprender de los más recientes desarrollos en la legislación de privacidad y cumplimiento de la ley en otros países.

Como pueden ver, estamos muy ocupados y buscando encontrarnos aún más ocupados en los meses venideros, en particular con nuestros socios de América Latina con quienes compartimos muchas cuestiones comunes. Con base en nuestros valores compartidos, los países de América Latina y la UE pueden claramente jugar un rol fundamental en la continua promoción y construcción de la convergencia en desarrollo en estándares de privacidad, para beneficiar a sus ciudadanos y sus economías.

2. ¿QUÉ HACE A UN PAÍS "ADECUADO" EN EL CAMPO DE LA PROTECCIÓN DE DATOS?¿CÓMO HA EVOLUCIONADO ESTE CONCEPTO DESDE LA DIRECTIVA 45/96/CE AL RGPD?

El RGPD ha esencialmente armonizado y modernizado las reglas de la protección de datos vigentes en Europa por más de 20 años bajo la Directiva 45/96. Mientras que ha introducido algunas no-

to the privacy legislation of the third country, its supervision and enforcement but also the conditions under which its public authorities can access personal data in particular for law enforcement and national security reasons. In other words, the assessment has to cover the entire possible "life cycle" of the data following its transfer.

At the same time, it is important to stress that the adequacy standard does not require a "photocopy", a point-to-point replication of EU rules, but rather that the foreign system overall ensures a comparable level of protection. To use the Court of Justice's words, this comparable level of protection can be ensured through "means [...] that may differ from those employed within the European Union". This is also reflected in the "adequacy referential" adopted this year by the European Data Protection Board (the body that brings together the data protection authorities of the EU Member States) and that guides the Commission in its adequacy talks with foreign countries.

As an adequacy finding is made at a certain point in time and privacy rules may evolve over time, both in the EU and the foreign country, the GDPR has also introduced an obligation for the Commission to closely monitor such decisions and adapt them in case of developments affecting the level of protection ensured by the third country in question. To that end, periodic reviews will be held, at least every four years. This dynamic approach applies also to existing adequacy decisions, adopted under the 1995 Directive, which could need to be amended or even withdrawn in case they would no longer meet the applicable standard. That is why we have launched an in-depth dialogue with the concerned countries, including of course Uruguay, to update our understanding of their privacy system and work towards ensuring the continuity of these pre-GDPR decisions under the new rules.

Another important innovation of the EU data protection reform in this area is the introduction of the possibility for adequacy findings also in the criminal law enforcement sector under Directive (EU) 2016/680. We are looking forward to explor-

vedades importantes, también se caracteriza por una importante continuidad de reglas previamente aplicables, incluyendo aquellas del área de las transferencias internacionales de datos. En lo que refiere específicamente a la adecuación luego de la sentencia Schrems del Tribunal de Justicia Europeo, el RGPD ha clarificado en buena manera el examen que debe aplicarse por la Comisión Europea cuando realiza una comprobación de adecuación. Se requiere evaluar si un tercer país asegura un nivel de protección "esencialmente equivalente" al garantizado en la UE. Esto involucra un análisis comprensivo, que no se limita a la legislación de privacidad del tercer país, su supervisión y cumplimiento, sino también a las condiciones bajo las cuales las autoridades públicas pueden acceder a la información personal en particular por razones de policía y de seguridad nacional. En otras palabras, el análisis debe cubrir todo el "ciclo de vida" posible de los datos luego de su transferencia.

Al mismo tiempo, es importante resaltar que el estándar de adecuación no requiere una "fotocopia" o una replicación punto a punto de las reglas de la UE, sino más bien que todo el sistema extranjero asegure un nivel de protección comparable. Para utilizar las palabras del Tribunal de Justicia, este nivel comparable de protección debe asegurarse a través de "medios (...) que pueden diferir de aquellos empleados en la Unión Europea". Esto también se refleja en la "marco de referencia de la adecuación" adoptado este año por el Comité Europeo de Protección de Datos (el cuerpo que une a las autoridades de protección de datos de los Estados Miembros de la UE) y que guía a la Comisión en sus conversaciones de adecuación con países extranjeros.

En tanto una comprobación se realiza en un momento del tiempo determinado y las reglas de privacidad evolucionan con el tiempo, tanto en la UE como en el país extranjero, el RGPD también ha introducido la obligación de la Comisión de monitorear en forma cercana tales decisiones y adaptarlas en el caso de desarrollos que afecten el nivel de protección asegurado por el tercer país

ing this new avenue with our international partners to facilitate law enforcement cooperation on the basis of strong data protection safeguards.

3. CONVENTION 108 WAS ONE THE FIRST INSTRUMENTS TO INTRODUCE THE CONCEPT OF "ADEQUATE" PROTECTION. ARE THERE ANY DIFFERENCES BETWEEN THE SCOPE OF SUCH CONCEPT IN THE MODERNIZED VERSION OF THE CONVENTION AND THE GDPR? HOW IMPORTANT IS BEING PART OF CONVENTION 108 WHEN BEING EVALUATED FOR AN ADECQUACY DECISION BY THE EUROPEAN COMMISSION?

Let me first say that the modernization of Convention 108 is a very significant development that will allow for a higher level of convergence among the signatory parties and, more generally, positively influence the international conversation on privacy at a time when there is a growing demand for common standards in this area. This is already reflected in the sharp increase of non-European countries that have recently joined Convention 108 either as Parties or Observers or that are in the process of acceding. As the only international treaty on data protection, it is also remarkable that it is a truly horizontal instrument that covers all types of processing including in the most sensitive areas such as national security.

That said, as any international convention, Convention 108 remains at a certain level of generality, it sets out a number of principles that have then to be further implemented and operationalized in domestic legislation. The GDPR is one of these laws that, while based notably on Convention 108, provides for a much more detailed data protection regime. That detailed legal framework with its rights, obligations and supervision/enforcement mechanisms constitutes the benchmark against which the adequacy ("essential equivalence") test has to be applied to benefit from free flow of data with the EU

Against that background, accession to Convention 108 does not automatically ensure a finding of adequacy under EU law but, as expressly recognized by recital no. 105 of the GDPR, it is certainly an important element to be taken into account by the European Commission when carrying out its assessment of the third country's data protection system. This will be even more true for the modernized Convention 108 that contains a number of enhanced protections and safeguards, for example as regards the role and powers of data protection authorities.

en cuestión. Con ese fin, se realizarán revisiones periódicas, al menos cada cuatro años. Esta aproximación dinámica se aplica también a decisiones de adecuación vigentes, adoptadas bajo la Directiva de 1995, que podrían ser modificadas o incluso retiradas en caso de que no se lograra llegar al estándar aplicable. Es por ello que se ha lanzado un diálogo profundo con los países correspondientes, incluyendo por supuesto a Uruguay, a efectos de actualizar nuestro conocimiento del sistema de privacidad y trabajar conjuntamente para asegurar la continuidad de estas decisiones pre-RGPD bajo las nuevas reglas.

Otra innovación importante de la reforma en protección de datos de la UE en esta área es la introducción de la posibilidad de comprobaciones de adecuación en el sector de policía bajo la Directiva (UE) 2016/680. Estamos deseosos de explorar esta nueva vía con nuestros socios internacionales para facilitar la cooperación en el cumplimiento de la ley con base en fuertes salvaguardas en protección de datos.

3. EL CONVENIO 108 FUE UNO DE LOS PRIMEROS INSTRUMENTOS EN INTRODUCIR EL CONCEPTO DE PROTECCIÓN "ADECUADA". ¿EXISTEN DIFERENCIAS ENTRE EL ALCANCE DEL CONCEPTO EN LA VERSIÓN MODERNIZADA DEL CONVENIO Y EL RGPD?¿QUÉ TAN IMPORTANTE ES FORMAR PARTE DEL CONVENIO 108 CUANDO SE ESTÁ SIENDO EVALUADO PARA UNA DECISIÓN DE ADECUACIÓN POR LA COMISIÓN EUROPEA?

Déjenme primero decirles que la modernización del Convenio 108 es un desarrollo muy significativo que permitirá un más alto nivel de convergencia entre las partes signatarias y, en general, una influencia positiva en las conversaciones internacionales en privacidad en un momento en que existe una demanda creciente para estándares comunes en el tema. Esto ya se ha reflejado en el fuerte crecimiento de países no europeos que han recientemente adherido al Convenio 108, tanto como Miembros u Observadores, o que se encuentran en proceso de adhesión. Por ser el único tratado internacional en protección de datos, también es destacable que es un instrumento verdaderamente horizontal que cubre distintos tipos de tratamiento, incluyendo áreas muy sensibles cómo la seguridad nacional.

Dicho esto, como cualquier convenio internacional, el Convenio 108 posee cierto nivel de generalidad, establece un conjunto de principios que

4. IN YOUR OPINION, WHAT ARE THE BENEFITS OF ACHIEVING AN ADEQUACY DECISION BY THE EUROPEAN COMMISSION FOR COUNTRIES THAT ARE NOT A PART OF THE EEA?

In our digital world, convergence of privacy standards pays off and brings very tangible benefits. EU adequacy is one of these benefits.

As a result of an adequacy decision by the Commission, data can flow freely between the EU and the third country in question with no need for additional safeguards to be put in place. It is therefore the most straightforward, less burdensome and less costly way to ensure secure and stable data flows. By assimilating transfers to the concerned foreign country to intra-EU transmissions of data, an adequacy decision also ensures privileged access to the EU single market – and its 500 million customers – for that country's commercial operators. In other words, it provides them with a clear competitive advantage.

5. HOW DOES THE NEW REGULATION IMPACT ON THOSE COUNTRIES THAT WERE CONSIDERED ADECQUATE UNDER THE RULES OF THE DIRECTIVE? HOW IS THE EUROPEAN COMMISSION PLANNING ON UNDERTAKING THE PROCESS OF MONITORING DEVELOPMENTS THAT MIGHT AFFECT ADECQUACY DECISIONS?

Let me first clarify that none of the current "adequate countries" is losing its adequacy status because of the entry into application of the GDPR: the new regulation provides expressly that the decisions adopted under Directive 95/46 remain in force until amended, repealed or replaced by a new Commission's decision.

That said, as explained above, adequacy decisions are "living" documents that need to be closely monitored, made subject to period reviews and adapted in case of developments affecting the level of protection ensured by the third country in question. In application of these requirements, the Commission will have to report to the Europe Parliament and the Council by May 2020 on the adequacy decisions adopted under Directive 45/96 (such as the one concerning Uruguay).

To that end, we are in contact with the authorities of the concerned countries to receive updated information on the functioning of their adequacy finding. In particular, this requires being informed on any relevant development of the privacy system that has taken place since the adoption

deben ser posteriormente implementados y operativizados en la legislación doméstica. El RGPD es una de esas leyes qué, aun cuando se basan en el Convenio 108, proveen un régimen de protección de datos mucho más detallado. Este marco legal detallado con sus derechos, obligaciones y mecanismos de supervisión/cumplimiento constituyen un parámetro contra el cual el examen de adecuación ("esencialmente equivalente") debe ser aplicado para beneficiarse de los libres flujos de datos con la UE.

Contra este escenario, la adhesión al Convenio 108 no garantiza automáticamente una decisión de adecuación bajo la ley de la UE, pero, como se ha reconocido expresamente por el Considerando N° 105 del RGPD, es seguramente un elemento importante a tener en cuenta por la Comisión Europea al llevar adelante la evaluación del sistema de protección del tercer país. Esto será aún más cierto para la versión modernizada del Convenio 108 que contiene un número de protecciones y salvaguardas aumentadas, como por ejemplo las que hacen al rol y los poderes de las autoridades en protección de datos.

4. EN SU OPINIÓN, ¿CUÁLES SON LOS BENEFICIOS PARA LOS PAÍSES QUE NO SON PARTE DEL AEE, DE ALCANZAR UNA DECISIÓN DE ADECUACIÓN POR LA COMISIÓN EUROPEA?

En nuestro mundo digital, la convergencia de estándares de privacidad rinde frutos y trae beneficios muy tangibles. La adecuación a la UE es uno de esos beneficios.

Como resultado de la decisión de adecuación por la Comisión, los datos pueden fluir libremente entre la UE y el tercer país en cuestión sin necesidad de poner en práctica salvaguardas adicionales. Es por ende la forma más directa, menos compleja y menos costosa de asegurar flujos de datos seguros y estables. Al asimilar las transferencias al país extranjero correspondiente, a las transmisiones de datos intra-UE, una decisión de adecuación asegura el acceso privilegiado al mercado único de la UE –y sus 500 millones de consumidores- para los operadores comerciales de ese país. En otras palabras, les otorga una clara ventaja competitiva.

of the decision, including in the field of enforcement, as well as on the rules applying to access to data by public authorities in particular for law enforcement and national security purposes (this has become a key requirement of the adequacy test under the GDPR). Receiving such information in time for our assessment is crucial to make this exercise a successful one and, ultimately, ensure the continuity and further development of the adequacy decision.

6. EUROPEAN DATA PROTECTION PRINCIPLES HAVE BEEN INFLUENCING NEW REGULATIONS WORLDWIDE. WHAT ARE IN YOUR OPINION THE MAIN BENEFITS OF HAVING AN HOMOGENEOUS SET OF DATA PROTECTION RULES ACROSS COUNTRIES?

There is indeed increased convergence in privacy standards at the international level. Today more than 120 countries, from almost all regions of the globe, have data protection laws in place. Many more, from Chile to India, are considering adopting legislation in this field. This expansion of privacy laws is remarkable not only from a quantitative but also from a qualitative point of view: many of the new or modernised laws tend to be based on common elements such as a comprehensive legislation (rather than sectorial rules), a set of enforceable rights, the setting up of an independent supervisory authority, etc.

This is not a one way process but the result of different data protection systems learning from each other (for ex. the GDPR borrowed from other systems principles such as accountability, safeguards such as data breach notification, tools such a privacy impact assessments). It also shows that we are all facing similar challenges and trying to seize similar opportunities: more than ever before, the issues we are dealing with are of a global nature, they are not confined to the borders of a continent – let alone a single country – and require a global answer. To give just one example, today many data breaches simultaneously affect persons

5. ¿CÓMO IMPACTA LA NUEVA REGULACIÓN EN LOS PAÍSES QUE ERAN CONSIDERADOS ADECUADOS BAJO LAS REGLAS DE LA DIRECTIVA?¿COMO ESTÁ PLANEANDO LA COMISIÓN EUROPEA LLEVAR ADELANTE LOS PROCESOS DE MONITOREO DE LOS DESARROLLOS QUE PUEDAN AFECTAR LAS DECISIONES DE ADECUACIÓN?

En primer lugar permítanme clarificar que ninguno de los actuales "países adecuados" perderá su estatus de adecuación sólo por la entrada en vigencia del RGPD: la nueva regulación establece expresamente que las decisiones adoptadas bajo la Directiva 95/46 se mantienen vigentes hasta su modificación, rechazo o reemplazo por una nueva decisión de la Comisión.

Dicho esto, como se explicó más arriba, las decisiones de adecuación son documentos "vivos" que necesitan ser monitoreados de cerca, sujetos a revisiones periódicas y, adaptados, en caso de desarrollos que afecten el nivel de protección asegurado por el tercer país en cuestión. En aplicación de estos requerimientos, la Comisión reportará al Parlamento Europeo y el Consejo en mayo de 2020 respecto de las decisiones de adecuación adoptadas bajo la Directiva 45/96 (como la referente a Uruguay).

Para ese fin, nos encontramos en contacto con las autoridades de los países correspondientes a efectos de recibir información actualizada sobre el funcionamiento de sus decisiones de adecuación. En particular, esto requiere ser informados de cualquier desarrollo relevante para el sistema de privacidad que se haya tomado desde la adopción de la decisión, incluyendo en el campo de cumplimiento de la ley, así como en las reglas aplicables al acceso a la información por autoridades públicas en particular para propósitos de policía y seguridad nacional (esto se ha convertido en un requerimiento esencial para el examen de adecuación bajo el RGPD). El recibir tal información en tiempo para nuestra evaluación es crucial para mantener el éxito de este ejercicio, y en definitiva, asegurar la continuidad y el futuro desarrollo de la decisión de adecuación.

in several jurisdictions with negative consequences for their rights and individual situations, consumer's confidence, the reputation and profit of the concerned companies etc.

And in a world that is so often characterised by uncertainty and instability, this developing convergence is very positive, for a number of reasons.

In particular, this trend offers new opportunities to facilitate data flows and thus trade, at both regional and global level. Being part of this global trend helps the domestic economy, by contributing to an environment conducive to direct investment and improving trust between commercial partners. It makes it easier for companies to navigate between different systems, by notably cutting compliance costs, and enhance the concerned country's integration in the global data driven economy.

As we have already stressed, having common data protection rules can also greatly facilitate the exchanges of data between public authorities, including in the context of law enforcement cooperation.

Last but certainly not the least, this convergence improves the level of protection of some of the most fundamental rights of an individual when his or her data is transferred abroad. That brings us back to the beginning of our conversation: the virtuous circle that modern privacy laws can achieve between better protection of privacy as a human right, enhanced consumers' confidence in how privacy and security of their data is guaranteed, particularly online, and economic growth.

6. LOS PRINCIPIOS DE PROTECCIÓN DE DATOS EUROPEOS HAN INFLUENCIADO NUEVAS REGULACIONES EN TODO EL MUNDO. ¿CUÁLES SON EN SU OPINIÓN LOS BENEFICIOS MÁS IMPORTANTES DE TENER UN CONJUNTO DE REGLAS EN PROTECCIÓN DE DATOS HOMOGÉNEAS EN DISTINTOS PAÍSES?

Existe de hecho un incremento en la convergencia en los estándares de privacidad a un nivel internacional. Hoy en día más de 120 países, de casi todas las regiones del globo, han adoptado leyes en protección de datos. Muchos más, desde Chile hasta India, están considerando adoptar leyes en este campo. Esta expansión de leyes de privacidad es destacable no sólo desde un punto de vista cuantitativo sino también cualitativo: muchas de las nuevas o modernizadas leyes tienden a estar basadas en elementos comunes tales cómo una legislación comprensiva (en lugar de reglas sectoriales), un conjunto de derechos exigibles, la creación de una autoridad de supervisión independiente, etc.

Este no es un proceso de una vía sino el resultado de distintos sistemas de protección de datos aprendiendo de los otros (por ejemplo, el RGPD tomó prestado de otros sistemas principios cómo el de responsabilidad demostrada, salvaguardas cómo la notificación de vulneraciones de seguridad, herramientas cómo los análisis de impacto en privacidad). También muestra que todos estamos enfrentando desafíos similares, y tratando de aprovechar oportunidades similares: más que nunca antes, las cuestiones con las que lidiamos son de una naturaleza global, no se encuentran confinadas a las fronteras del continente –menos aún, de un solo país- y requieren de una respuesta global. Para dar un solo ejemplo, hoy en días muchas vulneraciones de datos afectan en forma simultánea a personas en distintas jurisdicciones con consecuencias negativas para sus derechos y situaciones personales, la confianza en el consumidor, la reputación y ganancias de las compañías involucradas, etc.

Y en un mundo frecuentemente caracterizado por las incertezas y la inestabilidad, esta convergencia en desarrollo es muy positiva, por un conjunto de razones.

En particular, esta tendencia ofrece nuevas oportunidades para facilitar los flujos de datos y en consecuencia el comercio, tanto a nivel regional cómo global. Ser parte de una tendencia global apoya a la economía doméstica, contribuyendo a un ambiente conducente a la inversión directa y a mejorar la confianza entre socios comerciales. Hace más sencillo para las compañías el navegar

entre distintos sistemas, al reducir notablemente los costos de cumplimiento, y mejora la integración del país correspondiente en una economía global dirigida por los datos.

Cómo ya hemos remarcado, tener reglas de protección de datos comunes pueden también facilitar grandemente los intercambios de datos entre autoridades públicas, incluyendo en el contexto de la cooperación en el cumplimiento de la ley.

En último lugar, aunque no menos importante, la convergencia mejora el nivel de protección de algunos de los más fundamentales derechos de los individuos cuando sus datos están siendo transferidos al exterior. Esto nos lleva al inicio de nuestra conversación: el círculo virtuoso que las leyes de privacidad modernas pueden alcanzar, entre una mejor protección de la privacidad como derecho humano, una confianza de los consumidores más elevada en cuanto a cómo es garantizada la privacidad y seguridad de sus datos, particularmente en línea, y el crecimiento económico.

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

REVISTA PDP

Revista Uruguaya de Protección de Datos Personales

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay