RETOS

de la
PROTECCIÓN
de
DATOS
PERSONALES
en el
SECTOR
PÚBLICO

Directorio:

Oscar M. Guerra Ford
Comisionado Ciudadano Presidente

Jorge Bustillos Roqueñí
Comisionado Ciudadano

Areli Cano Guadiana
Comisionada Ciudadana

Salvador Guerrero Chiprés
Comisionado Ciudadano

Agustín Millán Gómez
Comisionado Ciudadano

© 2011
Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Queda prohibida la reproducción parcial o total, directa o indirecta del contenido de la presente obra, sin contar previamente con la autorización expresa y por escrito de los editores, en términos de lo así previsto por la Ley Federal del Derecho de Autor y, en su caso, por los tratados internacionales aplicables.

IMPRESO Y HECHO EN MÉXICO

www.infodf.org.mx

La Morena No. 865, esquina Av. Cuauhtémoc, Colonia Narvarte Poniente, Delegación Benito Juárez, C.P. 03020, México, D.F.

RETOS

de la
ROTECCIÓN
de
ATOS
ERSONALES
en el
ECTOR
ÚBLICO

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal
infodf

ÍNDICE

Introducción 9

Reconocimiento normativo del derecho a la protección de datos personales en el ámbito internacional
Agustín Millán Gómez 19

La agencia de Protección de Datos de la Comunidad de Madrid. Desarrollo normativo y evolución de sus funciones
Santiago Abascal Conde / Lourdes Hernández Crespo 49

Convergencias y divergencias: acceso a la información y la tutela de los datos personales
Miguel Pulido Jiménez 79

Las legislaciones de protección de datos personales en el país
Oscar M. Guerra Ford 103

Desarrollo legislativo en materia de datos personales en las entidades federativas, la importancia de una legislación especial en el ámbito estatal
Luis Gustavo Parra Noriega 145

La protección de los datos personales
Eugenio Monterrey Chepov / Gregorio Castillo Porras 178

La seguridad como una pieza clave en el rompecabezas de la protección de datos personales
Lina Ornelas Núñez / Samantha Alcalde Urbina 217

Protección de datos personales en los medios de comunicación
Blanca Lilia Ibarra Cadena 245

Políticas públicas para proteger los datos personales de los menores en internet y redes sociales
Miroslava Carrillo Martínez 267

La protección de los datos personales en el sector salud
Germán Fajardo Dolci 293

La protección de los datos personales en materia político - electoral
Jorge Bustillos Roqueñí 317

Protección de datos personales en los programas sociales
Pablo Yanes Rizo / Alejandro López Mercado
Rocío Aguilar Solache 347

Difusión y protección de datos personales por parte de los órganos de impartición de justicia: diez años de publicidad
Carlos G. Gregorio 373

Elementos fundamentales para la protección de datos personales en la procuración e impartición de justicia
Areli Cano Guadiana 401

Dilemas conceptuales en torno a la transparencia y la protección de datos personales en la procuración e impartición de justicia en el Distrito Federal
Miguel Ángel Mancera Espinosa 423

Datos personales e información de interés público en las averiguaciones previas
Darío Ramírez Salazar 453

Tensión y dilemas en la protección de los datos personales
Salvador Guerrero Chiprés 477

Introducción

Actualmente, la posibilidad de injerencias en nuestra vida privada ha incrementado exponencialmente con la evolución de las tecnologías de la información. La circulación de los datos personales es prácticamente ilimitada y la capacidad de elaborar perfiles de los ciudadanos al integrar distintas bases de datos es mayor.

En el ejercicio de sus funciones las autoridades gubernamentales recaban una gran cantidad de datos personales de sus gobernados, información patrimonial, del estado de salud, incluso de su vida familiar, entre otras. Además, el uso de tecnologías es más frecuente al momento de recabar y tratar los datos personales para la realización de trámites.

Un tratamiento inadecuado de la información personal podría traducirse en usos que afecten la vida de las personas, exponiéndolos al riesgo de ser objetos de discriminación o hacerlos blanco de delitos graves como el secuestro o el robo de identidad. Por este motivo el tratamiento de esta información debe ser tratada con apego a los principios legalidad, calidad, disponibilidad, confidencialidad, seguridad que permitan que esta información sólo accedida por personas autorizadas.

Actualmente es fácil realizar transferencias de información con gran rapidez y la conectividad existente entre las redes de información vulnera de manera importante la privacidad de las personas. Los gobiernos, están obligados a proteger el vasto cúmulo de información personal que tiene sobre sus gobernados, así como limitar la recolección de los datos personales a los supuestos previstos en la legislación vigente.

Este libro tiene como objetivo abordar algunos de los retos y dilemas que enfrentan los gobiernos al implementar las normativas en materia de protección de datos personales, en un país donde hay un fuerte impulso a las políticas de transparencia y rendición de cuentas.

Sin lugar a dudas no hay soluciones únicas, los razonamientos vertidos por los autores nos inducen a una profunda reflexión de la heterogeneidad normativa que existe en México al regular el derecho

constitucional a la protección de los datos personales, pero más aún, nos muestran los dilemas que surgen al interpretar las leyes para ponderar el interés público y derecho personal de la protección de la información de carácter personal.

Es posible encontrar diversos casos prácticos que muestran como el órgano garante del Distrito Federal, el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, ha realizado ejercicios de ponderación de derechos, conocidos como pruebas de interés público, para resolver en qué casos debían ser divulgados ciertos datos personales.

El texto del Lic. Agustín Millán, Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, presenta un análisis del estado actual que guarda el derecho a la protección de datos personales en el mundo. Para lo cual realiza un análisis de la normativa supranacional más relevante Las cuales, desde su perspectiva se han constituido como un referente importante para múltiples naciones.

De acuerdo a la revisión presentada por el Lic. Millán, actualmente, existen 77 países que cuentan con una legislación reglamentaria en materia de protección de datos personales. Según el autor este dato se constituye en un referente respecto del impacto que, a nivel internacional, conlleva que cada uno de los Estados cuente con una normativa interna, adoptando los principios internacionales dictados a proteger los datos de carácter personal, tanto en poder del propio Estado como en posesión de particulares.

Posteriormente, Santiago Abascal Conde y Lourdes Hernández Crespo, presentan un texto en el que muestra experiencias relevantes de la Agencia de Protección de Datos de la Comunidad de Madrid en la implementación de la Ley de Protección de Datos Personales, con el objetivo de contribuir a la identificación de experiencias para facilitar el ejercicio de las atribuciones de órganos garante homólogos en otros países. En este trabajo destaca de manera particular el esfuerzo realizado por la agencia para trabajar de manera conjunta con servidores públicos, logrando un equilibrio adecuado entre asesoría y fiscalización, que le ha permitido a este órgano regulador lograr una mayor protección de los datos personales en posesión de las autoridades públicas.

En su artículo Miguel Pulido, Director Ejecutivo de Fundar, Centro de Análisis e Investigación, presenta una clara distinción de las características del derecho de acceso a la Información y del derecho a la protección de los datos personales, así como las áreas de coincidencia y se precisan las relaciones recíprocas en términos de alcances y límites, a partir de ejemplos concretos del ámbito federal y del Distrito Federal.

Miguel Pulido concluye que estos dos derechos comparten, entre otras cosas, identidad de actores, fuentes normativas y órganos garantes. No obstante, se trata de dos derechos provenientes de tradiciones jurídicas diversas, con implicaciones prácticas distintas y con posibilidades de colisión muy amplias. Para la solución de los casos de enfrentamiento entre derechos, el autor considera necesario realizar un ejercicio de ponderación de derechos dentro del marco normativo que permita divulgar ciertos datos personales, sin causar lesiones jurídicas que las personas no deban soportar y siempre que existan razones de interés público.

En el artículo que elaboré, se presenta un estudio comparativo de las legislaciones existentes en México, tanto en el ámbito local como el federal, en el que se muestra la heterogeneidad normativa existente en la actualidad; pues mientras algunas entidades federativas cuentan con leyes especiales en materia de protección de datos personales, otros estados regulan este derecho constitucional a través de las leyes de transparencia y acceso a la información, lo cual genera una regulación incompleta e inadecuada en la mayoría de los casos. Al regular el derecho a la protección de datos personales a través de leyes de transparencia se le concibe como una limitante al derecho de acceso a la información y no como un derecho autónomo e independiente, con reglas propias y diferentes. Por ello, aludo a la relevancia de impulsar la creación de leyes especializadas en la protección de datos personales en cada entidad federativa, con el fin de proteger, de manera eficiente, la privacidad de sus gobernados. Asimismo, en mi artículo se presenta un análisis de los resultados obtenidos en el Distrito Federal al implementar la Ley de Protección de Datos Personales para el Distrito Federal.

El Mtro. Gustavo Parra Noriega, Diputado del Estado de México, señala que el derecho de acceso a la información pública y el de protección de datos personales, son dos derechos autónomos e independientes entre los cuales debe existir un sano equilibrio. Por ello, al ser dos

derechos independientes, regidos por principios y criterios diferentes resulta plenamente justificado que exista una legislación independiente y especial para la protección de los datos personales, el cual con las citadas reformas a los artículos 6º y 16 de nuestra Carta Magna, se perfila como un derecho fundamental. Por ello, presenta una propuesta de los elementos mínimos que deben ser incluidos en la elaboración de una Ley de Protección de Datos Personales en el ámbito estatal y explica las razones de la pertinencia de incluir estos aspectos.

En la misma línea de los dos autores anteriores, el Lic. Eugenio Monterrey Chepov, Comisionado Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios y el Mtro. Gregorio Castillo Porras, señalan que aunque el derecho de acceso a la información pública y el de protección de los datos personales tienen orígenes compartidos, es necesario realizar algunas distinciones importantes, para ello se discute la distinción o, por el contrario, la sinonimia entre privacidad e intimidad y analiza la relación entre estos derechos y la protección de los datos. Asimismo, los autores incluyen una revisión de los antecedentes del derecho a la protección de datos personales en México, América Latina y Europa. Agrega, que al ser dos derechos distintos, con sus propias dinámicas y naturaleza, es necesario emitir una ley especial en materia de protección de datos personales en los gobiernos estatales.

El artículo de la maestra Lina Ornelas aborda el tema de las medidas de seguridad que deben ser adoptadas para proteger la información que poseen las instituciones gubernamentales al ser el activo más valioso en sus actividades cotidianas. La autora destaca que aun cuando asegurar la confidencialidad, la integridad y la disponibilidad de la información es costoso, es más onerosa la pérdida de información ya sea que esta ocurra por causas internas, o bien, por la obtención de la misma por agentes externos (hackeo). Por ello la seguridad de la información debe ser vista no sólo como un tema tecnológico, sino como un elemento organizacional de amplio espectro.

La Mtra. Blanca Lilía, Presidenta de la Comisión Transparencia y Acceso a la Información Pública del Municipio de Puebla, apoyada en la idea de Norberto Bobbio (1986), de asumir a la democracia como el gobierno del poder público en público. Plantea que aún cuando la sociedad tiene derecho a saber y los medios tienen el derecho y la

obligación de informar todo aquello que revista importancia para la sociedad y sus integrantes, estos derechos y obligaciones se concretan al deber de informar sin afectar los derechos de las personas.

La autora señala que con la finalidad de establecer un referente claro sobre los datos que pueden o no ser divulgados, el cual sirva de base en las redacciones y áreas de producción de noticias, resulta trascendental que las autoridades competentes y los institutos de transparencia y protección de datos impulsen en conjunto con los medios de comunicación y las áreas de comunicación social de los gobiernos, un modelo único relativo al tratamiento de los datos personales.

La Lic. Miroslava Carrillo Martínez, Comisionadada Ciudadana del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios aborda el tema de la protección de los datos personales de los menores en el uso de Internet. La autora señala que los menores de edad encarnan un sector social creciente respecto al uso de las redes sociales y las nuevas tecnologías, lo cual los ubica como un grupo vulnerado o potencialmente vulnerable, en sus derechos humanos y en sus garantías individuales, pues en la actualidad, los integrantes de este segmento social tienen acceso libre y directo a las TIC; además, por el simple hecho de navegar en Internet, deben proporcionar los datos personales que les requieren los sistemas de interacción.

Considerando los retos que implica el avance tecnológico, como el concepto de la nueva comunidad digital –especialmente, en el caso de los menores de edad y en la protección de sus datos personales–, las estrategias establecidas en las políticas públicas no deben limitarse a fortalecer el ámbito legal, se requiere el trabajo conjunto de las instituciones académicas y educativas, organizaciones no gubernamentales, órganos garantes, padres de familia y autoridades.

El doctor German Fajardo Dolci, Presidente de la Comisión Nacional de Arbitraje Médico, aborda el problema del tratamiento inequitativo que reciben los usuarios de los servicios médicos privados en relación a los que acuden al sector público pues, mientras los prestadores de servicios médicos privados atienden las peticiones de sus pacientes en términos de las disposiciones sanitarias, principalmente la "Norma Oficial Mexicana 168. Del Expediente Clínico", y dan acceso únicamente a un resumen clínico, los que reciben atención médica

en los hospitales públicos pueden acceder a una copia íntegra del expediente clínico. Con lo cual, a criterio del autor se ha propiciado un régimen diferenciado, y de alguna manera discriminatorio, en el tratamiento de los datos clínicos, con un efecto desigual en lo que respecta a los derechos del paciente, que por atenderse en el sector público adquirió un mayor derecho en comparación al que lo hizo en el servicio privado.

El Presidente de la Comisión Nacional de Arbitraje Médico, concluye que la protección efectiva de los datos personales en el sector salud puede conducir a mejorar los procedimientos médicos; evitar un uso discriminatorio o lesivo de la intimidad; brindar información falsa, inexacta o desactualizada en perjuicio de los pacientes; establecer estándares que coadyuven a la investigación en la ciencia médica, así como a integrar de una mejor manera la historia clínica y su interoperabilidad por las instituciones del sector salud.

En el artículo realizado por el Lic. Jorge Bustillo Roqueñí, Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, se efectúa un esbozo de la naturaleza y relevancia que tiene la información que se procesa en el espacio electoral y se estudian las características de los datos personales que recaban los organismos electorales en el ejercicio de sus funciones. Se presentan un par de casos en los que se refleja precariedad e insuficiencias en los esquemas de gestión y administración de los datos bajo resguardo de un organismo electoral, como son el problema de la venta de los padrones de electores y la existencia de registros duplicados de empadronados.

Por otra parte, el Comisionado Bustillos, estudia dos casos prácticos de tensión entre el derecho a la información y la protección de datos personales, brinda elementos argumentativos para divulgar determinados datos contenidos en el padrón de militantes de los partidos políticos y el nombre de quienes realizan aportaciones a los partidos políticos. La protección de los datos personales en los programas sociales es abordada en el texto de Alejandro López Mercado, Rocío Aguilar Solache y Pablo Yanes Rizo, en el que se realiza un repaso de las implicaciones que supone la protección de datos personales de los beneficiarios de los programas sociales, y las contradicciones que surgen con el derecho de acceso a la información pública. Para ello

se hace una revisión de la normatividad aplicable en esas materias y un somero análisis de su correlación y la problemática que enfrentan las instituciones públicas en la construcción de los padrones de los programas sociales, y se da cuenta de los retos y rezagos que todavía existen en este rubro, así como de los desafíos y ventajas que supone la conformación de un Sistema Único de Padrones de beneficiarios de Programas Sociales.

El Dr. Carlos G. Gregorio, investigador del Instituto de Investigación para la Justicia, presenta un análisis del cambio que representa la publicación de información judicial con la irrupción de Internet, creando múltiples lagunas axiológicas, nuevos riesgos y nuevas posibilidades de progreso. Para el autor, las diferencias entre la publicación en papel y la publicación en Internet son el foco de la discusión, como también el debate sobre si tiene relevancia o no al momento de ponderar los derechos, en particular la protección de los datos personales –sensibles– y la presunción de inocencia, entre otros.

Para el investigador del Instituto de Investigación para la Justicia, aún quedan muchas preguntas por resolver ¿Cuando se inicia un proceso judicial ceden las partes sus datos personales? ¿Cuando un poder judicial publica información en Internet, está cediendo datos para que puedan ser utilizados con cualquier otra finalidad? ¿Es la publicación en Internet una cesión indiscriminada?

En su artículo, la Lic. Areli Cano Guadiana, Comisionada Ciudadana del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, analiza el estado que guardan la procuración e impartición de justicia con respecto a la protección de datos personales, y se analiza el tratamiento y gestión de los datos personales desde la experiencia del órgano garante del Distrito Federal, de tal forma que en la última parte, se esbozan algunos elementos para la reflexión en torno al sistema judicial y la protección de datos personales frente a la construcción de una sociedad de derechos.

La Comisionada Cano, muestra la imperiosa necesidad de contar con diagnósticos integrales que consideren dimensiones cuantitativas y cualitativas, y de cuyo análisis se desprenda un conocimiento efectivo y certero sobre el estado en que se encuentran la procuración e impartición de justicia. Asimismo, señala que vale la pena reflexionar

sobre la pertinencia de contar con un código de buenas prácticas en torno a la protección de datos personales, que fuese un referente común para todas las instancias, y que en materia de justicia, sea interpretado observando a la unidad del sistema jurídico, y atendiendo a la armonización para evitar antinomias.

En el trabajo del Dr. Miguel Ángel Mancera Espinosa, Procurador General de Justicia del Distrito Federal se abordan algunos dilemas conceptuales en torno a la transparencia y la protección de datos personales en la procuración e impartición de justicia en el Distrito Federal. Por tal motivo, se explican diversos conceptos y se analizan algunas tensiones particulares entre el derecho de acceso a la información pública y la protección de datos personales en el contexto de la procuración de justicia en el Distrito Federal.

En el tema de la protección de datos en la procuración de justicia, el Mtro. Darío Ramírez, Director de la Oficina para México y Centroamérica de ARTICLE XIX, presenta un análisis minucioso de las ventajas y desventajas de divulgar información relativa a las averiguaciones previas y contextualiza los supuestos en los que debe existir transparencia. Asimismo, evidencia y ejemplifica algunas consecuencias jurídicas de no permitir que los inculpados puedan acceder a los expedientes de las averiguaciones previas. Por otra parte, muestra una crítica a la decisión del InfoDF de resolver que la exhibición en medios de responsables de delitos graves se ajusta a los principios de licitud, consentimiento y confidencialidad.

El Dr. Salvador Guerrero Chiprés, Comisionado Ciudadano del InfoDF, muestra en su artículo, a partir de la presentación de casos específicos, las tensiones conceptuales y prácticas inherentes al derecho de acceso a la información pública y al de la protección datos personales. Para lo cual se inicia con el debate sobre las contradicciones normativas y teóricas que supone el ejercicio de los derechos.

En su artículo el Comisionado Guerrero, estudia dos casos que presentan como el InfoDF decidió proteger el derecho a la autodeterminación informativa de los particulares. En el primero de ellos, se resolvió sobre la procedencia de cancelar el nombre de la demandante del boletín laboral electrónico publicado por la Junta Local de Conciliación y Arbitraje del Distrito Federal. Mientras que en

el segundo, se determinó que la Procuraduría General de Justicia del Distrito Federal realizó un tratamiento ilícito de datos al divulgar el domicilio particular de dos presuntos responsables de un delito.

Con la lectura de los diferentes trabajos que integran esta obra es posible tener un claro panorama del estado actual que guarda el derecho a la protección de los datos personales en el mundo y en México. Además es posible encontrar una diversidad de puntos de vista sobre cómo ponderar derechos al aplicar las normas de protección de datos personales y de acceso a la información pública de manera armónica.

Mtro. Oscar M. Guerra Ford
Comisionado Ciudadano Presidente del InfoDF

Reconocimiento normativo del Derecho a la Protección de los Datos Personales en el ámbito internacional

Agustín Millán Gómez

Agustín Millán Gómez

Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, cuenta con más de 30 años de experiencia laboral en el sector público, iniciando en la Secretaría de Turismo del Gobierno Federal; posteriormente, en el INEGI desempeña su labor en distintas posiciones administrativas como Jefe de Departamento, Subdirector, Director de Área, Asesor del Presidente del INEGI, Director Regional, Titular de la Unidad de Enlace en materia de Transparencia y Director General de Difusión. Más tarde funge como Coordinador General de Transparencia del Gobierno del estado de México; y Director General de Relaciones Públicas y Gestión Empresarial del Gobierno del estado de Aguascalientes.

Obtuvo su licenciatura en Economía en la Universidad Autónoma Metropolitana y realizó estudios de Maestría en Administración Pública en el Instituto Nacional de Administración Pública (INAP). Además, cuenta con un Diplomado en Alta Dirección de Entidades Públicas por el INAP y múltiples cursos y seminarios en áreas de administración, economía, transparencia gubernamental, archivos públicos, datos personales y calidad total, entre otros.

Es miembro de la Asociación de Economistas Egresados de la UAM, de la Asociación de Egresados del INAP, del Colegio Nacional de Economistas, es Evaluador Senior del Premio Nacional de Calidad y Coordinador de la Comisión de Comunicación Social de la Conferencia Mexicana de Acceso a la Información Pública.

Introducción

En una gran cantidad de países, las tecnologías de la información y los medios de comunicación han observado vertiginosos avances durante los últimos 10 años. Herramientas eficaces en la transmisión y difusión de todo tipo de información son utilizadas actualmente. No sorprende el hecho de que los flujos de datos involucren grandes volúmenes de información de carácter personal, ya sea entre entidades privadas y públicas, en entornos de corte doméstico e internacional. Ante estos acontecimientos, resulta de gran relevancia realizar una exploración del avance que presenta el marco normativo que regula al derecho a la protección de los datos personales a nivel internacional.

Para ello, haremos una breve referencia a la evolución emergente de los derechos humanos, a saber: primera generación (o reconocimiento de los derechos individuales); segunda generación (o reconocimiento de los derechos económico-sociales); tercera generación (o reconocimiento de derechos en grupos sociales); y cuarta generación (reconocimiento de los derechos de la sociedad digital, ligado al avance de las Tecnologías de Información y Comunicación, con la finalidad de posicionar el origen y relevancia de la protección de los datos personales en el mundo globalizado contemporáneo.

Posteriormente se hará una breve exploración de las legislaciones supranacionales, emitidas con la finalidad de proteger y auspiciar el desarrollo de derechos humanos y libertades fundamentales, para asegurar la garantía colectiva de los derechos enunciados en la Declaración Universal. Además, en un entorno de transacciones y transferencias digitales de información, y atendiendo sus compromisos internacionales, veremos que los países europeos fueron los primeros en adoptar leyes en materia de protección de datos.

Finalmente se revisará el avance en el reconocimiento que los países han dado al tema a nivel constitucional y legal para regular la protección de los datos personales.

Antecedentes

Es un hecho irrefutable que la Revolución Francesa detonó el reconocimiento de los derechos humanos, con diversos enfoques en su clasificación. Entre éstos, destacan el historicista,[1] el de jerarquía,[2] y por generaciones. Por su uso común a escala mundial, el último será utilizado en este apartado (Bustamante, 2001).

De acuerdo a Bustamante (2001) los derechos civiles y políticos de primera generación derivaron de la expresión de libertad de los individuos, defendiéndolos frente al poder del Estado. Éstos se encuentran recogidos en la Declaración Universal de los Derechos Humanos (1948), y en los Pactos Internacionales de los Derechos Civiles y Políticos, así como de los Derechos Económicos, Sociales y Culturales, ambos de 1966.

Los derechos de segunda generación surgieron a consecuencia de las tradiciones de pensamiento humanista y socialista. Son de naturaleza económica y social, e inciden sobre la expresión de igualdad de los individuos. A diferencia de los anteriores, con ellos se exige cierta intervención del Estado, para garantizar el acceso a derechos cuya pretensión es compensar desigualdades naturales, creadas por las ventajas y desventajas de las clases, las etnias y las religiones, que motivan diferencias sociales entre los individuos desde su nacimiento.

Ante el reconocimiento de nuevas necesidades, que obligan a desarrollar nuevos haberes que garanticen el acceso universal a formas más avanzadas de ciudadanía y civilidad, de libertad y de calidad de vida, la tercera generación está constituida por los derechos de la solidaridad. Aparecen en la segunda mitad del Siglo XX, por la acción de determinados colectivos que reclaman derechos legítimos para ciertos grupos de edad, minorías étnicas o religiosas, países del Tercer Mundo, a fin de evitar discriminaciones económicas y sociales. Durante las últimas décadas, estos derechos abren camino al gran reto del Siglo XXI: las nuevas formas que, en el entorno del ciberespacio, cobran estos

[1] El enfoque historicista, parte de la protección progresiva de los derechos.

[2] Enfoque basado en la jerarquía, distingue entre los Derechos Esenciales y los Derechos complementarios.

derechos generacionales. Para Ortega (2004) los derechos humanos de cuarta generación garantizan el nuevo estatus del individuo de la sociedad digital, en los que la universalización del acceso a las Tecnologías de Información y Comunicación, la libertad de expresión en la red, la libre distribución de la información y el conocimiento, juegan un papel determinante. En especial, los derechos que protegen la vida privada y procuran la igualdad en las condiciones de acceso a las nuevas tecnologías, así como la utilización de las telecomunicaciones, soporte del ejercicio de los derechos de libertad de expresión e información.

Estos derechos de cuarta generación buscan garantizar la integración de los sistemas de comunicación y los medios de comunicación social, evitar la concentración de medios y el control de la información en Internet, así como procurar la garantía del pluralismo. No escapa al conjunto el derecho a la autodeterminación informativa que, en consideración de Ortega (2004) pertenece al contexto de la era informática.

Normatividad supranacional que regula el derecho a la protección de datos personales

Entre los instrumentos internacionales que refieren el reconocimiento del derecho a la protección de los datos de las personas, encontramos los siguientes:

La Declaración Universal de los Derechos del Hombre (1948), en cuyo artículo 12 se establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, domicilio o correspondencia, ni de ataques a su honra o reputación y a ser protegido legalmente contra tales injerencias.

El artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales (1950), reconoce el derecho de la persona al respeto de su vida privada y familiar, su domicilio y su correspondencia.

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966) y el artículo 11 de la Convención Americana sobre Derechos Humanos (1969), señalan que 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.

La Resolución 509 de la Asamblea del Consejo de Europa (1968), sobre los derechos humanos y nuevos logros científicos y técnicos, emitida, entre otras razones, "con la pretensión de reforzar… la protección jurídica de los individuos con relación al tratamiento automatizado de datos de carácter personal que les conciernen".[3]

La Resolución 509 detonó diversas leyes en países europeos. El primer Estado soberano que dispuso Leyes de Protección de Datos fue Suecia, promulgando la suya en 1973.[4] También repercutió en el "Land Hessen" alemán, con su ley de 1970, y la Ley de Protección de Datos de la República Federal Alemana de 1977. También se debe considerar la Ley de Informática, Ficheros y Libertades de Francia, las Leyes sobre Ficheros Públicos y Privados de Dinamarca; la Ley de Protección de Datos de Austria —todas de 1978—, y la Ley sobre utilización de datos en tratamientos informáticos de Luxemburgo, de 1979.[5] Otro antecedente es la Fair Credit Reporting Act (1970) de los Estados Unidos de Norteamérica, Ley en que, si bien no hace mención a archivos automatizados, sí constituye una primera regulación del tratamiento genérico de los datos personales del individuo y dio origen a la Privacy Act del 31 de diciembre de 1974.

Directrices de la Organización para la Cooperación y el Desarrollo Económico

El primer instrumento supranacional que analiza el derecho a la protección de datos personales, en adelante PDP, son las Directrices de la Organización para la Cooperación y el Desarrollo Económico

[3] Tomado de Lucrecio Rebollo Delgado, "Vida privada y protección de datos: un acerca miento a la regulación internacional europea y española" p. 906. Consultable en http://www.bibliojuridica.org/libros/6/2758/10.pdf.

[4] Tomado de Alejandra Castro Bonilla, "La Protección del Derecho a la Intimidad en el Tratamiento de Datos Personales: El caso de España y la nueva legislación Latinoamericana."p. 101 Consultable en: http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/57/pr/pr33.pdf.

[5] Lina Ornelas Nuñez y Sergio López Ayllón, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", p. 59.

(OCDE, 1980), relativas a la protección de la intimidad y la circulación transfronteriza de datos personales, que contienen los tres principios aplicables a sus países miembro: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas.

Los principios que rigen a las Directrices de la OCDE, cuya aplicación puede ser nacional e internacional, abarcan todos los medios de procesamiento informático de datos sobre individuos —desde computadoras locales hasta redes con complejas ramificaciones nacionales e internacionales—, todos los tipos de procesamiento —desde la administración de personal hasta la compilación de perfiles de consumidores— y todas las categorías de datos —desde los de tráfico común hasta los de contenidos, triviales o delicados.

Estas Directrices se han utilizado a lo largo de los años en un gran número de instrumentos de regulación nacional, o de autorregulación, y todavía se usan ampliamente en los sectores público y privado.[6]

Las Directrices se estructuran en cinco apartados: a) Generalidades; b) Principios básicos de aplicación nacional; c) Principios básicos de aplicación internacional: restricciones en el libre flujo y la legitimidad; d) Implantación nacional; y Cooperación internacional. Los principios básicos de aplicación internacional inciden sobre las restricciones en el libre flujo y la legitimidad, pues establecen que los países miembro deben considerar las implicaciones que el procesamiento nacional y la reexportación de datos personales puedan tener para otros países, así como tomar pasos razonables y apropiados para asegurar que su flujo transfronterizo, incluido el tránsito a través de un país miembro, se realice de forma ininterrumpida y segura.

Asimismo, impone una restricción para el intercambio transfronterizo de los datos, cuando el país receptor todavía no observe de forma sustancial las Directrices, o cuando la reexportación de los datos burle la legislación nacional sobre privacidad. Estas Directrices también permiten que cada país miembro pueda establecer restricciones a ciertas categorías de datos personales regidas por normativas específicas, contenidas en su legislación nacional sobre privacidad,

[6] Disponible al 15 de noviembre de 2011 en http://www.oecd.org/dataoecd/16/51/15590267.pdf.

y que por su naturaleza no tienen una protección equiparable en el país receptor, con la limitante a la elaboración de leyes, políticas y prácticas que pudieran crear obstáculos al flujo transfronterizo de datos personales, excediendo los requisitos para tal protección.

Para Lina Ornelas (2010), estas Directrices se emitieron a partir del reconocimiento de tres problemáticas centrales:

1. El uso de tecnologías para tratar datos personales pueden ponerlos a disposición de miles de usuarios, en lugares geográficamente dispersos, dando lugar a la creación de redes complejas de datos.

2. El peligro que representan las disparidades en las legislaciones nacionales, tendientes a conciliar la protección de información personal con la transmisión de enormes cantidades de datos, a través de las fronteras nacionales.

3. La diversidad en las legislaciones nacionales, que trae como consecuencia restricciones y obstáculos a la libre circulación transfronteriza de datos personales, ocasionando graves trastornos en importantes sectores de la economía.

Convenio 108

Ahora bien, a consecuencia del trabajo desarrollado en el Consejo Europeo por el aumento de la circulación transfronteriza de datos, el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, se constituye como el primer instrumento regional que regula el tema de PDP, ante el tratamiento automatizado de los mismos. La finalidad y objeto del Convenio es garantizar a cualquier persona física, el respeto de sus derechos y libertades fundamentales —en concreto, su derecho a la vida privada— en el territorio de cada parte, sean cuales fueren su nacionalidad o su residencia, con respecto al tratamiento automatizado de sus datos.

Asimismo, los Estados firmantes tienen la obligación de adoptar en su régimen interno, medidas para hacer efectivos los principios que rigen a la protección de datos, en los términos siguientes: respecto al

principio de calidad, señala expresamente que los datos personales sometidos a tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; serán adecuados, pertinentes y no excesivos en relación con la finalidad que motivó su registro; serán exactos y puestos al día en casos necesarios; se conservarán de modo que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades que motivaron su registro.

En cuanto a las medidas de protección, señala que se deberán adoptar medidas de seguridad apropiadas en los ficheros automatizados, contra la destrucción accidental o no autorizada, la pérdida accidental, y el acceso, modificación o difusión no autorizados. También impone restricciones al tratamiento automatizado de datos relativos al origen racial, opiniones políticas, convicciones religiosas o de otro tipo, así como los datos relativos a la salud o a la vida sexual. En estos casos, los datos no podrán tratarse en forma automática, a menos que el derecho interno prevea garantías apropiadas.

El Convenio 108 fue reforzado con principios rectores para la reglamentación de ficheros computarizados de datos personales, adoptados mediante la Resolución 45/95[7] de las Naciones Unidas en diciembre de 1990.

A diferencia del Convenio, la Resolución centra su normativa en los sistemas de datos personales en posesión de instituciones gubernamentales. En su preámbulo indica que los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado. Los principios consagrados en la Resolución 45/95 son los siguientes:

1. *Licitud y lealtad*: Las informaciones sobre las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

[7] Consultable en http://www.paxsocial.com.ar/resol.45-95.htm.

2. *Exactitud*: Las personas encargadas de la creación de un fichero, o de su funcionamiento, deberán verificar la exactitud y pertinencia de los datos registrados; evitar errores por omisión; actualizarlos periódicamente, o cuando se utilicen las informaciones contenidas en un expediente.

3. *Finalidad*: La finalidad de un fichero y su utilización deberán especificarse y justificarse, así como ser objeto de conocimiento de la persona interesada, a fin de asegurar que: a) los datos personales recogidos son pertinentes a la finalidad perseguida; b) ningún dato es utilizado o revelado sin consentimiento del interesado, o con un propósito incompatible con el especificado; c) el período de conservación de los datos no excede el necesario para alcanzar la finalidad con que se han registrado.

4. *Acceso de la persona interesada*: Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne; a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos; a obtener rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando su información sea comunicada, a conocer los destinatarios. Las disposiciones de este principio son aplicables a todas las personas, al margen de su nacionalidad o residencia.

5. *No discriminación*: A reserva de las excepciones previstas en el principio 6, no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, la participación en una asociación, o la afiliación a un sindicato.

6. *Facultad de establecer excepciones*: Sólo pueden autorizarse excepciones a los principios 1 a 4, si son necesarias para proteger la seguridad nacional, el orden público, la salud o moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas, con la reserva de que las excepciones estén expresamente previstas por la ley, o una reglamentación equivalente, adoptada conforme al sistema jurídico nacional, en el que se definan los límites y establezcan las garantías apropiadas.

Las excepciones al principio 5 deberían estar sujetas a las mismas garantías previstas para las excepciones a los principios 1 a 4. Sólo podrían autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de estos derechos y de lucha contra la discriminación.

7. *Seguridad*: Se deberían adoptar medidas apropiadas para proteger los ficheros contra los riesgos naturales, como pérdida accidental o destrucción por siniestro, y contra riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

Directiva 95/46/CE

Ahora bien, con la Directiva 95/46/CE de 24 de octubre de 1995, "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", se pretendió establecer un piso mínimo en la Unión Europea para proteger a las personas por vía de sus datos personales, sin descuidar su libre flujo transfronterizo. Sus principios rectores señalan que los Estados miembro dispondrán que los datos personales sean tratados de manera leal y lícita; recogidos con fines determinados, explícitos y legítimos; no ser objeto de tratamiento incompatible con dichos fines (no se considera incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembro establezcan las garantías oportunas); deben ser adecuados, pertinentes y no excesivos con relación a los fines por los que se recaban y tratan; ser exactos y, cuando sea necesario, actualizados; deberán tomarse medidas razonables para que los datos inexactos o incompletos, sean suprimidos o rectificados; y conservados de forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos.

La Directiva también indica que los Estados miembro establecerán garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. Para ello, señala que el responsable del tratamiento garantizará el cumplimiento de estos elementos, so pena que el

tratamiento sea considerado ilícito. No se puede perder de vista que el responsable tiene el compromiso de cumplir lo señalado por la Directiva, y lo dispuesto en la Ley aplicable en el Estado.

En forma independiente, se establece que el tratamiento de los datos personales debe cumplir con el principio de legitimidad, para el cual es necesario que exista el consentimiento previo e inequívoco del titular, o bien sea necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales adoptadas a petición del interesado.

En otros casos el principio de legitimidad también se cumple cuando el tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; para la protección del interés vital del titular; para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección. Ligado a estos principios tenemos al de confidencialidad, en el que sólo el responsable o el encargado del tratamiento podrán tratar los datos a que legítimamente tengan acceso.

Asimismo, el principio de seguridad entraña la obligación para el responsable del tratamiento de aplicar medidas técnicas y de organización adecuadas para la PDP, contra la destrucción o pérdida accidental o ilícita de los datos, y contra la alteración, difusión o acceso no autorizados, en particular cuando el tratamiento incluya su transmisión dentro de una red, y contra cualquier otro tratamiento ilícito.

Recientemente, el Grupo de Trabajo Artículo 29[8] ha buscado

[8] El Grupo de trabajo del artículo 29 está compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea.
Sus funciones, la localizamos en el artículo 30 de la Directiva, que señala:
"a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;
b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de

incorporar a dicha Directiva el principio de responsabilidad, el cual, implica "… que los responsables del tratamiento de datos garanticen la adopción de medidas eficaces que aporten una auténtica protección de datos…".[9]

Es de resaltar que este principio no es nuevo en el ámbito del derecho a la PDP. La OCDE lo incorporó en las directrices sobre privacidad adoptadas en 1980, señalando que "… todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios expuestos".[10]

Directiva 97/66/CE

Otro instrumento de la Unión Europea marcó un hito en el derecho a la PDP. La Directiva 97/66/CE del Parlamento Europeo y del Consejo, "relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones",[11] instrumento que complementa a la Directiva 95/46/CE, y tiene por objeto armonizar las disposiciones de los Estados miembro, necesarias para garantizar un nivel equivalente de protección de las libertades y derechos fundamentales, en particular el derecho a la intimidad en el tratamiento de los datos en el sector de las telecomunicaciones, así como su libre circulación.

Es importante resaltar la confidencialidad de las comunicaciones

---

la Comunidad y en los países terceros;
c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria".

[9] Tomado del Dictamen 3/2010 sobre el principio de responsabilidad. Adoptado el 13 de julio de 2010.

[10] Tomado del Dictamen 3/2010 sobre el principio de responsabilidad. Adoptado el 13 de julio de 2010, Numeral 16.

[11] Esta Directiva estuvo vigente hasta el 12 de julio de 2002, fue derogada por la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las (comunicaciones electrónicas).

realizadas a través de redes y servicios públicos de telecomunicación,[12] cuya garantía estará avalada por Estados miembro mediante normas nacionales. La excepción a este punto la constituyen las grabaciones legalmente autorizadas.

Asimismo, esta Directiva incorporó el principio de temporalidad, al señalar que los datos sobre tráfico y comunicaciones relacionados con usuarios y abonados, almacenados por el proveedor de una red o servicio público de telecomunicación, deberán destruirse o hacerse anónimos en cuanto termine la comunicación.

Respecto de la facturación a usuarios y los pagos de las interconexiones, los datos podrán ser tratados únicamente hasta la expiración del plazo en el cual pueda impugnarse legalmente la factura, o exigirse el pago.

Directiva 2002/58/CE

La Directiva 97/66/CE fue derogada por la Directiva 2002/58/CE, que versa sobre la privacidad y las comunicaciones electrónicas, garantizando el tratamiento de datos personales y la protección de la privacidad en este tipo de comunicaciones[13]. En su preámbulo, señala que los avances tecnológicos vividos desde la publicación de la Directiva 97/66/CE hacen necesaria su actualización, a fin de responder las necesidades imperantes.

Asimismo, busca proteger no solamente el derecho a la intimidad, sino también intereses legítimos de personas morales, en virtud de que los datos tratados en redes de comunicación electrónicas contienen información relativa a la vida privada de una persona física, identificada o identificable, y asimismo afectan de una u otra

[12] Artículo 5.1. Directiva 97/66/CE.

[13] El artículo 19 de la Directiva 2002/58/CE, señala al respecto:
Se deroga la Directiva 97/66/CE con efecto a partir de la fecha contemplada en el apartado 1 del artículo 17. "Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva". El apartado 1 del artículo 17, señala: "Los Estados miembros pondrán en vigor antes del 31 de octubre de 2003 las disposiciones necesarias para dar cumplimiento a lo establecido en la presente Directiva…"

forma los intereses de una persona moral.[14] Por lo anterior, señala la Directiva, el tratamiento de los datos debe mantenerse en tanto dure el servicio prestado, incluyendo el período de facturación y demás pagos conexos, por lo que otro tipo de procesamiento deberá contar con el consentimiento expreso e informado del interesado.

Un apartado importante sobre los sistemas de geolocalización es desarrollado en la Directiva, al señalar en el considerando 35 que en las redes móviles digitales se tratan datos sobre localización que proporcionan la posición geográfica del equipo terminal del usuario móvil, para hacer posible la transmisión de las comunicaciones, además de que las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario, utilizados para la prestación de servicios de valor añadido, tales como servicios de información sobre tráfico y orientaciones individualizadas a los conductores. De esta manera, la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Aún en los casos en que hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización.

Al igual que la Directiva 97/66/CE, éste instrumento contempla límites al derecho a la PDP o los intereses legítimos de las personas morales, estableciendo que los Estados miembro podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones, cuando tal limitación constituya una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución del delito o la utilización no autorizada del sistema de comunicaciones electrónicas a que hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE.[15] También indica que todas las medidas contenidas en el

[14] Tomado del Considerando 26, Directiva 2002/58/CE

[15] Artículo 13 Excepciones y limitaciones
1. "Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa;"
c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea,

presente apartado deberán ser conformes con los principios generales del Derecho comunitario.

El desarrollo normativo e interpretativo del derecho a la intimidad y la PDP no sólo ha tenido lugar en la Unión Europea. En el año 1999, en el seno del Foro de Cooperación Economía Asia Pacífico (APEC), fue establecido un Grupo de Manejo del Comercio Electrónico, con el objeto de desarrollar legislaciones y políticas en materia de privacidad, compatibles para los países partícipes. El resultado de estos trabajos es la emisión de lineamientos generales a ser incorporados en los cuerpos legales para el logro de un flujo seguro de datos, en una perspectiva que evite generar obstáculos en el fomento al comercio para fomentar el comercio entre los países integrantes.

Declaración de Madrid

En otro escenario, derivado de los trabajos de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[16] celebrada el 5 de noviembre de 2009, se emitió la Declaración de Madrid,[17] que recoge la propuesta conjunta para la redacción de estándares internacionales encaminados a la protección de la privacidad, en relación con el tratamiento de datos personales. Al margen de su intención armonizadora en la emisión de instrumentos normativos, es de resaltar la colaboración y adhesión consensuada de más de 50 países, que agrega un valor importante, puesto que se enfatiza la vocación universal de los principios y garantías que configuran

incluidos los asuntos monetarios, presupuestarios y fiscales; "f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); "g) la protección del interesado o de los derechos y libertades de otras personas.

[16] La 30ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad adoptó en Estrasburgo unánimemente la Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales. La resolución estableció el mandato de crear un Grupo de Trabajo, bajo coordinación de la Agencia Española de Protección de Datos, como Autoridad organizadora de la 31ª Conferencia Internacional y con la participación de las Autoridades de protección de datos interesadas en ello, con el objetivo de elaborar una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal.

[17] Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.

el derecho a la PDP, y reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante. La Declaración tiene como objeto definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos personales, así como facilitar los flujos internacionales que de ellos se haga, necesarios en un mundo globalizado. La Declaración se compone de 6 partes: a) Disposiciones generales; b) Principios básicos; c) Legitimación para el tratamiento; d) Derechos del interesado; e) Seguridad; y f) Cumplimiento y supervisión.

Memorándum de Montevideo

Asimismo, derivado de los trabajos del "Seminario Derechos, Adolescentes y Redes Sociales en Internet" realizado en Montevideo, Uruguay los días 27 y 28 de julio de 2009, se elaboró el Memorándum sobre la PDP y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes (también conocido como Memorándum de Montevideo),[18] el cual reconoce la importancia de la Internet como un medio de comunicación al que los menores de edad acceden cada vez con mayor facilidad, si bien con amplios beneficios para la educación y como medio que permite acceder a información para ampliar conocimientos y tener contacto con personas de todo el mundo, también se reconocen los peligros a los que los niños, niñas y adolescentes se exponen, justamente por esta nueva dinámica de la Sociedad de Información, donde el intercambio de información y el contacto con otras personas son los motores para que exista la preocupación gubernamental, en América Latina y el Caribe, para establecer normativamente un equilibrio entre su uso y la promoción y fortalecimiento de la PDP, específicamente en este sector vulnerable de la sociedad. Este documento se compone de 32 numerales que contienen, groso modo, las siguientes recomendaciones:

- Recomendaciones para los Estados y entidades educativas.
- Para la prevención y educación de niñas, niños y adolescentes.
- Recomendaciones para los Estados sobre el marco legal.
- Recomendaciones para la aplicación de las leyes por parte de los Estados.

[18] Disponible al 15 de noviembre en http://memorandumdemontevideo.ifai.org.mx/.

- Recomendaciones en materia de políticas públicas.
- Recomendaciones para la industria.

En el apartado de las consideraciones finales, se exhorta a los países involucrados a buscar un diálogo constante en esta materia y, de manera especial, se apela al cumplimento de las obligaciones de los Estados y a la responsabilidad social empresarial para encontrar las mejores formas de implementarlo.

Reconocimiento normativo en las leyes nacionales

La normativa supranacional se ha constituido como un referente importante para múltiples naciones, los países miembro de las organizaciones emisoras de los ordenamientos citados han adoptado leyes reglamentarias en su derecho interno, tomando como base los principios establecidos en los mismos, para lograr la protección de los datos personales y, en algunas legislaciones, el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos personales. Sin embargo, el reconocimiento normativo de estos importantes derechos ha ido más allá de las naciones europeas. Actualmente existen 77 países que cuentan con una legislación reglamentaria en materia de PDP —sin que sea nuestra intención entrar al análisis de cada una de ellas — este dato se constituye en un referente respecto del impacto que a nivel internacional conlleva que cada uno de los Estados cuenten con una normativa interna, adoptando los principios internacionales dictados a proteger los datos de carácter personal, tanto en poder del propio Estado como en posesión de particulares.

Cuadro 1. Países con Leyes reglamentarias y referencia constitucional. (Continuación)

País	Nombre de la Ley	Año de promulgación	Reconocimiento Constitucional	Artículo
70. España	Ley Orgánica de Protección de Datos de Carácter Personal	**1992**	**Si**	**18**
71. Suecia	Ley de Datos Personales	**1973**	**Si**	**3**
72. Suiza	Ley de Protección de Datos	**1992**	**Si**	**13**
73. Taiwan	Ley de Protección de Datos Personales	**1995**	**Si**	**12**
74. Túnez	Ley de Protección de Datos Personales	**2011**	**Si**	**9**
75. Ucrania	Ley sobre la Protección de Datos Personales	**2011**	**Si**	**32**
76. Reino Unido	Ley de Protección de Datos 1998	**1984**	**Si**	**16**
77. Uruguay	Ley de Protección de Datos Personales	**2008**	**Si**	**10 y 28**

Fuente: Elaboración propia del autor, con base en lo señalado por Greenleaf (2011).

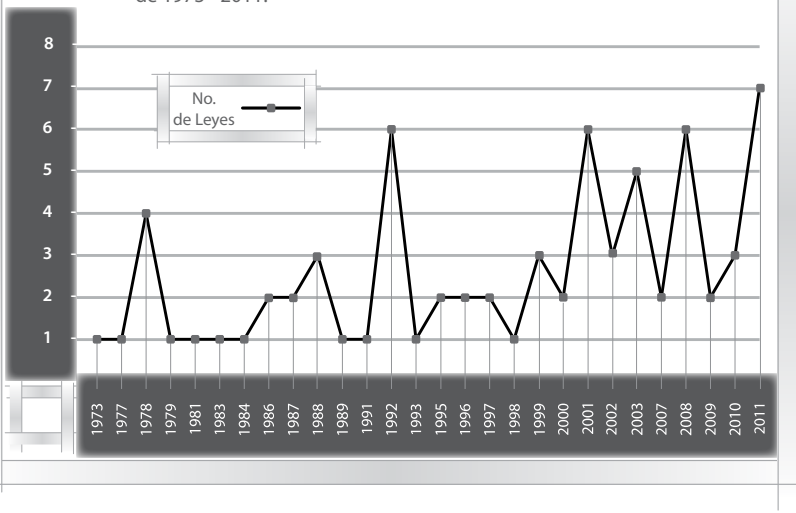
En este sentido, atentos al hecho de que la Organización de Naciones Unidas (ONU) se compone de 193 países miembro,[19] y que sólo 77 países cuentan con una norma reglamentaria en esta materia, hasta ahora sólo el 39.8% del total de países miembro ha adoptado regulaciones en materia de protección de datos personales.

Asimismo, en la figura 1, se observa que 45 de los 77 países forman parte de otras organizaciones internacionales que se han distinguido por impulsar marcos adecuados en la materia, como la APEC (Cooperación Económica Asia-Pacífico), con 9 países; 32 en la OCDE; 4 en la ECOWAS (Comunidad Económica de Estados de África Occidental). Los 32 países restantes no pertenecen a ningún organismo.

[19] Disponible al 15 de noviembre en http://www.un.org/es/members/growth.shtml#2000.

La aprobación de 77 leyes en otros tantos países ocurrió en el transcurso de 38 años, que corren a partir de 1973, y hasta la última ley emitida en 2011. Despuntes importantes son evidentes en los años 1992, 2001 y 2008, al promulgarse 6 leyes en cada uno de estos años y 7 en el 2011 (ver gráfica 1).

Gráfica 1. Comportamiento de la promulgación de leyes reglamentarias de 1973 - 2011.



Esta tendencia tuvo lugar al margen de que, en forma expresa, no exista un reconocimiento a nivel constitucional para que el Estado en cuestión proceda a la emisión de normas internas que regulen el derecho a la protección de datos personales. Así, en 23 países, existe una Ley reglamentaria aunque el derecho al a protección de datos personales no está reconocido expresamente en la constitución nacional, un claro ejemplo lo constituye Francia que tiene una Ley reglamentaria en materia de protección de datos personales, expedida en 1978, aunque no cuentan con un reconocimiento expreso a nivel constitucional pues en el preámbulo de su Constitución sólo se establece que el pueblo francés proclama solemnemente su adhesión a los derechos humanos.

Existen otros 54 países donde la emisión de una norma especial encuentra sustento en la constitución, como en México, donde la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la protección de los datos personales en los artículos 6 (Reformado el 20 de julio de 2007)[20] y 16 (Reformado el 1 de junio de 2009)[21] al señalar que: a) la información sobre la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; b) el derecho de toda persona al acceso gratuito de sus datos personales o a la rectificación de éstos, y c) 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, en la cual se establecerán los supuestos de excepción a los principios que rijan el tratamiento de datos.

Conclusión

En su evolución, el derecho a la PDP ha cobrado reconocimiento y relevancia internacional en los últimos años, a medida que han avanzado las tecnologías de la información y comunicación, así como la evolución de la sociedad en sociedades digitales.[22] La tendencia viene acompañada de la exigencia de los titulares de la información de que sus datos personales se encuentren protegidos de cualquier difusión, tratamiento u obtención no autorizados.

La adopción de instrumentos supranacionales y el avance en la expedición de leyes reglamentarias deberían estar íntimamente ligados, ello atendiendo a los compromisos adquiridos para la emisión de normas internas acordes a los principios reconocidos internacionalmente.

[20] Disponible al 15 de noviembre de 2011 en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_174_20jul07_ima.pdf.

[21] Disponible al 18 de noviembre de 2011 en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf.

[22] En estas sociedades existe un intercambio de información, ya sea pública o de particulares a nivel global y por lo tanto, subsiste un tratamiento de datos personales tanto de órganos de gobierno como de particulares.

Sin embargo, vemos que este avance ha sido lento, considerando que en 38 años sólo el 40% de países que forman parte de la ONU han emitido leyes en esta materia y aún, cuando en la última década se han adoptado 40 de las 76 leyes reglamentarias, es decir, un trabajo legislativo del 52%.

Nuestro país se encuentra dentro de los que incluyeron el reconocimiento de este derecho en la última década, al 2011 han transcurrido apenas 9 años desde que se emitió la primera ley específica en el estado de Colima en el 2003.

Es necesario que el trabajo legislativo a nivel internacional de los Estados e internamente en nuestro país, rindan frutos emitiendo leyes de protección de datos atendiendo a esta nueva era de la sociedad digital e intercambio masivo de información, para el debido establecimiento de estándares de seguridad para la protección de los datos que son objeto de transferencias, el reconocimiento del responsable del tratamiento, ya sea de carácter público o privado, así como de los procedimientos encaminados a la supervisión de la debida protección de los datos personales.

Cuadro 1. Países con Leyes reglamentarias y referencia constitucional.

País	Nombre de la Ley	Año de promulgación	Reconocimiento Constitucional	Artículo
1. Albania	Ley de Protección de Datos de Carácter Personal	1999	Si	35
2. Alemania	Ley Federal de Protección de Datos	1977	No	–
3. Andorra	Ley de Protección de Datos Personales	2003	Si	14
4. Angola	Ley de Protección de Datos	2011	Si	32
5. Argentina	Ley de Protección de Datos Personales	2000	Si	43
6. Australia	Ley de Privacidad	1988	No	–
7. Austria	Ley de Protección de Datos	1978	No	–
8. Azerbaiyán	Ley de Datos, Procesamiento de Datos y Protección de Datos	1998	Si	46
9. Bahamas	Ley de Protección de Datos	2003	Si	15
10. Bélgica	Ley de Protección de la Privacidad en relación con el Tratamiento de Datos Personales.	1992	Si	22
11. Benin	Ley de Protección de Datos Personales	2009	No	–
12. Bosnia y Herzegovina	Ley de Protección de Datos Personales	2001	Si	2
13. Bulgaria	Ley para la protección de Datos de Carácter Personal	2002	Si	32
14. Burkina Faso	Ley de Protección de Información Personal	2004	Si	6
15. Canadá	Ley de Protección de Información Personal y Documentos Electrónicos	2002	No	–
16. Cabo Verde	Ley de Protección de Datos *Ley N. 133N12001*	2001	No	–
17. Chile	Ley de Privacidad	1999	Si	19
18. Colombia	Ley de Protección de Datos	2008	Si	15
19. Costa Rica	Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales	2011	Si	24
20. Croacia	Ley de Protección de Datos Personales	2003	Si	35
21. Chipre	Ley del tratamiento de Datos Personales, Protección de las Personas	2001	Si	15
22. República Checa	Ley de Protección de Datos Personales	1992	No	–
23. Dinamarca	Ley sobre el tratamiento de Datos Personales	1978	No	–

Fuente: Elaboración propia del autor, con base en lo señalado por Greenleaf (2011).

Cuadro 1. Países con Leyes reglamentarias y referencia constitucional. (Continuación)

País	Nombre de la Ley	Año de promulgación	Reconocimiento Constitucional	Artículo
24. Estonia	Ley de Protección de Datos	2003	Si	6
25. Islas Feroe	Ley sobre tratamiento de Datos Personales	2010	No	–
26. Finlandia	Ley de Datos Personales	1987	Si	10
27. Francia	Ley relativa a la Protección de las Personas por el Tratamiento de Datos Personales	1978	No	–
28. Macedonia	Ley de Protección de Datos Personales	2005	Si	18
29. Gibraltar	Ley de Protección de Datos	2004	Si	1
30. Grecia	Ley sobre la protección de las personas con respecto al tratamiento de datos personales	1997	Si	9ª
31. Guernsey	Ley de Protección de Datos de la Bahía de Guernsey	1986	No	–
32. Hong Kong SAR	Ordenanza de Privacidad de los Datos Personales	1995	No	–
33. Hungría	Ley de protección de datos personales y la divulgación de la información pública	1992	Si	59
34. Islandia	Ley sobre la Protección y Tratamiento de Datos Personales	1989	Si	71
35. India	Normas con Arreglo a la Ley de Tecnología de Información	2011	No	–
36. Irlanda	Ley de Protección de Datos	1988	No	–
37. Isla de Man	Ley de Protección de Datos	1986	No	–
38. Israel	Ley de Protección a la Privacidad de 1981	1981	No	–
39. Italia	Consolidación de la Ley en materia de Protección de Datos Personales	1996	No	–
40. Japón	Ley sobre la Protección de Datos Personales	2003	No	–
41. Jersey	Ley de Protección de Datos de Jersey	1987	No	–
42. República de Kirguistán	Ley de Datos Personales	2008	Si	29
43. Letonia	Ley de protección de datos personales de personas físicas	2000	Si	96
44. Liechtenstein	Gesetz über die Abänderung des Datenschutzgesetzes	2002	No	–
45. Lituania	Ley sobre la Protección Legal de los Datos Personales	1996	Si	22
46. Luxemburgo	Ley de Protección de Datos	1979	Si	11

Fuente: Elaboración propia del autor, con base en lo señalado por Greenleaf (2011).

Cuadro 1. Países con Leyes reglamentarias y referencia constitucional. (Continuación)

País	Nombre de la Ley	Año de promulgación	Reconocimiento Constitucional	Artículo
47. Macao SAR	Ley de Protección de Datos Personales (Ley 8/2005)	2005	No	–
48. Malasia	Ley de Protección de Datos Personales	2010	No	–
49. Malta	Ley de Protección de Datos	2001	Si	32
50. República de Mauricio	Ley de Protección de Datos	2004	Si	3
51. México	Ley Federal de Protección de Datos Personales en Posesión de Particulares	2010	Si	6 y 16
52. República del Moldavia	Ley de Protección de Datos Personales	2007	Si	28
53. Mónaco	Ley de Control del Tratamiento de Datos Personales	2008	Si	22
54. Montenegro	Ley sobre Protección de Datos Personales	2008	Si	43
55. Marruecos	Ley de Protección de Datos	2009	Si	11
56. Países Bajos	Ley de Protección de Datos Personales	1988	Si	10
57. Nueva Zelanda	Ley de Privacidad 1993	1993	No	–
58. Noruega	Ley de Datos Personales	1978	Si	100
59. Perú	Ley de Protección de Datos Personales	2011	Si	2
60. Polonia	Ley sobre la Protección de Datos Personales	1997	Si	47 y 51
61. Portugal	Ley de Protección de Datos de Carácter Personal	1991	Si	35
62. Rumania	Ley sobre la Protección de las Personas con respecto al Tratamiento de Datos Personales y la Libre Circulación de estos Datos	2001	SI	26
63. Rusia	Ley Federal sobre Datos Personales	2011	Si	23 y 24
64. San Marino	Ley que regula la Recogida Sitemática de los Datos Personales	1983	Si	6
65. Senegal	Ley de Protección de Datos Personales	2007	Si	13
66. Serbia	Ley de protección de Datos Personales	2008	Si	42
67. Eslovaquia	Ley de Protección de Datos Personales	1992	Si	16 y 22
68. Eslovenia	Ley de Protección de Datos Personales	1999	Si	38
69. Corea del Sur	Ley de Protección de Datos	2001	Si	17

Fuente: Elaboración propia del autor, con base en lo señalado por Greenleaf (2011).

Cuadro 1. Países con Leyes reglamentarias y referencia constitucional. (Continuación)

País	Nombre de la Ley	Año de promulgación	Reconocimiento Constitucional	Artículo
70. España	Ley Orgánica de Protección de Datos de Carácter Personal	**1992**	**Si**	**18**
71. Suecia	Ley de Datos Personales	**1973**	**Si**	**3**
72. Suiza	Ley de Protección de Datos	**1992**	**Si**	**13**
73. Taiwan	Ley de Protección de Datos Personales	**1995**	**Si**	**12**
74. Túnez	Ley de Protección de Datos Personales	**2011**	**Si**	**9**
75. Ucrania	Ley sobre la Protección de Datos Personales	**2011**	**Si**	**32**
76. Reino Unido	Ley de Protección de Datos 1998	**1984**	**Si**	**16**
77. Uruguay	Ley de Protección de Datos Personales	**2008**	**Si**	**10 y 28**

Fuente: Elaboración propia del autor, con base en lo señalado por Greenleaf (2011).

Referencias

Bustamante Donas, Javier, (2001) *Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica*, Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Información, Número 1, Septiembre - Diciembre 2001. Disponible hasta el 15 noviembre de 2011 en http://www.oei.es/revistactsi/numero1/bustamante.htm.

Castro Bonilla, Alejandra, (2002) *La Protección del Derecho a la Intimidad en el Tratamiento de Datos Personales: El caso de España y la nueva legislación Latinoamericana*. Disponible hasta el 15 de noviembre de 2011 en: http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/57/pr/pr33.pdf.

Constitución Política de los Estados Unidos Mexicanos, última reforma publicada el 13 de octubre de 2011, Disponible hasta el 15 de noviembre de 2011 en http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf.

Convención Americana sobre Derechos Humanos. Disponible hasta el 15 de noviembre de 2011 en http://www.oas.org/juridico/spanish/firmas/b-32.html.

Convenio para la Protección de los Derechos y las Libertades Fundamentales. Disponible hasta el 15 de noviembre de 2011 en http://extranjeros.mtin.es/es/NormativaJurisprudencia/Internacional/ConveniosMultilaterales/documentos/conveurop1950.pdf.

Convenio 108 del Consejo de Europa. Disponible hasta el 15 de noviembre de 2011 en http://www.ifai.org.mx/pdf/ciudadanos/sitios_de_interes/datos_personales/Convenio108.pdf.

Declaración de Madrid. Disponible hasta el 15 de noviembre de 2011 en: http://www.declaraciondemadrid.org/.

Declaración Universal de los Derechos del Hombre. Disponible hasta el 15 de noviembre de 2011 en http://unesdoc.unesco.org/images/0017/001790/179018m.pdf.

Directiva 95/46/CE. Disponible hasta el 15 de noviembre de 2011 en http://www.cert.fnmt.es/legsoporte/Directiva%2095_46_CE%20Datos%20CaracterPersonal.pdf.

Directiva 97/66/CE. Disponible hasta el 15 de noviembre de 2011 en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf.

Directiva 2002/58/CE. Disponible hasta el 15 de noviembre de 2011 en http://www.cert.fnmt.es/legsoporte/Directiva%2058-2002%20DatoscaracterPersonal%20(es).pdf.

Directrices de la Organización para la Cooperación y el Desarrollo Económico. Disponible hasta el 15 de noviembre de 2011 en http://www.csi.map.es/csi/pdf/ocde_directrices_esp.pdf.

Greenleaf, Graham (2011) *76 global data privacy laws* Data Protection & Privacy Information Worldwide, Privacy Laws & Business, septiembre.

Memorándum de Montevideo. Disponible hasta el 15 de noviembre de 2011 en: http://memorandumdemontevideo.ifai.org.mx/.

Ortega Martínez, Jesús, (2004) *Sociedad de la Información y derechos humanos de la cuarta generación. Un desafío inmediato para el derecho constitucional*. Disponible hasta el 15 de noviembre de 2011 en http://www.bibliojuridica.org/libros/4/1510/26.pdf .

Ornelas Núñez, Lina (2010) *El derecho de las niñas, niños y adolescentes a la protección de datos personales: evolución de derechos y su exigencia frente a las redes sociales*, Compendio de Lecturas y Legislación, Protección de Datos Personales, H. Cámara de Diputados e IFAI, Tiro corto Editores, México.

Ornelas Núñez, Lina y Sergio López Ayllón (2010) *La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo*, Compendio de Lecturas y Legislación, Protección de Datos Personales, H. Cámara de Diputados e IFAI, Tiro corto Editores, México.

Pacto Internacional de Derechos Civiles y Políticos. Disponible hasta el 15 de noviembre de 2011 en: http://www2.ohchr.org/spanish/law/ccpr.htm.

Rebollo Delgado, Lucrecio, (2011) *Vida privada y protección de datos: un acerca miento a la regulación internacional europea y española*.

Disponible hasta el 15 de noviembre de 2011 en: http://www.bibliojuridica.org/libros/6/2758/10.pdf.

Resolución 45/95 de las Naciones Unidas. Disponible hasta el 15 de noviembre de 2011 en http://www.paxsocial.com.ar/resol.45-95.htm.

La Agencia de Protección de Datos de la comunidad de Madrid. Desarrollo normativo y evolución de sus funciones

Santiago Abascal Conde

Lourdes Hernández Crespo

Santiago Abascal Conde

Director de la Agencia de Protección de Datos de la Comunidad de Madrid.Ha desarrollado una importante carrera política en el País Vasco. Ha sido miembro de la Junta Directiva Nacional del PP; Presidente de Nuevas Generaciones del PP el País Vasco y Secretario de Educación del PP del País Vasco. También ha sido concejal del PP en el Ayuntamiento de Llodio (Álava) y Procurador de las Juntas Generales de Alava. Presidente y fundador de la Fundación DENAES para la Defensa de la Nación Española. Colabora habitualmente con varios medios de comunicación como El Semanal Digital, COPE, Grupo Intereconomía y esRadio. Asimismo ha publicado varios libros como ¿Derecho de autodeterminación? Sobre el pretendido derecho de secesión del Pueblo Vaso y Secesión y exclusión en el País Vasco; y ha participado en diversos foros como la entrega de la Primera Edición de los "Premios Españoles Ejemplares" otorgados por la Fundación DENAES; inauguración del Monumento a las Víctimas del Terrorismo en Madrid, el 17 de mayo de 2008; I Encuentro Cívico "El Español en España".Licenciado en Sociología por la Universidad de Deusto.

Lourdes Hernández Crespo

Jefe del Servicio de Inspección y Tutela de Derechos de la Agencia de Protección de Datos de la Comunidad de Madrid. Licenciada en Derecho por la Universidad Complutense de Madrid. Master en Derecho de la Telecomunicación y sector Audiovisual por la Universidad C.E.U San Pablo.

Introducción

En el presente trabajo se realizará un análisis de la experiencia de la Agencia de Protección de Datos de la Comunidad de Madrid en la implementación de la Ley de Protección de Datos Personales, con el objetivo de contribuir a la identificación de experiencias para facilitar el ejercicio de las atribuciones de órganos garante homólogos en otros países. Se analizarán las competencias de la Agencia de Protección de Datos de la Comunidad de Madrid y los resultados más importantes.

Legislación, competencias y desarrollo normativo

La Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) es creada por la Ley 13/1995, de 21 de abril, de tratamiento automatizado de ficheros con datos de carácter personal. Fue la primera Ley de Protección de Datos Personales (Reigada, 2005) y creó la primera Agencia Autonómica de Protección de Datos Personales.[1]

La Ley 13/1995, de 21 de abril, define la Agencia como Ente de Derecho Público que actúa en el ejercicio de sus funciones, con plena independencia respecto de la Administración de la Comunidad de Madrid, vela por el cumplimiento de la legislación sobre protección de datos y controla su aplicación, especialmente en lo relativo a los derechos de acceso, rectificación, cancelación y oposición. La Agencia inició actividades en el año 1997.

La Ley 13/1995, de 21 de abril, limitaba las competencias de la Agencia a los ficheros de datos de carácter personal creados o gestionados por la Administración de la Comunidad de Madrid (art. 2). La aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, amplió el ámbito de actuación de la Agencia, extendiendo su ámbito competencial a aquellas Administraciones Públicas vinculadas y dependientes de la Comunidad de Madrid, como son las Entidades

[1] La Ley 13/1995, de 21 de abril había sido modificada parcialmente por la Ley 13/1997, de 16 de junio y por la Ley 6/1999, de 30 de marzo.

Locales, Universidades Públicas y Corporaciones de Derecho Público, en este último caso siempre y cuando los ficheros sean creados o gestionados para el ejercicio de potestades de derecho público.[2] De esta manera, el ámbito competencial de la APDCM abarca un territorio de alrededor de seis millones y medio de habitantes,[3] con 155.000 empleados públicos en la Administración Autonómica y 240.000 empleados públicos trabajando en el resto de Administraciones Públicas del territorio de la Comunidad de Madrid.

La APDCM es una administración independiente, con autonomía presupuestaria y de personal. Su Director es inamovible durante su mandato, hecho limitado por causas tasadas de cese, susceptibles de revisión jurisdiccional. Con excepción de lo anterior, no existe poder de remoción del Gobierno de la Comunidad Autónoma sobre el Director de la APDCM,[4] ni está sometida a órdenes, instrucciones ni directrices administrativas. El Director de la APDCM ejerce sus funciones con plena independencia y objetividad, sin estar sujeto a mandato imperativo o instrucción alguna en el desempeño de aquéllas.[5]

La Agencia tiene un carácter de administración independiente en el ejercicio de las funciones de inspección, supervisión y sanción, para hacer cumplir la legislación de protección de datos personales y de garantía de los derechos de las personas.

La relación de colaboración con las Administraciones Públicas de la Comunidad de Madrid sometidas a su control ha sido siempre una prioridad de la Agencia. El ejercicio de una función pública de soberanía, y el desarrollo de una función de autoridad, no está reñida con una vocación de colaboración. En esta línea de colaboración, la APDCM han firmado Convenios de Cooperación con las seis

[2] Artículo .2 Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

[3] Datos del Instituto Nacional de Estadística 2011.

[4] Artículo 15 Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

[5] Artículo 16.2 Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. A.

Universidades Públicas de la Comunidad de Madrid, con la Federación de Municipios de Madrid, que agrupa a los 179 Ayuntamientos de la Comunidad de Madrid, y con la Unión Interprofesional, que representa a los 24 Colegios Profesionales de la Comunidad de Madrid. Con la firma de los Convenios se busca facilitar la comunicación, creando Comisiones de Seguimiento que permiten una planificación conjunta y el conocimiento de las preocupaciones y dificultades encontradas en el cumplimiento de la legislación de protección de datos.

Funciones normativas

La APDCM ha llevado a cabo un desarrollo normativo de la legislación de protección de datos único en nuestro país.[6] En la primera etapa, el desarrollo normativo ha ido enfocado a regular las funciones de la Agencia con el objetivo de impulsar su actividad. Así, a propuesta de la Agencia, el Consejo de Gobierno de la Comunidad de Madrid aprobó el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros, así como su inscripción en el Registro de ficheros de Datos Personales.[7] El Decreto también prevé un informe preceptivo de la Agencia a las disposiciones de carácter general que proceden a declarar ficheros, que permite control necesario para desarrollar una actividad preventiva, a objeto de evitar en lo posible el incumplimiento de la legislación. Adicionalmente, contiene disposiciones encaminadas a favorecer la simplificación administrativa, que ahorran trámites y hacen más sencillo el cumplimiento de la legislación. Además, se prevé la inscripción de oficio en el Registro de la Agencia y regula el tipo de disposición de carácter general que debe ser utilizado para declarar los ficheros por la Administración Autonómica, la Asamblea de Madrid, los Ayuntamientos, las Corporaciones de Derecho Público y las Universidades Públicas.[8]

---

[6] Este desarrollo normativo puede consultarse en el *"Repertorio de Legislación y Jurisprudencia sobre Protección de Datos"*, segunda edición, Ed. Thomson Reuters, Madrid, 2010.

[7] Disponible en http://www.madrid.org/wleg/servlet/Servidor?opcion=VerHtml&nmnorma=2269&cdestado=P.

[8] Por Resolución de 9 de enero de 2007, del Director de la Agencia de Protección de Datos de la Comunidad de Madrid, se establecen los modelos de impresos y los medios por los que debe procederse a la notificación de inscripciones de creación, modificación o supresión de ficheros,

En esta primera etapa, merece resaltar la aprobación del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.[9] Este Decreto permitió fortalecer las garantías de la Administración, de los empleados públicos y de los ciudadanos en esta actividad coercitiva de la Agencia. El Reglamento regula, por una parte, la función de control sobre los ficheros de datos creados o gestionados por la Administración de la Comunidad de Madrid, Entidades Locales, Universidades Públicas y Corporaciones de Derecho Público del territorio de nuestra Comunidad, para comprobar el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en sus disposiciones de desarrollo, y especialmente, en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

Otra de las funciones atribuidas a la Agencia es la de atender peticiones y resolver reclamaciones formuladas por los interesados para la protección de sus derechos de acceso, rectificación, cancelación y oposición, en relación con los ficheros de datos. El Decreto 67/2003 persiguió también fortalecer y desarrollar la función de tutela de la Agencia, y evitar que los derechos de protección de datos reconocidos a los ciudadanos puedan verse vulnerados por una actuación contraria a la Ley. Con este Reglamento se desarrollan las garantías tanto en el procedimiento de infracción administrativa como de tutela de derechos; y se establece un control preventivo a través de los planes sectoriales de inspección, cuyo cometido es analizar el ámbito de aplicación de la Ley 8/2001, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, el nivel de adaptación y cumplimiento de los principios de protección de datos.

Durante una segunda etapa, la actividad normativa ha ido encaminada a regular la organización administrativa de la Agencia, adaptando su estructura al incremento de las responsabilidades administrativas.

---

al Registro de Ficheros de Datos Personales (BO. Comunidad de Madrid 7 febrero 2007, núm. 32, [pág. 30]) En la Actualidad es posible la declaración de ficheros con certificado electrónico.

[9] Disponible en http://www.madrid.org/cs/Satellite?cid=1247227049662&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado#a1142575940340.

Por ello, la Agencia impulsó la aprobación por parte del Consejo de Gobierno, del Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.[10] Este Estatuto separó algunas funciones que por su naturaleza no podían residir en la misma unidad administrativa. Así, crea dos nuevas unidades administrativas dependientes del Director de la Agencia: La Subdirección General de Registro de Ficheros y Consultoría, y la Subdirección General de Inspección y Tutela de Derechos. El Decreto tuvo, además, la virtualidad de ser el primer estatuto de una autoridad de control que regula la actividad de consultoría.

La tercera etapa de actividad normativa de la Agencia ha tratado de cumplir una función valorativa o de interpretación, que contribuya a adaptar el ordenamiento jurídico de protección de datos personales a las Administraciones Públicas. El derecho fundamental a la protección de datos personales tiene contenidos distintos frente a tratamientos realizados por las Administraciones Públicas y los particulares, porque los ficheros públicos y los privados son cualitativamente distintos. Por ello, es necesario llevar a cabo una adecuación del derecho a la protección de datos personales en las Administraciones Públicas, interpretándolo de conformidad con los derechos fundamentales, que exigen una actividad pública objetiva de prestación de los mismos, en especial en las Autoridades Autonómicas, ya que su único ámbito de control son los tratamientos de datos personales realizados por las Administraciones Públicas (Davara, 2003: 32-34).

La Agencia ha procedido al análisis del contenido del derecho fundamental a la protección de datos personales para la Administración Autonómica, Local, Colegios Profesionales y Universidades Públicas, mediante la aprobación de algunas Recomendaciones en ámbitos públicos específicos,[11] producto del esfuerzo de interpretación del derecho fundamental a la protección de datos en el ámbito público, que recogen los criterios establecidos por la Agencia en la respuesta a consultas formuladas por responsables públicos.

[10] Disponible en http://www.madrid.org/cs/Satellite?cid=1247227037983&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_contenidoFinal.

[11] Todo ello en virtud de lo previsto en el artículo 15.d) de la Ley 8/2002, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

De esta forma, se aprobó la Recomendación 1/2004, de 14 de abril, sobre utilización y tratamiento de datos del padrón municipal de habitantes por los Ayuntamientos de esta Comunidad Autónoma. El padrón municipal es uno de los ficheros públicos que contiene más datos personales y también uno de los que presenta más problemas. Los accesos a sus contenidos son fuente de conflicto permanente entre el derecho a la autodeterminación informativa y la actividad administrativa de prestación y garantía de otros derechos de carácter social. La Recomendación analiza el derecho a la protección de datos en relación al fichero del padrón municipal, configurando una nueva interpretación de su finalidad (APDPCM, 2004).

Igualmente, preocupada por la seguridad de los ficheros manuales de historias clínicas de los servicios sanitarios públicos de la Comunidad de Madrid, la Agencia aprobó la Recomendación 2/2004, de 30 de julio, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas. La aparición en algunas ocasiones de historias clínicas abandonadas en soporte de papel, y la alarma social causada y trasladada a los medios de comunicación, llevaron a la Agencia aprobar la Recomendación 3/2004, con la pretensión de ser un documento que resuelva las dudas, al abordar cuestiones como el archivo y custodia de las historias clínicas, su seguridad, la conservación y las cesiones de datos de la historia clínica.[12]

En este mismo contexto se produce con la aprobación de la Recomendación 1/2005, de 5 de agosto, de la APDCM, sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid. La APDCM consideró conveniente realizar una serie de recomendaciones sobre medidas de custodia y archivo de historias sociales no informatizadas, que sirvieran de ayuda y referencia a los centros e instituciones públicas de prestación de servicios sociales de la Comunidad de Madrid desde la óptica de la protección de datos.

[12] La Recomendación tuvo en cuenta el Dictamen del Grupo de Expertos en Información y Documentación Clínica de la Consejería de Sanidad y Consumo de la Comunidad de Madrid, así como los distintos protocolos de custodia de historias clínicas que tienen los hospitales de la Comunidad. En todo caso, deberán todavía desarrollarse los principios establecidos en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

En relación a las consultas que se venían planteando a la APDCM por la Administración Autonómica y por Ayuntamientos y Universidades Públicas, respecto de la posibilidad de facilitar a las secciones sindicales, comités de empresa y juntas de personal, en su condición de órganos de representación de los empleados públicos, determinada información personal de dichos empleados, se aprueba la Recomendación 1/2006, de 3 de abril, de la APDCM, sobre cesiones de datos de empleados públicos de la Comunidad de Madrid a las secciones sindicales, comités de empresa y juntas de personal. Con esta Recomendación se trata de dar respuesta a supuestos concretos y reales planteados, sobre la posibilidad de acceder a determinada información de los empleados públicos para el ejercicio de su actividad sindical.

Para comprobar el grado de adecuación a la normativa de protección de datos en los Servicios Sociales, la APDCM llevó a cabo durante 2007 un Plan de Inspección sobre los ficheros más importantes en este campo, como pueden ser los ficheros "Ingreso Madrileño de Integración", "Reconocimiento de minusvalías" y "Adopciones". En total se inspeccionaron 12 ficheros de datos personales y se procedió a elaborar y aprobar la Recomendación 1/2008, de 14 de abril, sobre el tratamiento de datos personales en los Servicios Sociales de la Administración de la Comunidad de Madrid y en los Servicios Sociales de los Entes Locales de la misma Comunidad. Esta Recomendación trata de la primera norma en protección de datos que recoge supuestos específicos de aplicación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos.

Derivada del análisis exhaustivo que la Agencia venía realizando sobre la publicación de datos personales a través de Internet, se aprueba la Recomendación 2/2008, de 25 de abril, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios web institucionales y en otros medios electrónicos y telemáticos. En ella se establece un conjunto de criterios que permiten que la publicidad, como tratamiento, respete el derecho fundamental a la protección de datos personales, tratando de equilibrar la aplicación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, con la aplicación de la normativa de protección de datos. En consecuencia, habrá que

valorar, por una parte, el nivel de injerencia en el derecho fundamental a la protección de datos personales, derivado del nivel de publicidad, del tipo de dato personal al que se va a tener acceso —si es o no de público conocimiento— y las consecuencias negativas que esto puede tener en el interesado y, por otra, el interés público real que hay en el acceso a esa información administrativa.

Desde la publicación de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos se reconoce a los ciudadanos el derecho "a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos".

Para hacer compatible el acceso electrónico de los ciudadanos a los servicios públicos con el respeto y defensa del derecho fundamental a la protección de datos, la Agencia aprueba la Recomendación 3/2008, de 30 de abril, sobre tratamiento de datos de carácter personal en servicios de administración electrónica.[13]

Entre las diversas formas de tratamiento de datos personales, la imagen de las personas se ha convertido en un elemento permanente de nuestra realidad, expandiéndose la utilización de cámaras y videocámaras a un número cada vez mayor de Órganos de la Administración Autonómica, Ayuntamientos, Universidades Públicas, Corporaciones de Derecho Público y otras Instituciones de la Comunidad de Madrid. La instalación de esto dispositivos prolifera, entre otros sectores, en la educación, en la sanidad, en los transportes y las infraestructuras y en todo tipo de centros oficiales.

En el año 2007, la APDCM, procedió a la elaboración y posterior aprobación de la Instrucción 1/2007, de 16 de mayo, sobre el

[13] Todas las Recomendaciones reseñadas se pueden descargar a través la página web de la Agencia de Protección de datos de la Comunidad de Madrid http://www.madrid.org/cs/Satellite?cid=1247227049662&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado#a1142575940641.

tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid. Con esa Instrucción se pretende ofrecer una adecuada respuesta normativa a este tema, facilitando la interpretación normativa de lo dispuesto en la Ley Orgánica de Protección de Datos y favoreciendo su correcta aplicación en relación con la instalación de estos sistemas de tratamiento de imágenes.

Tras la entrada en vigor de la Instrucción 1/2007, fruto de la experiencia acumulada, la Agencia consideró adecuada la publicación de una Guía de videovigilancia, que sirve de soporte a los responsables de ficheros, así como los encargados de tratamiento del ámbito competencial de esta Agencia, para cumplir con la normativa de protección de datos cuando se decida la utilización de estos sistemas.

Además de exponer cuáles son los requisitos de obligado cumplimiento, la Guía recoge diversa información útil para los responsables, como es la utilización de un "check-list" para saber si se cumplen los requisitos que impone la normativa de protección de datos con carácter previo al funcionamiento de las cámaras.[14]

En el año 2009 la APDCM aprobó dos nuevas Instrucciones, dirigidas, sobre todo, a los responsables de ficheros del ámbito sanitario. Por un lado, la Instrucción 1/2009, de 17 de diciembre de 2009, sobre el tratamiento de datos personales de los recién nacidos en los centros asistenciales que integran la red sanitaria única de utilización pública de la Comunidad de Madrid.

Su finalidad es mejorar los procedimientos de toma de huellas, tanto del recién nacido como de la madre, permitiendo realizar una identificación y vinculación inequívoca de ambos, evitando confusiones y problemas de intercambio de bebés en los centros asistenciales.

Por otro lado, la Instrucción 2/2009, de 21 de diciembre de 2009, sobre el tratamiento de datos personales en la emisión de justificantes médicos, incide en la necesidad de que no se faciliten a los departamentos de personal más datos de los que realmente son necesarios para

[14] Colección Guías de Protección de Datos, disponible en el sitio web de la Agencia www.apdcm.es, canal "Publicaciones".

justificar una ausencia al trabajo, evitando que se pueda conocer el diagnóstico o causa concreta de la enfermedad del trabajador.[15]

La declaración de ficheros y su inscripción

Una de las funciones de la APDCM es garantizar que los tratamientos de datos personales que manejan las Administraciones Públicas de la Comunidad de Madrid se encuentren declarados y estén inscritos en el Registro de Ficheros. Para ello, la Agencia desarrolla una labor de apoyo y asesoramiento a los responsables de los ficheros en lo concerniente a la creación, modificación y supresión de ficheros de datos de carácter personal y su inscripción en el Registro de Ficheros. La experiencia demuestra que un responsable público que no declara ficheros, no respeta los principios ni los derechos de protección de datos personales.[16] La declaración y la inscripción de los ficheros es un paso necesario para que los Registros puedan cumplir su función de garantizar el principio de publicidad, y que cada ciudadano pueda ejercitar el derecho de consulta al registro general.[17]

La Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, establece en su artículo 18 que la APDCM llevará un Registro de Ficheros de Datos de Carácter Personal con una doble finalidad: facilitar al ciudadano el ejercicio de sus derechos respecto a los tratamientos de datos realizados por instituciones públicas de la Comunidad de Madrid, y servir de medio instrumental para el cumplimiento de sus funciones al resto de unidades y órganos de la Agencia. La consulta al Registro es gratuita y está disponible para cualquier persona a través de Internet, en el sitio web

[15] Todas las Recomendaciones reseñadas se pueden descargar a través la página web de la Agencia de Protección de datos de la Comunidad de Madrid http://www.madrid.org/cs/Satellite?cid=1247227049662&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado#a1142575940413.

[16] La declaración e inscripción de ficheros no está extendida en la Unión Europea. Sólo es obligatoria en España y Austria. En Gran Bretaña, se inscriben casi todos los ficheros a excepción de algunas categorías de tratamientos. En cambio, en Italia la regla general es la no inscripción salvo supuestos específicos como los ficheros genéticos o de seguros.

[17] Ley Orgánica 15/1999 de Protección de Datos (LOPD), artículo 14 *"cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".*

de la Agencia www.apdcm.es, canal "Registro de Ficheros". Tal como establece el artículo 20.2 de la Ley 8/2001, periódicamente la APDCM remitirá a la Agencia Española de Protección de Datos el contenido del Registro de Ficheros de Datos Personales de la Comunidad de Madrid, al objeto de su inscripción en el Registro General de Protección de Datos.

Las inscripciones de nuevos ficheros realizadas durante el año 2010 mantienen una tendencia estable de crecimiento respecto a años anteriores, debido al alto nivel de regularización existente en determinados ámbitos de competencia de la APDCM, especialmente en su Administración. Uno de los motivos del incremento de inscripciones responde al creciente número de ficheros de videovigilancia.[18]

La tutela de derechos y el control de ficheros

La Agencia tiene también la función de velar por el cumplimiento de los derechos de información, acceso, oposición, rectificación y cancelación (Derechos ARCO), atender las peticiones y resolver las reclamaciones formuladas por los interesados para la protección de sus derechos. También debe velar porque los derechos de acceso, rectificación y cancelación sean reales y efectivos. Decía un jurista italiano, Giannini, que no hay ningún derecho si no hay un tribunal que lo aplique. En todo caso, la actividad inspectora de la Agencia orienta su labor a elaborar un catálogo de recomendaciones para adaptar los tratamientos de datos personales a la legislación, y evitar en lo posible la comisión de infracciones. En los últimos años se ha producido un incremento de la actividad de control de la Agencia, consecuencia tanto del aumento competencial como de una mayor sensibilización de los ciudadanos acerca de su derecho fundamental a la protección de los datos de carácter personal.

La Subdirección de Inspección y Tutela de Derechos es la unidad administrativa de la APDCM a la que compete el ejercicio de las funciones derivadas de la potestad de inspección, reguladas en el artículo 19 de la Ley 8/2001, de 13 de julio, por lo que es competencia

[18] Datos extraídos de la Memoria de las actividades realizadas en la Agencia de Protección de Datos de la Comunidad de Madrid durante el año 2010 en el sitio web de la Agencia www.apdcm.es, canal "Publicaciones".

de esta unidad administrativa el impulso y la instrucción de los procedimientos a que den lugar las reclamaciones y denuncias de los ciudadanos para la protección de sus Derechos ARCO, así como de los procedimientos de infracción de las Administraciones Públicas que se tramiten como consecuencia del ejercicio de la función de control, para determinar la existencia o no de una infracción prevista en la Ley Orgánica 15/1999 de Protección de Datos.

Por un lado, el procedimiento administrativo de tutela de derechos se inicia siempre mediante reclamación interpuesta por el ciudadano, cuando éste considera que el responsable del fichero no ha atendido correctamente sus Derechos ARCO.

Este procedimiento se encuentra regulado en el Decreto 67/2003, de 22 de mayo. Se distingue por su carácter contradictorio, de manera que tanto el ciudadano como el responsable del fichero pueden presentar alegaciones para su defensa. La resolución de la APDCM será estimatoria si considera que el Derecho ARCO no ha sido debidamente atendido, o desestimatoria en caso contrario. En definitiva, se trata de garantizar los Derechos ARCO de los ciudadanos.

Durante el año 2010 tramitaron 58 expedientes de tutela de derechos, en su mayoría sobre el acceso a la historia clínica. También destacan las peticiones de tutela de derechos por cancelación de datos en los Boletines Oficiales.[19]

Por otro lado, el procedimiento de inspección inicia siempre de oficio, si bien la mayoría de las veces viene motivado por la presentación de una denuncia ciudadana. La Agencia abre este tipo de procedimientos por varias vías: bien cuando inicia un plan de inspección, bien cuando aparece alguna noticia en prensa de la que puede derivar una infracción en la materia, o bien cuando se tiene constancia por otros medios de que puede existir un posible incumplimiento de la normativa de protección de datos. Al igual que el procedimiento de tutela de derechos, el procedimiento de inspección se encuentra establecido en el Decreto 67/2003, de 22 de mayo. Regula el supuesto de que existan indicios de que se ha vulnerado la protección de datos

[19] Datos extraídos de la Memoria de las actividades realizadas en la Agencia de Protección de Datos de la Comunidad de Madrid durante el año 2010 en el sitio web de la Agencia www.apdcm.es, canal "Publicaciones".

en las actuaciones realizadas, por parte del responsable del fichero. Asimismo, desde la creación de la APDCM hasta la fecha, se han tramitado 1469 expedientes de inspección. De los 176 expedientes tramitados en 2010, se debe distinguir los que corresponden a la función inspectora y los que corresponden a la función de tutela de derechos. Respecto de los primeros, se han tramitado 118 procedimientos, correspondiendo 45 a la Administración de la Comunidad de Madrid, 53 a la Administración Local, 2 a las Universidades y 1 a las Corporaciones de Derecho público. A su vez, 17 resultaron ser de la competencia de la Agencia Española de Protección de Datos.

Es importante señalar que buena parte de la actividad de inspección se centra en actuaciones llevadas a cabo de oficio por la Subdirección General de Inspección y Tutela de Derechos. Estas actuaciones se concretan en el diseño de diferentes Planes de Inspección desarrollados desde la puesta en funcionamiento de la Agencia.

El artículo 18 del Decreto 67/2003, de 22 de mayo, regula los Planes Sectoriales de Inspección, como una de las manifestaciones de la función de control de la Agencia. De carácter preventivo, estos Planes consisten en analizar —por cada uno de los sectores de la actividad administrativa pública, cuyos ficheros se encuentran bajo el ámbito de aplicación de la Ley 8/2001, de 13 de julio— cuál es el grado de adecuación y cumplimiento que tienen a los principios de la protección de datos, así como garantizar que los responsables de los ficheros públicos hacen efectivo el cumplimiento de los Derechos ARCO que ejercen los ciudadanos.

Una vez analizada la información y concluidas las actuaciones y comprobaciones necesarias, el Director de la Agencia dictará, de conformidad con el artículo 15.d) de la Ley 8/2001, de 13 de julio, instrucciones precisas, en las que se determinará si los ficheros públicos objeto del plan sectorial están adecuados o no a la normativa de protección de datos. Entre otros, merece destacar el "Plan de Inspección de Servicios Sociales 2007-2008", que tuvo como objetivo realizar una inspección preventiva en el ámbito de los Servicios Sociales, tanto de la Comunidad de Madrid como de sus Ayuntamientos. En el año 2008 la APDCM puso en marcha el Plan de Inspección 2008-2010 sobre el cumplimiento de la normativa de protección de datos en su recogida a través de páginas web de los Ayuntamientos de esta Comunidad,

para conocer el grado de cumplimiento de la Recomendación 3/2008, de 30 de abril, de la APDCM, sobre tratamiento de datos de carácter personal en los servicios de Administración, que citábamos en apartado anteriores.

En el ámbito de la Administración Local y en reconocimiento del derecho de los ciudadanos a relacionarse con la administración por medios electrónicos (Ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos), numerosos Ayuntamientos de la Comunidad de Madrid han puesto en servicio páginas web para que el ciudadano pueda realizar trámites administrativos, acercando al ciudadano a la Administración municipal. Así, a través de los portales disponibles se permite al ciudadano acceder a información y servicios de su competencia, presentar solicitudes y recursos, realizar trámites de audiencia, efectuar pagos, etc.

El Plan de Inspección concluye en el 2010 con la realización de actuaciones de investigación y el dictado de instrucciones singulares de adecuación en un total de sesenta Ayuntamientos de la Comunidad de Madrid.

En las instrucciones dictadas se ha hecho especial hincapié, entre otras cuestiones, en el cumplimiento del deber de información en la recogida de datos, previsto en artículo 5 de la Ley Orgánica de Protección de Datos, en la creación de los correspondientes ficheros con datos personales y su inscripción en el Registro de la APDCM, en la "Política de Privacidad" de las webs inspeccionadas, en las fórmulas adoptadas para la publicación de sesiones y acuerdos del Pleno de la Corporación, en la utilización de "Foros de opinión", la "Publicación de Imágenes" y de datos relativos a procesos selectivos y no selectivos.

Por último, la APDCM da publicidad a resúmenes de las resoluciones más destacadas, dictadas por el Director de la Agencia en el ejercicio de sus competencias de control y de tutela de derechos, sobre los ficheros de datos creados o gestionados por las Administraciones e instituciones públicas de la Comunidad de Madrid.

Las resoluciones se publican[20] de forma totalmente anonimizada, porque su difusión va encaminada a aumentar la transparencia y la seguridad jurídica, dando a conocer así los criterios de la Agencia, y permanecen accesibles tanto en la revista digital datospersonales.org, como a través del canal "Servicios" del sitio web de la Agencia, en el que se incorporaron dos nuevos apartados denominados "Resoluciones tutela de derechos" y "Resoluciones función de control". En el futuro cada resolución se clasificará atendiendo al ámbito sectorial respectivo (Administración Autonómica, Universidades, Corporaciones Locales, Corporaciones de Derecho Público, Instituciones y Organismos Públicos).

Actividad consultiva y de asesoramiento jurídico a los responsables de ficheros y empleados públicos

La actividad principal de la Agencia está orientada a la colaboración con las Administraciones Públicas, ayudando a que las necesidades de la gestión pública se adecuen al derecho fundamental a la protección de datos personales. Es un rasgo distintivo de la APDCM su labor de consultoría y apoyo a los responsables de los ficheros públicos, para que puedan conocer y respetar el ordenamiento jurídico de protección de datos personales. Así, la Agencia ha colaborado con la Administración Autonómica, Administraciones Locales, Universidades Públicas y Corporaciones de derecho público para ayudarles a desarrollar sus actividades.

La Agencia no ha pretendido ejercer sólo las funciones de vigilancia y control sobre ficheros de datos de carácter personal creados o gestionados por las Administraciones Públicas, sino que ha colaborado con los responsables de ficheros y los empleados públicos en lo concerniente a la creación, modificación y supresión de ficheros, así como en el cumplimiento de los principios y derechos de protección de datos, facilitando la experiencia y el conocimiento que tiene el personal de la Agencia.

De esta manera, la APDCM ha desarrollado una intensa labor de asesoramiento jurídico dirigida a los responsables públicos. Además

[20] Sitio web de la Agencia www.apdcm.es, canal "Consultas y Resoluciones".

de informar los proyectos de disposiciones de creación, modificación y supresión de ficheros, la Agencia informa también sobre aquellos proyectos de disposiciones generales que pueden incidir en el derecho fundamental a la protección de datos personales. Al mismo tiempo, responde las consultas jurídicas de los responsables de ficheros acerca de la legitimidad de algunos tratamientos de datos personales.

La actividad consultiva de la Agencia, además de dar seguridad jurídica, permite desarrollar una actividad preventiva, que evita se vulnere este derecho fundamental. De esta forma, desarrolla una importante labor consultiva sobre protección de datos, ante preguntas planteadas por los responsables de ficheros.[21] La APDCM resuelve estas consultas con una respuesta firmada por su Director, misma que es vinculante, de manera que no se de la contradicción de que dos órganos de la Agencia mantengan opiniones distintas, con la incertidumbre y desazón que deja esto en los ciudadanos y los empleados públicos. La mayoría de las consultas son relativas a cesiones de datos o la adecuación de su tratamiento a la legislación. Las consultas, además de dirigirse al responsable del fichero, también se publican en las Memorias, en la web y en la revista datospersonales.org para dar mejor a conocer los criterios de la Agencia.[22]

La APDCM elabora un Plan de Actuaciones para cada una de las Consejerías de la Administración Regional, Ayuntamientos, Colegios Profesionales y Universidades Públicas, donde se expone la actividad prevista para ese año en relación con esa Administración Pública —que parte de la situación actual— y se desarrolla a través de distintos indicadores o cuadros de mandos. Esta planificación se envía a comienzo de año a cada Administración Pública, a la vez que se comunica al consultor responsable de las labores de asesoramiento y apoyo en esa Administración. La Agencia realiza reuniones de asesoramiento e información dirigidas a los responsables de ficheros y a los empleados públicos, la mayoría in situ en los centros públicos.

[21] Por ejemplo, la Comunidad de Madrid consulta si puede ceder datos sobre familias numerosas a un Ayuntamiento a efectos de procedencia o revocación de beneficios fiscales; un hospital pregunta si pueden estar presentes en las consultas asistenciales intérpretes para facilitar la atención a los inmigrantes; un Ayuntamiento consulta si puede tratar los datos biométricos de sus empleados para el control de presencia o si puede ceder información sobre empleados públicos a las organizaciones sindicales, etc.

[22] Sitio web de la Agencia www.apdcm.es, canal "Consultas y Resoluciones".

La Agencia ha desarrollado también algunos Planes de Actuación como el realizado en los Centros de Acceso Público a Internet, para promover el respeto al derecho fundamental a la protección de datos, impulsando la declaración de los ficheros, revisando el cumplimiento del principio de información y facilitando el ejercicio de los derechos. Igualmente se realizó el Plan para la prevención de cesiones de datos a empresas funerarias, que sólo pueden hacerse con consentimiento de los familiares.

En la actividad del año 2010 son dignas de mención las jornadas de formación llevadas a cabo, entre las que resaltan las dedicadas a: la formación de Directivos de la Comunidad de Madrid; a los requisitos de protección de datos en la Administración-e; a la correcta implantación de los sistemas de videovigilancia y a las normas de seguridad, en la que se hizo entrega a los asistentes de la publicación de la APDCM, denominada *Seguridad y Protección de Datos Personales*, que ofrece a los responsables de ficheros información y las directrices necesarias para implantar una política de seguridad, que traslade a la práctica los preceptos legales del Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos Personales.

La Unidad de Consultoría también ha realizado iniciativas sectoriales de interés e impacto en la protección de datos personales. Así, ha tenido y tiene gran relevancia y trascendencia social la iniciativa puesta en marcha por la APDCM para concienciar a los alumnos de Enseñanza Secundaria de la Comunidad de Madrid, de los riesgos que existen para su privacidad en Internet, especialmente en las redes sociales.

La Agencia elaboró un Plan de Comunicación en Protección de Datos Personales para Escolares, el 28 de enero de 2009, coincidiendo con el Día Europeo de la Protección de Datos Personales. La finalidad de este Plan era dar a conocer entre los alumnos el derecho fundamental a la protección de datos personales, exponiendo los riesgos a su privacidad que provienen de las modernas tecnologías de la información y las comunicaciones, tratando de que los menores se conciencien acerca de la necesidad de un uso responsable de éstas.

La sesión informativa se realizó en los 404 Institutos de Educación Secundaria de la Comunidad de Madrid, recibiendo la sesión informativa un total de 80.000 alumnos de edades entre 15 y 16 años. La sesión informativa fue impartida por más de 60 expertos en protección

de datos (Jueces, Magistrados, Abogados, Juristas) y personal de la APDCM. Para cubrir el resto de Institutos de Educación Secundaria se contó con la colaboración de los orientadores de los mismos, así como tutores y jefes de estudios.

El objetivo de realizar la sesión informativa en estos Institutos era suscitar un debate acerca de los tratamientos de datos personales que los jóvenes realizan cotidianamente a través del uso de redes sociales, mensajerías instantáneas, chats, telefonía móvil, etc., y de sus consecuencias presentes y futuras, teniendo en cuenta que ninguna información desaparece. Para ello, la sesión estuvo estructurada de la siguiente forma: A través de los materiales audiovisuales e impresos entregados en las sesiones, y mediante el uso de un lenguaje coloquial comprensible a la audiencia a la que va dirigido, se reflejan los diferentes problemas que lleva consigo el uso de Internet en la actualidad, como es el caso, por ejemplo, del ciberbullying, el spam o el phising. Esta iniciativa tuvo una gran repercusión en los diferentes medios de comunicación social, tanto en prensa escrita como en Internet y televisión.[23]

Por último, la APDCM también realizó esta misma sesión informativa a más de 100 padres y madres de alumnos, ya que éstos son los primeros que deben conocer los peligros que sus hijos pueden encontrarse en el uso de las tecnologías.

La actividad formativa y las publicaciones

La efectividad del derecho fundamental a la protección de datos personales depende del cumplimiento de un conjunto de obligaciones por parte de los responsables de ficheros y de los empleados públicos, que, antes de nada, deben conocer. Las infracciones en el ámbito público no se producen en su mayoría de mala fe, o la búsqueda de un enriquecimiento ilícito, sino por desconocimiento de la normativa por los empleados públicos. Así, en la XXIV Conferencia Internacional de Protección de Datos y Autoridades de Control, celebrada en Cardiff en el 2002, se concluyó que la mejor forma de garantizar este derecho es

[23] Todo el material e información relacionada con el tema puede consultarse en el sitio web de la Agencia www.apdcm.es, enlace "Jóvenes e Internet".

a través de la formación y concienciación de ciudadanos y empleados públicos en la importancia de este derecho fundamental.

La Agencia ha desplegado una extensa actividad formativa dirigida a los empleados públicos que recogen, graban, conservan, modifican y cancelan datos personales de los ciudadanos. Es de enorme importancia que se formen en protección de datos ya que los principios de calidad, información, consentimiento y los derechos ARCO de los ciudadanos tienen como trasunto los deberes de los empleados públicos, entre ellos el deber de secreto (artículo 10, Ley Orgánica 15/1999 de Protección de Datos).

Para considerar la importancia real de esta actividad formativa, hay que pensar, por ejemplo, en la información personal que maneja el Colegio de Abogados de Madrid, la Universidad Complutense, el Ayuntamiento de Madrid, el Hospital La Paz, las residencias de personas mayores o los más de 1.200 centros educativos de la Comunidad de Madrid.[24]

Las Jornadas de formación son una ocasión inmejorable para exponer los criterios de la Agencia y compartir experiencias y dificultades reales que tienen en su aplicación las Administraciones y empleados públicos. Así, la APDCM ha celebrado 3.788 sesiones informativas a las que han acudido 48.257 empleados públicos.[25]

La APDCM también ha desarrollado una intensa actividad de publicación de libros que cumplen la finalidad formativa. Así, la Agencia inició la Colección de Protección de Datos en la editorial Cívitas-Thomson-Aranzadi, tras la firma de un Convenio de colaboración. Con la publicación de libros se cumple también una función de adecuación de este ordenamiento jurídico de protección de datos personales a las Administraciones Públicas. Dentro de la Colección se han publicado Manuales y Guías, que tratan de facilitar el conocimiento de este

[24] También hay que mencionar los programas específicos de formación continua de protección de datos para las Administraciones Locales –con un programa para el personal y cargos electivos de las Corporaciones Locales de la Comunidad de Madrid- y para educadores y responsables de centros educativos.

[25] Datos extraídos de la Memoria de las actividades realizadas en la Agencia de Protección de Datos de la Comunidad de Madrid durante el año 2010 en el sitio web de la Agencia www.apdcm.es, canal "Publicaciones".

derecho fundamental de un modo accesible para todos. Así, se publicó el Manual de Protección de Datos para las Administraciones Públicas, que pretende ser un instrumento que facilite la formación en el derecho fundamental a la protección de los datos personales de los empleados públicos del territorio de la Comunidad de Madrid.

La Agencia ha publicado también guías que dan conocer sus en sectores específicos, facilitando el cumplimiento de las obligaciones de los responsables de ficheros y de los empleados públicos. Las Guías tienen un contenido formativo teórico que expone de manera sencilla conceptos fundamentales del derecho a la protección de datos personales, incluyendo respuestas a las consultas más frecuentes. Al mismo tiempo, es un documento práctico que permite a los responsables de los ficheros el cumplimiento de sus obligaciones en la materia durante todo el proceso de tratamiento, y ayudan a identificar los tratamientos de datos de carácter personal y declararlos a través de una disposición de carácter general. Además, muestran ejemplos de cláusulas o leyendas para facilitar el cumplimiento del principio de información y modelos de ejercicio de los derechos de acceso, rectificación y cancelación.

Así, la Guía de Protección de Datos para Colegios Profesionales analiza la distinción entre los ficheros públicos y los ficheros privados de los colegios profesionales, relevante a la hora de determinar su régimen jurídico —procedimiento de declaración y régimen sancionador— y la autoridad de control.

La Guía de Protección de Datos para Universidades analiza el derecho a la confidencialidad de los datos personales de los alumnos, y el derecho de acceso de los padres a los expedientes académicos de sus hijos, la gestión de la matriculación a través de entidades financieras y la emisión del carné del estudiante junto con tarjetas de crédito o débito, la publicación de listados y calificaciones de alumnos en tablones de anuncios y sitios web, los directorios de correos electrónicos y la cesión de datos del censo electoral a las candidaturas en los procesos electorales universitarios.

La Guía de Protección de Datos Personales para Servicios Sociales Públicos parte de que la asistencia social y la prestación de servicios sociales son actividades que tratan de ayudar a las personas y que

requieren el manejo de datos personales de distintos colectivos —beneficiarios, familiares, empleados, etcétera—, pero al mismo tiempo tienen que respetar los principios y los derechos de protección de datos.

La Guía de Protección de Datos Personales para Ayuntamientos recuerda que existe la obligación de informar en los cuestionarios o impresos que se utilizan para la recogida de los datos, de manera expresa, precisa e inequívoca, de la existencia de un fichero, de su finalidad, de los destinatarios de la información, del responsable del fichero y de su dirección y del ejercicio de los derechos de acceso, rectificación y cancelación.

La Guía de Protección de Datos Personales para Servicios Sanitarios Públicos trata de dar respuesta a las necesidades formativas y las preocupaciones que tienen todos los que trabajan en el ámbito sanitario por el tratamiento de historias clínicas.

Por otra parte, la APDCM, como parte de su contribución a dar certeza y seguridad jurídica en esta materia, ha elaborado un Repertorio de Legislación y Jurisprudencia sobre Protección de Datos. Está publicado dentro de la colección "Protección de Datos" de la editorial Civitas-Thomson, y reúne la legislación española, tanto a nivel nacional como autonómico, incluyendo no sólo normas generales de protección de datos, sino también normas sectoriales que afectan a ámbitos diversos como la administración pública, la hacienda pública, sanidad y farmacia, seguridad ciudadana, telecomunicaciones y sociedad de la información, etc. Al mismo tiempo, se recogen las normas europeas e hispanoamericanas más relevantes de protección de datos.

La obra contiene también un conjunto de Sentencias del Tribunal Constitucional y de la Audiencia Nacional, que constituyen buena muestra de la jurisprudencia de protección de datos personales en nuestro país. Si una excepción fundamental al principio de consentimiento en el tratamiento de los datos personales es la existencia de una previsión legal que así lo establezca, es de gran utilidad disponer de una recopilación de las referencias legislativas relativas a esta cuestión. De todos los proyectos de la APDCM que han contribuido a impulsar la concienciación de la importancia de este derecho fundamental, quisiera destacar la revista digital de la Agencia datospersonales.org, nacida en marzo de 2003, continúa publicándose

en la actualidad, superando los 6000 y llegando a las 70.000 páginas vistas por mes. De periodicidad bimensual, la revista se ha consolidado como un instrumento riguroso y práctico de difusión del conocimiento en materia de protección de datos personales, habiéndose convertido en la publicación digital de referencia en lengua española sobre este derecho fundamental, siendo la primera revista científica en este ámbito. La revista trata de analizar aquellas novedades en comunicaciones y tecnologías de la información que pueden mejorar la seguridad y la confidencialidad de los datos personales. La perspectiva abarca tanto la Unión Europea como nuestro país, con una especial atención a la actividad desarrollada por la APDCM.

La revista cuenta en el menú de navegación con las siguientes secciones: "La Opinión de los Expertos", consistente en artículos doctrinales sobre las materias antes descritas; "Actualidad Normativa", que contiene comentarios de la regulación aprobada en España y en la Unión Europea; "Jurisprudencia", donde se comentan Sentencias de actualidad; "Informes de la APDCM", donde se dan a conocer los criterios interpretativos de la Agencia en el ámbito de sus competencias; "Noticias de la APDCM", en la que se comentan acontecimientos relativos a la vida de la Agencia y a su actividad; "Temas de Actualidad", que consiste en noticias relativas a temas de protección de datos, telecomunicaciones, etcétera; y "Cuestiones Prácticas", que bajo el formato de FAQ's trata de resolver las preguntas más frecuentes, donde contamos con la colaboración de despachos profesionales.

La revista dispone también de un menú de servicios que permite no sólo buscar números anteriores o artículos concretos, sino también enviar artículos de opinión a través de la Tribuna Abierta, anunciar jornadas y eventos o hacer sugerencias, dándole mayor interactividad. Quisiera destacar la creación de un "Foro", como nuevo canal donde los suscriptores de la revista pueden plantear consultas e intercambiar opiniones sobre protección de datos.[26] En general, la personalidad gráfica de la revista —look & feel— está centrada en materializar que la protección de datos no es sólo un ordenamiento jurídico, sino un derecho fundamental que afecta a personas.[27]

[26] La Revista incluye el Aviso Legal de la página así como la Política de Privacidad por la que se rige el sitio web.

[27] En lo que hace referencia a la arquitectura técnica de la revista, quiero destacar la mejora de

En el año 2007 se pone en marcha un nuevo proyecto: la Revista Española de Protección de Datos (REPD), que dirige la APDCM y que edita Thomson-Civitas. Las tecnologías de la información y la comunicación están transformando las empresas y las Administraciones Públicas, acelerando los procesos de globalización y las transferencias internacionales de información. Este desarrollo de nuevas tecnologías afecta específicamente a la vida y a la libertad de las personas, tanto en su vertiente individual como social. Nos encontramos, por tanto, ante una sociedad en transición hacia un mundo distinto, lo que debe acentuar nuestra reflexión. Por ello, la protección de datos personales preserva la capacidad de decisión del individuo y su autonomía personal, y le rodea de una mínima calidad de vida, especialmente en relación con los menores y su libre desarrollo de la personalidad. No obstante, hay que hacer hincapié en que la protección de los datos personales, si bien tiene como beneficiario directo a la persona interesada, no es algo que concierna al sujeto individual, sino que afecta a la sociedad en su conjunto. Hay que superar una concepción individualista de este derecho, para reflexionar sobre cómo la protección de datos personales concierne no sólo al ciudadano, sino a todos como sujetos políticos de una sociedad libre y, por tanto, atañe a la calidad de nuestra democracia. La protección de datos personales afecta también al principio democrático, en cuanto al establecimiento de modelos de democracia y participación electrónica, en la definición de información que debe suministrarse al Parlamento o al uso —o abuso— de los registros de población por los distintos gobiernos, para llevar a cabo una actividad de difícil deslinde entre la comunicación institucional y la pura política.

La Revista Española de Protección de Datos quiere ser una revista preferentemente jurídica, que estudie el ordenamiento de protección de datos personales y que enjuicie la actividad de los poderes públicos y de los particulares. No obstante, la protección de datos personales es un ámbito donde están presentes y entran en conflicto intereses

la rapidez de descarga a través de la reconfiguración de los procedimientos de almacenamiento temporal de las páginas. Se ha procedido también al desarrollo informático de los nuevos canales, se ha previsto la habilitación de la administración remota de los foros a través de certificados electrónicos personales y se ha establecido la posibilidad de descarga e impresión en formato pdf de algunos artículos. Igualmente se ha elaborado el procedimiento de gestión de la revista digital que regula su elaboración y difusión. En la Memoria de la Agencia se han incluido los principales parámetros de análisis de la revista -cuadro de evolución semanal de nuevos suscriptores y páginas vistas al mes, así como las secciones más visitadas-.

y valores, donde se observan los problemas que plantea proteger ámbitos de libertad informática, al tiempo que se permite la actividad de las Administraciones Públicas y de las empresas. Por ello, la Revista no quiere cerrarse en el análisis "lege lata", sino que quiere estar atenta a las demandas de la sociedad en este ámbito, aportando propuestas de "lege ferenda" y ofreciendo a los Tribunales criterios de interpretación de las normas jurídicas que tengan en cuenta la eficacia de las distintas soluciones.

La promoción del derecho fundamental a la protección de datos personales entre los ciudadanos

Una de las funciones más importantes de la Agencia es dar a conocer entre los ciudadanos la existencia y la importancia del derecho fundamental a la protección de datos personales. La función ha sido desarrollada a través de varias actuaciones: En primer lugar, la Agencia ha respondido a consultas a través del servicio de atención al ciudadano, auténtico canal individual para el ciudadano que desea conocer mejor los principios y derechos de protección de datos que le concede la legislación.[28] En segundo lugar, la Agencia ha distribuido durante los últimos años decálogos de derechos de los ciudadanos y carteles que les informan sobre su derecho fundamental a controlar su información personal, sobre el principio de calidad, sobre el principio de información, o sobre el derecho de acceso a sus datos personales.[29]

En tercer lugar, la Agencia ha intensificado su relación con el ámbito educativo, tanto a nivel escolar como universitario. Así, la Agencia elaboró un "Cuaderno Informativo sobre Protección de Datos para Escolares" que trata de ser una aproximación a esta materia orientada y dirigida a menores, quienes, en muchas ocasiones, ceden sus datos personales y deben ser conscientes de su valor, y de que un uso o cesión abusiva puede afectar a su intimidad personal y familiar. La Agencia ha mantenido una estrecha relación con las Universidades

[28] Durante el año 2010 la Agencia ha respondido un total de 1800 consultas.

[29] Dentro del esfuerzo por dar a conocer la Agencia, en el año 2002 se modificó su logotipo, adaptándolo a una Comunidad de interior, para que simbolizase también -con la referencia al papel, al CD y al disquete tradicional- las distintas formas en que pueden registrarse datos de carácter personal.

Públicas y Privadas de la Comunidad de Madrid, permitiendo que sus estudiantes hagan las prácticas en la sede de la Agencia. En cuarto lugar, la Agencia ha aprobado su Carta de Servicios —que se encuentra en su segunda edición—, una buena muestra de la preocupación por acercar esta Administración a los ciudadanos y mejorar el grado de satisfacción por el servicio público que ofrecemos. Además de informar a los ciudadanos de los servicios que prestamos, en la Carta se establecen objetivos de calidad, indicadores para la medición de estos objetivos y un sistema de sugerencias y reclamaciones.[30]

Sólo nos queda esperar que el esfuerzo que hace la APDCM, y que de manera resumida se ve reflejado en este estudio, sirva para que los responsables puedan ver la tutela del derecho a la autodeterminación informativa no como una carga a soportar, sino como un valioso instrumento y una oportunidad para ofrecer cada día a los ciudadanos servicios públicos de mayor calidad, en los que se hace compatible la eficacia administrativa y el respeto a los derechos. La situación de las Administraciones Públicas de la Comunidad de Madrid respecto al cumplimiento de la legislación de protección de datos es positiva. Sin embargo, esto no debe llevarnos a una situación de complacencia por lo conseguido, sino que tiene que ser un acicate para seguir trabajando aún más, de manera que el hecho diferencial de nuestra Comunidad Autónoma sea el servicio a los ciudadanos y la protección de los derechos, en este caso, de la libertad informática y del derecho a la intimidad.

Referencias

Agencia de Protección de Datos de la Comunidad de Madrid (2010) *Repertorio de legislación y jurisprudencia sobre protección de datos*. Presentación, Santiago Abascal Conde. Editorial Civitas-Thomson Reuters, 2010.

Agencia de Protección de Datos de la Comunidad de Madrid (2004) *Guía de Protección de datos personales para Ayuntamientos* Civitas. Madrid 2004.

Agencia de Protección de Datos de la Comunidad de Madrid (2011) *Memoria de las actividades realizadas en la Agencia de Protección de Datos de la Comunidad de*

[30] En los últimos años la Agencia ha editado más de 20.000 Cartas de Servicios,

Madrid durante el año 2010, disponible al 11 de diciembre de 2011 en www.apdcm.es, canal "Publicaciones".

Davara, M.R (2003) *La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos*, XVII Encuentros sobre Informática y Derecho, Universidad Pontificia de Comillas, Madrid.

Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid, disponible al 12 de diciembre en.http://www.madrid.org/cs/Satellite?cid=1247227037983&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_contenidoFinal.

Recomendación 3/2008 de la Agencia de Protección de datos de la Comunidad de Madrid, de 30 de abril, sobre tratamiento de datos de carácter personal en servicios de administración electrónica. Disponible al 10 de diciembre de 2011 en http://www.madrid.org/cs/Satellite?cid=1247227049662&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado#a1142575940641.

Colección Guías de Protección de Datos, disponible al 12 de diciembre de 2011 en el sitio web de la Agencia www.apdcm.es, canal "Publicaciones".

Reigada A. Troncoso (2005) *Las Comunidades Autónomas y la protección de datos personales: marco constitucional y posibilidades para el futuro*, en Revista Parlamentaria de la Asamblea de Madrid, núm. 12.

Reglamento de desarrollo de las funciones de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal, disponible al 12 de diciembre de 2011 en http://www.madrid.org/cs/Satellite?cid=1247227049662&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_listado#a1142575940340.

Convergencias y divergencias: Acceso a la Información y la tutela de los datos personales

Miguel Pulido Jiménez

Miguel Pulido Jiménez

Director Ejecutivo de Fundar, Centro de Análisis e Investigación A.C., es catedrático de Derecho de la Información en la Universidad Iberoamericana. En el ámbito docente ha sido profesor de los servicios profesionales de la Secretaría de Gobernación y de la Comisión de Derechos Humanos del Distrito Federal. También ha impartido múltiples diplomados y cursos sobre el tema de transparencia y acceso a la información en distintas instituciones. Es autor de diversos ensayos entre los que destaca "Construir Obra Pública, Edificar Ciudadanía", su más reciente publicación.

Licenciado en Derecho por el Instituto Tecnológico y de Estudios Superiores de Monterrey (Campus Monterrey). Se especializó en Derechos Humanos y Procesos de Democratización en la Facultad de Derecho de la Universidad de Chile. Cursó estudios de posgrado en la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM).

Introducción

En los últimos 10 años en México se ha dado un rápido desarrollo normativo en materia de acceso y control de la información en poder del Estado. El primer avance se dio con la regulación del derecho de acceso a la información pública gubernamental (DAI). Desde 2002, nuestro régimen de acceso a la información ha desarrollado 32 leyes locales, 1 ley federal y una reforma al artículo 6 de la Constitución que incorpora de manera detallada el DAI, al régimen constitucional, en una dimensión que tradicionalmente se asocia el derecho a saber o la transparencia.

Pero existe otra cara del acceso a la información (principalmente en poder del Estado): aquel que regula la posibilidad de conocer y controlar la que es de carácter personal, que nos pertenece, pero que está bajo custodia y tratamiento de un tercero. Es cierto que algunas de las legislaciones de transparencia previeron desde el inicio regulaciones en materia de protección y tutela de los datos personales en poder de los órganos de Estado, sin embargo, los hitos en esta materia los tenemos a partir de dos reformas a artículos de la Constitución, al artículo 6 (en 2007) y al artículo 16 (en 2009).

Con el contenido del presente artículo precisamente se busca describir los elementos distintivos del derecho de acceso a la información frente a la protección de datos personales (y viceversa). Para ello es pertinente describir, primero, cuáles son las características de cada derecho. Posteriormente se enlistan brevemente las áreas de coincidencia. Por último, se precisan las relaciones recíprocas en términos de alcances y límites, a partir de ejemplos concretos.

Para los fines del presente artículo, se hizo una selección del espectro de análisis como consideración metodológica, pues el espacio disponible no permite abordar en amplitud las condiciones de multiplicidad jurídica mexicana.

Así las cosas, a pesar de que México es un Estado federado y había múltiples experiencias disponibles, se usan como referente el ámbito Federal y en el local, el Distrito Federal.

Derecho de Acceso a la Información Pública

¿Qué entendemos por el derecho de acceso a la información?

El derecho de acceso a la información pública implica que existe una persona titular de la potestad jurídica para solicitar y obtener información pública gubernamental, la cual podemos definir como aquella que los órganos de Estado generan, obtienen, adquieren, transforman o conservan por cualquier motivo, y de forma especial la que documenta el ejercicio de sus facultades o su actividad.[1]

Una vez que la información es producida, procesada o, en ciertos casos, simplemente acopiada, sus tenedores están obligados a administrarla adecuadamente con el fin de que la sociedad disponga de ella. En consecuencia, suele hablarse de acceso a la información pública gubernamental siempre que se trate de la interacción entre personas y una agencia estatal, que tenga por objeto conocer la información generada o depositada en sus archivos por esta última. El acceso a la información admite, por una parte, el derecho a conocerla y, por otra, la obligación del Estado de permitir el acceso a ella (Pulido, 2006).

Evolución normativa

El derecho a la información en México se ha construido principalmente por iniciativas políticas de gran escala. La primera de ellas fue la reforma constitucional de 1977, cuando se incluyó en la Carta Magna la siguiente expresión: "el Derecho a la Información será garantizado por el Estado". Posteriormente, en el año de 2002 se discutió y a la postre se aprobó la Ley Federal de Transparencia y Acceso a la

[1] El artículo 11 de la Ley de Transparencia y Acceso a la Información del Distrito Federal señala: "quienes generen, administren, manejen, archiven o custodien información pública, serán responsables de la conservación de la misma en los términos de esta Ley y de las demás disposiciones aplicables. El ente obligado que, por disposición de la normatividad en materia de archivos, custodie información de otros Entes Obligados, deberá canalizar las solicitudes de información hacia el Ente que generó el documento. Toda la información en poder de los Entes Obligados estará a disposición de las personas, salvo aquella que se considere como información de acceso restringido en sus distintas modalidades".

Información Pública Gubernamental. De ahí, tan sólo en un lapso de 7 años se elaboraron 33 leyes sobre la misma materia, se crearon el mismo número de órganos garantes, se fijaron normas archivísticas y han venido al cauce dos grandes plataformas informáticas de acceso a la información.

Esta tendencia se explica dentro de lo que Ackerman y Sandoval (2006) denominan como la "(e)xplosión global de leyes de acceso a la información". Sin embargo, esto no significa que exista cohesión u homologación normativa, resultado entre otras cosas del régimen federal mexicano.[2]

México es un conformado por 31 entidades federativas y un Distrito Federal. De ahí que actualmente el régimen de acceso a la información sea resultado de una multiplicidad de marcos normativos (un artículo Constitucional, una Ley federal, 32 leyes locales -31 de ellas estatales y 1 para el Distrito Federal-, cientos de Reglamentos y miles de lineamientos administrativos y Decretos) así como de instituciones (al menos 33 órganos garantes, con una diversidad muy amplia de naturalezas jurídicas que recorren desde los órganos de integración honoraria hasta otros con características de autonomía constitucional, cientos de Comités de Información y cientos de Oficinas de Información Pública o Unidades de Enlace).

Sujetos o entes obligados, los protagonistas en la vigencia del DAI

Considero que una primera característica en la que conviene detenerse es en describir qué se entiende por "sujeto obligado". Para ello podemos encontrar al menos tres fuentes principales en el marco normativo.

La primera es la más reciente, y la encontramos a partir de la reforma constitucional de 2007, en el artículo 6º constitucional, el cuál prevé lo siguiente:

[2] Evidencia de esto puede encontrarse en el Índice del Derecho de Acceso a la Información en México (IDAIM), Resultados de la Medición. Disponible en http://www.checatuley.org/resultados.pdf.

> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por lo siguientes principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes.

Es decir, desde el prisma constitucional, es la naturaleza pública de las instancias y agencias de Estado en su sentido más amplio, la que las hace sujetas el ejercicio del derecho de acceso a la información y por consecuencia les da el carácter de sujetos obligados.

En el ámbito estrictamente federal, encontramos dos fundamentos adicionales. El primero es el artículo 13, fracción XIV, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIP) que expresamente identifica como sujetos obligados a los siguientes:

> a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República
>
> b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos
>
> c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;
>
> d) Los órganos constitucionales autónomos
>
> d) Los tribunales administrativos federales y
>
> f) Cualquier otro órgano federal

No obstante, sólo los previstos en el inciso a) son sujetos obligados en términos lisos y llanos. Es decir, están bajo el imperio del Instituto Federal de Acceso a la Información y Protección de Datos y su conducta se rigen directamente por la Ley Federal de Transparencia. De hecho,

así es como nos aproximamos al segundo fundamento para identificar sujetos obligados de la Ley pero tutelados por instancias distintas, pues el artículo 61 establece que:

> El Poder Legislativo Federal, a través de la Cámara de Senadores, la Cámara de Diputados, la Comisión Permanente y la Auditoría Superior de la Federación; el Poder Judicial de la Federación a través de la Suprema Corte de Justicia de la Nación, del Consejo de la Judicatura Federal y de la Comisión de Administración del Tribunal Federal Electoral, los órganos constitucionales autónomos y los tribunales administrativos, en el ámbito de sus respectivas competencias, establecerán mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios establecidos en esta Ley.

La última fuente normativa de referencia para identificar a los sujetos obligados se conforma por las legislaciones estatales y la del Distrito Federal. Los casos son de lo más diverso, pero en términos generales podemos decir que incluyen al ejecutivo, legislativo y judicial, así como las siguientes instituciones públicas 1) el órgano de fiscalización superior federal o del estado; 2) el tribunal electoral; 3) los tribunales administrativos; 4) los organismos públicos autónomos; 5) el instituto electoral local; 6) las comisiones de derechos humanos locales; 7) las universidades e instituciones de educación superior públicas; 8) las juntas de conciliación y arbitraje; y 9) los ayuntamientos.

En el caso específico del Distrito Federal, de acuerdo al artículo 4 de la Ley de Transparencia y Acceso a la Información del Distrito Federal se consideran entes obligados los siguientes:

> La Asamblea Legislativa del Distrito Federal; la Contaduría Mayor de Hacienda de la Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; el Tribunal de lo Contencioso Administrativo del Distrito Federal; el Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; los órganos

> autónomos por ley; la Jefatura de Gobierno del Distrito Federal; las dependencias; los órganos desconcentrados; los órganos político administrativos; los fideicomisos y fondos públicos y demás entidades de la administración pública; los partidos políticos; aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público;

El punto central de esta referencia es subrayar que el criterio relevante para identificar lo que debe entenderse por sujeto o ente obligado está directamente relacionado con la naturaleza pública de la instancia que posee o detenta la información, más no a sus funciones. Este paradigma permite que muchos actores salgan de la esfera de acción y obligación propia de un sujeto obligado, sin importar la relevancia de la información que posean. Dicho de otra forma, en México no son considerados como sujetos obligados, las empresas y organismos privados que tienen una relación con el Estado desde el punto de vista concesionario, accionario y regulatorio. Por ejemplo, el uso adecuado de concesiones de agua potable, o la exploración y explotación de minerales o cualquier privado que brinde servicios públicos, está fuera del alcance directo de las leyes de transparencia. Más adelante veremos que en oposición, la protección de datos personales en México sí ha previsto la regulación de los particulares.

Órganos de control. Guardianes del derecho, promotores de la apertura

El IFAI tiene como mandato el "promover y difundir el ejercicio del derecho de acceso a la información; resolver la negativa a las solicitudes de acceso a la información; y proteger los datos personales en poder de las dependencias y entidades" (artículo 33 de la LFTAIPG). Por su parte, el InfoDF tiene por mandato "dirigir y vigilar el cumplimiento de la (…) Ley y las normas que de ella deriven, así como de velar porque los principios de certeza, legalidad, independencia, imparcialidad y objetividad imperen en todas sus decisiones. En el marco de sus atribuciones, el Instituto se regirá por los principios de austeridad,

racionalidad y transparencia en el ejercicio de su presupuesto". (Artículo 63 LTAIPDF). Una esquematización de las funciones principales derivadas de ambos mandatos legales (sólo en materia de acceso a la información), puede ser la siguiente:

1. Funciones resolutivas y reguladoras. Tanto el InfoDF como el IFAI conocen de los recursos de revisión y de las controversias respecto a la interpretación de la Ley, función que deberá realizar con apego a lo establecido en la Constitución y los tratados internacionales.

2. Funciones de vigilancia para impulsar el cumplimiento de las leyes de transparencia, en sus ámbitos de competencia.

3. Función de promoción para fomentar y difundir los beneficios del derecho de acceso a la información pública gubernamental e impulsar una cultura de transparencia y rendición de cuentas.

4. Por último, funciones operativas y administrativas que son necesarias para la buena operación de los institutos y asegurar el cumplimiento de sus demás funciones.

Derecho a la protección de los datos personales

¿Qué entendemos por el derecho a la protección de los Datos Personales?

Se trata de la protección jurídica con la que cuentan las personas respecto a la recopilación, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre cierta información personal con características particulares a la que se le han llamado datos personales. Por datos personales suele entenderse la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable entre otros, la relativa a su origen racial o étnico, las características físicas, morales o emocionales a su vida afectiva y familiar, información genética, número de seguridad social, la huella digital, domicilio y teléfonos particulares, preferencias sexuales, estado de salud físico

o mental, correos electrónicos personales, claves informáticas, cibernéticas, códigos personales; creencias o convicciones religiosas, filosóficas y morales u otras análogas que afecten su intimidad.[3]

Evolución normativa

Como se dijo líneas arriba, desde la promulgación de las leyes de transparencia se incorporó al marco normativo mexicano una laxa protección y tutela de los datos personales. Sin embargo, fue a partir de la reforma constitucional del artículo 6º cuando se estableció el mandato expreso de legislar en la materia y se precisó su fuente constitucional.

> El artículo 6 constitucional establece:
> Para el ejercicio del derecho de acceso a la información, la Federación, los estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
> (…)
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Posteriormente, se reformó el artículo 16 de la Constitución incluyendo expresamente el derecho a la protección de los datos personales. El artículo constitucional incorporó el siguiente texto:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismo, así como a manifestar 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 públicas o para proteger los derechos de terceros.[4]

[3] Ver artículo 4.

[4] Adicionado mediante decreto publicado en el DOF el 1 de junio de 2009. El texto puede consultarse aquí: http://info4.juridicas.unam.mx/ijure/fed/9/17.htm.

Ambos antecedentes constitucionales son importantes. En el caso del Distrito Federal, en cumplimiento de la modificación al artículo 6º constitucional, el 3 de octubre de 2008 se aprobó la Ley de Protección de Datos Personales para el Distrito Federal.

En el caso federal, a la luz del artículo transitorio tercero de la reforma al artículo 16 se aprobó una Ley Federal de Protección de Datos Personales en Posesión de Particulares. Éste marco normativo se complementa con el contenido de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental que contiene diversos apartados orientados a la tutela de los datos personales, pero en poder de entes públicos.

En suma, como se aprecia el marco normativo en materia de protección de datos personales también tuvo sus primeras expresiones en legislación secundaria, posteriormente reformas constitucionales especificaron de mejor forma su alcance y por último estas reformas tuvieron un nuevo impacto en la creación o modificación de legislación secundaria. Tanto en este caso, como en el del acceso a la información, se trató de relaciones pendulares.

Sujetos o entes regulados. El delicado mandato del autocontrol

Al igual que en el caso del acceso a la información, tenemos distintas fuentes de interpretación sobre quiénes son los sujetos obligados y cuál es la implicación de serlo. La primera es la constitucional, y del contenido de los artículos arriba referidos puede desprenderse que, en realidad, se trata de una tutela amplía que, por principio, pone el énfasis en el derecho de las personas a proteger su información y datos personales y no frente a quién es oponible. El énfasis constitucional, en este caso está en el sujeto activo del derecho, a quien se define con amplio detalle.

La segunda fuente es la legislación específica. En este caso, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la cual es de orden público y de observancia general en toda la República. La propia Ley reconoce como finalidad el regular el "tratamiento legítimo, controlado e informado (de los datos) a efecto de garantizar

la privacidad y el derecho a la autodeterminación informativa de las personas".

A la luz de esta Ley, podemos identificar como sujetos regulados a los particulares (no importa si son personas físicas o morales) de carácter privado que lleven a cabo el tratamiento de datos personales. Es importante aclarar que en tanto que ya existe una legislación particular para las sociedades de información crediticia (bancos y buros de crédito) la ley expresamente señala en el artículo 2 que no serán de su ámbito de aplicación. Sobre este tema no abundamos por su alta especificidad.

La tercer fuente para identificar a los entes regulados en materia de datos personales son las legislaciones especiales de protección de datos personales en poder de instancias públicas. Es el caso del Distrito Federal y la Ley de Protección de Datos para el Distrito Federal, la cual prevé en el artículo 2 que son entes públicos:

> La Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público.

Lo importante de la identificación de estos entes o sujetos regulados es establecer que sobre ellos pesa un estándar de comportamiento y obligaciones específicas[5] para el tratamiento de los datos basados en

[5] El artículo 13 de la Ley de Protección de Datos para el Distrito Federal establece que: los

principios. Estos principios son la licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

El órgano de control. Guardianes de la privacidad

En el caso Federal, a partir de 2010, las funciones (y el nombre del Instituto Federal de Acceso a la Información Pública) cambiaron, ampliándose su mandato en materia de datos personales, como resultado de la aprobación de la Ley Federal de Protección de Datos Personales.

A grandes rasgos las características de la intervención institucional del IFAI serán (a partir de enero de 2012) las siguientes:

- El Instituto será la autoridad garante en materia de protección de datos. En este sentido vigilará a los sujetos regulados, podrá además realizar estrategias de intervención preventiva y resolverá las controversias en la materia.

- El IFAI garantizará la no injerencia arbitraria o ilegal en la vida privada de las personas, provocada por el mal uso de los datos personales, tal como está previsto en el artículo 16 de la Constitución.

- El IFAI estará facultado para imponer infracciones y sanciones a quienes hagan mal uso de los datos personales que obren en sus bases de datos o en su poder. Podrá, además, realizar actividades de capacitación así como establecer estándares de seguridad. En el aspecto contencioso atenderá quejas, llevará a cabo procesos conciliatorios, inspecciones sobre el manejo

entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad al tipo de datos contenidos en dichos sistemas. Dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro. Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el ente público otorgó el tratamiento del sistema de datos personales.

de las bases de datos y en los casos en los que detecté el incumplimiento de la normatividad, emitirá sanciones.[6]

En el caso del Distrito Federal, las atribuciones del InfoDF se pueden agrupar en las siguientes categorías:

- Cuenta con facultades regulatorias, para establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley.

- Puede normar los procedimientos para realizar solicitudes de ejercicio de los derechos ARCO, así como determinar las medidas de seguridad para los sistemas de datos personales.

- Cuenta con atribuciones diversas a la de solución de controversias como consulta, de opinión, para formular observaciones y recomendaciones a los entes públicos y para orientar y asesorar a las personas. También facultades de divulgación y promoción, lo que incluye la realización de estudios, organizar seminarios y otras actividades para promover el conocimiento de la Ley.

Encuentros y desencuentros. La relación entre ambos derechos

Tomando en cuenta lo expuesto, es posible establecer algunas líneas de relación entre ambos sistemas normativos y derechos. Una primera categoría de interacción se da en términos de identidad a propósito de la normatividad que los regulan y los órganos que los tutelan. Otro espacio de convergencia se refiere a los sujetos involucrados en la vigencia de ambos derechos y por último revisaremos las intersecciones que surgen cuando hay colisión entre las normas, o cuando los sistemas normativos funcionan como límites recíprocamente.

[6] Documentos y herramientas que explican el papel del IFAI en la protección de los datos personales están disponibles en: http://www.ifai.org.mx/Particulares/faq.

Casos en los que se comparten esferas

El derecho de acceso a la información pública gubernamental y la protección de datos personales son dos expresiones de un mismo fenómeno: el derecho a conocer y acceder información que está en poder de terceros, de forma preponderante, la que se encuentra en poder de los órganos de Estado. En un caso se trata del derecho de conocer la información pública con la intención de transparentar y abrir lo que sucede en le gobierno, mientras que en otro se trata del derecho a conocer la información propia y de asegurarse que dicha información no saldrá a la luz pública de forma indebida.

A la luz de lo anterior, una primera categoría de interacción se da cuando ambos sistemas comparten la normatividad que los regula, los entes o sujetos que son regulados o que están obligados por la norma y los órganos que garantizan el derecho. Este es el caso de los datos personales en posesión de dependencias del gobierno federal y el acceso a la información en el mismo ámbito. En este caso, el órgano garante y responsable de la interpretación de ambos derechos es el IFAI y la Ley, para ambos casos, es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Los sujetos obligados son los señalados por dicha ley y que fueron explicados con detalle en el apartado II.3 de este mismo artículo.[7]

En el caso del Distrito Federal, en cambio, hay identidad en el órgano garante y en los entes obligados, sin embargo, existen dos marcos normativos plenamente diferenciados en términos de objeto de tutela, por una parte, la Ley de Transparencia y Acceso a la Información del Distrito Federal y, por otra, la Ley de Protección de Datos Personales para el Distrito Federal. Sin embargo, a pesar de que la fuente normativa es distinta, lo cierto es que los entes regulados (en materia de datos personales) y los entes obligados (en materia de acceso a la información) son los mismos, por lo que existe una identidad de actores.

[7] Es importante señalar que desde hace varios años está pendiente una reforma a la LFTAIPG. En los dictámenes que se discuten en la Cámara de Diputados (uno de ellos ya aprobado en la Cámara de Senadores) se incluye una prueba de daño y una prueba de interés público.

En lo que hace a la tutela de la protección de datos personales en poder de agentes privados, el IFAI también es el órgano regulador de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. En éste caso, al no existir un derecho de acceso a documentos públicos en poder de particulares (o alguna otra consideración similar) debe descartarse automáticamente la idea de duplicidad de funciones de tutela. Sumado a ello, debe anotarse ya una primera diferencia sustancial entre ambos derechos. El derecho a la protección de datos personales sí opera sobre los datos en posesión de particulares mientras que en el derecho de acceso a la información pública, sólo son sujetos obligados entes públicos, nunca los de carácter privado.

Divergencias entre derechos

La primera diferencia sustancial entre ambos derechos deriva de la naturaleza de cada uno de ellos, así como de su propia genealogía jurídica. Mientras el derecho de acceso a la información es un derecho fundamental de carácter civil y político (en el ámbito internacional de los derechos humanos se le ha ligado a la libertad de expresión y en el caso mexicano incluso se ha reconocido como parte del derecho al voto), el derecho a la protección de los datos personales, es un derecho de personalidad y directamente relacionado con los derechos de fuente patrimonial. Una segunda diferencia sustancial, deriva del fundamento teleológico de cada uno de estos derechos. Como se dijo líneas arriba, el derecho de acceso a la información está alineado a los objetivos fundamentales del republicanismo, con él se busca involucrar a la ciudadanía en los asuntos públicos y parte de la consideración de que el ejercicio del poder es de carácter temporal y delegativo (es decir, se hace en nombre de otros) por lo que la información con la que se trabaja le pertenece a la sociedad.

En oposición, el derecho a la protección de los datos personales está directamente vinculado a la noción de privacidad, a la defensa de la vida privada y a asegurar que las personas puedan controlar la información que les pertenece y que está en poder de otros sujetos.

La tercera categoría de diferencias deriva del sentido técnico de interpretación que corresponde a cada derecho. El derecho de acceso

a la información debe seguir guías de interpretación hermenéuticas orientadas a establecer el interés público y en aplicar el principio de máxima publicidad.

Esto tiene implicaciones prácticas y sencillas, tanto los sujetos obligados como los órganos de tutela deben obedecer el mandato de optimización fáctica y jurídica para que la mayor cantidad de información en poder de las dependencias públicas sea conocida.

En los casos en los que la información pública y otras categorías de información colisionen, deberán hacerse ejercicios de ponderación y demostrarse (por la vía de la prueba del daño) que la divulgación de la información causa un daño mayor al beneficio de su conocimiento.

En cambio, en la protección de los datos personales se debe acudir a criterios distintos, aquellos que sirven en la búsqueda de la interpretación más extensiva para un derecho protegido.

El principio *pro homine* adquiere una relevancia particular en tanto las restricciones para el tratamiento de los datos, la proporcionalidad de su procesamiento o la necesidad de garantizar la seguridad de su uso deberán ser siempre leídas a la luz de la mayor protección posible en beneficio de la persona titular del derecho.

La interpretación en materia de protección de datos personales deberá asegurar que no existen intervenciones indebidas o ilegales y que, en todo caso, las personas tienen control sobre su propia información, sin importar si ésta se encuentra en poder de sujetos públicos o privados.

Colisión de derechos. Algunas lecciones a la luz de casos prácticos

Debido a su reciente emergencia, positivación y desarrollo institucional, al momento no existen en México mecanismos explícitos para la solución de conflictos entre ambos derechos. Es poca la actividad jurisdiccional en la materia y las reformas constitucionales aún no han sido interpretadas. Sin embargo, la práctica ha originado algunos criterios, en la mayoría de los casos siguiendo reglas de aplicación que resuelven parcialmente las tensiones entre normas. Por ejemplo,

desde la aplicación de la Ley Federal de Transparencia y Acceso a la Información, el IFAI ha resuelto las fronteras entre derechos.

Los casos han sido moderadamente fáciles, pues han consistido en aplicar, por ejemplo, el artículo 12 de la Ley de Transparencia que prevé expresamente que la información concerniente a las personas que reciban recursos públicos, es pública.

Destacan, por ejemplo, casos sobre los nombres de beneficiarios de programas sociales y el acceso a los padrones que contienen información personal, pero que a la luz del artículo 12, existen las condiciones de legalidad y licitud para divulgarla. El caso del recurso de revisión 2431/09, tramitado ante el IFAI, sobre el acceso a los nombres de beneficiarios del Seguro Popular es uno de los más destacados en el que la discusión en el pleno versó sobre el equilibrio entre acceso a la información y protección de datos personales.[8] La lección del caso es que, a pesar de que una norma ordene la legalidad de la divulgación de los datos, las dependencias pueden hacer ejercicios de ponderación para determinar cuánta información es relevante publicar desde la perspectiva del acceso a la información.

Otros casos relevantes han sido sobre los datos personales de los servidores públicos. Estos fueron de los primeros casos resueltos por el IFAI y la interpretación hoy día es compartida por el IndoDF en el sentido de divulgar la información. Como ejemplo está el recurso de revisión 129 sobre la Cédula profesional de los mandos altos y medios de la SSP y PFP con relación del puesto desempeñado. La Secretaría de Seguridad Pública originalmente clasificó la información argumentando que era confidencial, porque afecta la vida privada y la intimidad de las personas. No obstante, el IFAI revocó la resolución instruyendo que se entregara la información, en caso de obrar en sus archivos. La segunda lección, a la que quiero hacer referencia, es que es posible aplicar el estándar de publicidad de la información de las y los servidores públicos, frente a un estándar de protección de la misma información, en el caso de los particulares.

[8] Lo recuperado por la prensa se puede consultar en la siguiente liga: http://www.jornada.unam.mx/2009/07/16/sociedad/037n1soc.

El tercer tipo de casos son una mezcla de condiciones especiales en las que personas desempeñan actividades que no siendo de carácter particular, tienen una relevancia pública. Como ejemplo podemos citar la controversia respecto al derecho a conocer las actas de asamblea del Consejo Consultivo de la Comisión Nacional de los Derechos Humanos.[9] En ese caso el juez resolvió que dado que "los miembros del consejo de la CNDH desempeñan una función pública dentro de un organismo público, cuyas facultades se encuentran plenamente definidas", y que la información solicitada "se relaciona con una reunión de interés público", "la negativa a proporcionar esos datos viola la garantía de acceso a la información pública." Aquí, la lección aprendida está directamente relacionada con el impacto pretendido y conscientemente asumido de las conductas realizadas por las personas. El carácter público de las actas deriva de su condición de documento público, el de los datos personales ahí contenidos, del tipo de actividad desempeñada por los consejeros.

La cuarta y última lección aprendida, deriva del contexto particular en el que vivimos y de la crisis de inseguridad pública. Ante la compleja situación que enfrentamos, diversas autoridades responsables de la seguridad pública y de la procuración justicia, han considerado que la exposición y exhibición de personas presuntamente responsables de delitos ante medios de comunicación es una medida que muestra a la sociedad el trabajo en el combate del delito y que existe un interés público en conocer la capacidad de acción del Estado en la lucha contra la delincuencia, particularmente la organizada. Es el caso de las quejas presentadas ante el InfoDF en las que personas alegan la violación a la protección de datos personales, al ser exhibidos frente a medios de comunicación.

En estos casos el marco normativo es explícito, las autoridades deben respetar el principio de licitud (no pueden tratar los datos personales en sentido opuesto a una restricción legalmente prevista y las investigaciones de delitos son por ley reservadas), el de proporcionalidad (deben usar los datos sólo para los fines para los cuáles fueron recabados, en este caso la investigación, no mostrar a la sociedad el trabajo de la autoridad), así como los de consentimiento

[9] Referencias de prensa pueden ser consultadas aquí: http://www.jornada.unam.mx/2007/10/12/index.php?section=politica&article=025n2pol.

y responsabilidad (los impactos negativos de la exhibición de las personas trastocan la vida de terceros y esto no se tiene en cuenta).

Sin embargo, a la fecha los casos han sido resueltos en sentido opuesto alegando que de la aplicación del principio de máxima publicidad y la prueba de interés público, resulta legal la revelación de la información personal. Lo que no toma en cuenta este razonamiento es que no existe colisión de derechos cuando una persona hace valer un interés jurídico tutelado (además bajo el principio pro homine), como el da la protección de datos personales, frente a consideraciones o posiciones en beneficio de las autoridades.[10]

Debe recordarse que los derechos fundamentales son de las personas y no de las autoridades y aunque la colisión de derechos en efecto podría existir (si una persona solicitara acceso a la información y alguien más pretendiera ejercer el derecho a la tutela de los datos personales), no abundo más porque no es el caso.

Por último, dado que no comparto el sentido de las resoluciones, desde mi perspectiva la lección del caso es que la aplicación de las pruebas de interés público y máxima publicidad no corresponden a la solución de casos centrados en la protección de datos personales y tampoco rompen los principios de licitud o de proporcionalidad.

Conclusión

Los derechos a la protección de los datos personales y al acceso a la información pública gubernamental comparten, entre otras cosas, identidad de actores, fuentes normativas y órganos garantes. No obstante, se trata de dos derechos provenientes de tradiciones jurídicas diversas, con implicaciones prácticas distintas y con posibilidades de colisión muy amplias.

Para la solución de los casos de enfrentamiento entre derechos, el marco normativo (tanto el constitucional como el legal) hoy día permite realizar ejercicios de ponderación y de aplicación de reglas

[10] Más información sobre el caso particular se puede consultar aquí: http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1085&Itemid=217 Y aquí: http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1087&Itemid=217.

explícitas para la protección de datos personales. En sentido contrario, los principios constitucionales también permiten encontrar soluciones en las que la divulgación de datos personales, sea posible sin causar lesiones jurídicas que las personas no deban soportar y siempre que existan razones de interés público. Pero en todo caso, lo más relevante es que la relación entre estos derechos es un proceso en construcción. Gracias a las normas, principios y reglas con las que contamos esta puede ser una relación armónica, que ponga siempre en balance la protección de las personas y el interés público.

Referencias

Ackerman, John y Sandoval, Irma Eréndira (2006) *Global Explosion of Freedom Information Laws*, Administrative Law Review, 58-1.

Pulido, Miguel. (2006) *El derecho de acceso a la información es un derecho humano*. Fundar, Centro de Análisis e Investigación, disponible al 14 de diciembre de 2011 en: http://es.scribd.com/FundarMx.

Comisión de Derechos Humanos del Distrito Federal (2008) *Diagnóstico de Derechos Humanos del Distrito Federal*, Varios, disponible al 14 de diciembre de 2011 en: http://www.derechoshumanosdf.org.

Diario Oficial de la Federación del 1 de junio de 2009. Texto disponible al 12 de diciembre en http://info4.juridicas.unam.mx/ijure/fed/9/17.htm.

Índice del Derecho de Acceso a la Información en México (IDAIM), Resultados de la Medición. Disponible al 13 de diciembre en http://www.checatuley.org/resultados.pdf.

Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales, documentos sobre protección de los datos personales, disponibles al 13 de diciembre en http://www.ifai.org.mx/Particulares/faq.

Las legislaciones de protección de datos personales en el país

Oscar M. Guerra Ford

Oscar M. Guerra Ford

Comisionado Presidente del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, desde marzo de 2006, y expresidente de la COMAIP. Ha sido Asesor en la Unidad de Coordinación con Entidades Federativas de la Secretaría de Hacienda y Crédito Público, Subdirector en Fundación UNAM, Secretario General de la Facultad de Economía de la UNAM y Profesor de tiempo completo (con licencia) por más de 25 años en la Facultad de Economía de la UNAM y desde 2006 es Comisionado Presidente del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

También ha sido Presidente de la Asociación de Economistas de América Latina y el Caribe, Presidente del Colegio Nacional de Economistas, Secretario Técnico del Consejo Nacional de Acreditación de la Ciencia Económica, Secretario General de la Asociación de Facultades, Escuelas e Institutos de Economía de América Latina.

Maestro en Ciencias Económicas por la Universidad Nacional Autónoma de México. Diplomado en "Principles & Techniques of Found Raising" en Indiana University. Licenciado en Economía por la Universidad Nacional Autónoma de México. Fue reconocido con la distinción "Universidad Nacional para Jóvenes Académicos 2000", en el área de docencia de Ciencias Económico-Administrativas así como con el otorgamiento de Diploma y Medalla de "Reconocimiento al Mérito Universitario" por 25 años de labor académica en la UNAM.

Introducción

Hace diez años, gracias a los trabajos del Grupo Oaxaca, se impulsó de manera decisiva, el derecho de acceso a la información pública en nuestro país. Con esta acción se abrió la puerta al reconocimiento de otro derecho: el de protección de los datos personales. Al proteger la información confidencial en las legislaciones de transparencia que, desde el 2002, fueron creadas, se protegieron los datos personales ante posibles intromisiones de los solicitantes.

Este fuerte vínculo entre el Derecho de Acceso a la Información y el Derecho a la Protección de los Datos Personales se observa en la reforma al artículo 6° constitucional del 2007, al incluir en este artículo la obligación de proteger los datos personales en posesión de las autoridades gubernamentales.

La evolución tecnológica actual ha dejado desprotegido el derecho a la intimidad y a la vida privada de las personas, aunque desde el 2002 se protegían los datos personales en posesión de las autoridades públicas, a través de la figura de "información confidencial", los datos personales en posesión de los particulares no estaban sujetos a tipo de protección alguna. Los datos personales que entregamos a las empresas para acceder a algún bien o servicio podían ser utilizados por ellas de manera indiscriminada. El 1 de junio de 2009, se añadió al artículo 16 de la Constitución Federal un párrafo que estableció el derecho de toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición (derechos ARCO) en los términos que fije la ley.

Al igual que en el derecho de acceso a la información pública, en este caso las entidades federativas se adelantaron a la federación al publicar leyes que protegían de manera especial los datos personales en posesión de las autoridades públicas.

El 21 de junio del 2003 se publicó en el Periódico Oficial "El Estado de Colima" La Ley de Protección de Datos Personales del Estado de Colima; el 23 de Agosto de 2008 se publicó la Ley de Protección de Datos Personales del Estado de Oaxaca y el 4 de octubre de 2008 la Ley de Protección de Datos Personales para el Distrito Federal.

Con el objetivo de realizar un diagnóstico del estado que guarda el derecho a la protección de los datos personales en México el presente trabajo se desarrollará de la siguiente manera: en primer lugar se realizará una revisión del reconocimiento constitucional al derecho a la protección de los datos personales; posteriormente, se presentarán los resultados del análisis comparativo de la normatividad que regula este derecho, para enfatizar algunos de los retos para consolidar este nuevo derecho; finalmente, debido a que el caso del Distrito Federa muestra un claro ejemplo de la preocupación de los ciudadanos por decidir sobre el uso y destino de sus datos, por ello en el apartado V se realizará en breve análisis del estado actual que guarda la protección de los datos personales en el Distrito Federal.

Los datos personales en la Constitución

El artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, reformado el 20 de julio de 2007, adiciona, en su párrafo segundo, los principios y bases por las cuales se regirá el derecho de acceso a la información en la federación, estados y municipios. Concretamente, la fracción II de este artículo instituye la protección de los datos personales en los términos y con las excepciones que fijen las leyes. En la fracción III del mismo artículo, se establece el acceso de los particulares a sus datos personales y a la rectificación de éstos.

El 30 de abril de 2009, se adicionó la fracción XXIX-O al artículo 73 de la Constitución, para especificar que sólo el Congreso tiene la facultad de legislar en materia de protección de datos personales en posesión de particulares. Y el 1° de junio del mismo año, se añadió un párrafo al artículo 16 Constitucional que señala lo siguiente: "… 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 públicas o para proteger los derechos de terceros". Con estas reformas a la Carta Magna, queda constituida la protección de datos personales como un derecho fundamental,[1]

[1] Véase Gómez-Robledo y Ornelas (2006: 14-18.).

así como el acceso, rectificación, cancelación y oposición por parte de las personas respecto de sus datos personales en poder de las instituciones.

Esto significa que los estados y la federación están obligados a legislar para normar los alcances e implicaciones del contenido de estas adiciones a los artículos referidos, con el propósito de garantizar el pleno ejercicio de tales derechos.

A dos años y medio de la reforma al artículo 16 constitucional, se tienen los siguientes resultados:

- Cuatro entidades cuentan con leyes específicas para la protección de datos personales (Colima, Distrito Federal, Guanajuato y Oaxaca).

- El Estado de Jalisco incorpora la normatividad en la materia en su Código Civil y su Ley de Transparencia y Acceso a la Información.

- Los 27 estados restantes incluyen la protección de datos personales en sus leyes de Transparencia.

- En el caso de la federación, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) determina la normatividad para proteger los datos personales en poder de las instituciones de gobierno, y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), los datos personales que poseen las personas físicas y morales en el sector privado.

Por la importancia de la protección de datos personales y los derechos ARCO, es necesario enfatizar que estos temas son independientes del derecho a la información; tal como lo expresa Ernesto Araujo: "…hablar del derecho a la información y la protección de datos personales es hablar de dos clases de disciplinas jurídicas diferentes, en virtud de su esencia, orígenes y fines. Sin embargo, ambas guardan una estrecha relación…" (Araujo, 2009:IX). En consecuencia, con todo y que estos derechos están vinculados, es conveniente impulsar la creación de leyes especializadas en protección de datos personales que contengan, al menos, los siguientes elementos:

- Ámbito de aplicación
- Principios
- Disposiciones en materia de seguridad
- Reconocimiento de los derechos ARCO
- Herramientas para garantizar la tutela de derechos
- Órgano garante con facultades suficientes
- Esquema de responsabilidades ante posibles incumplimientos de la Ley

Realidad de las legislaciones en el país

Las legislaciones sobre datos personales se pueden entender como "…las normas que garantizan las libertades públicas y los derechos fundamentales de las personas reconocidos en el ámbito de la información confidencial" (Araujo, 2009:155). En el caso de las entidades federativas, el terreno de aplicación de las legislaciones debe concentrarse en el sector público, toda vez que el Congreso ha determinado, con base en las facultades que le otorga el artículo 73, fracción XXIX-O, de la Constitución, el establecimiento de una Ley Federal para normar la posesión de datos personales en poder de los particulares; por lo tanto, el órgano garante de la federación tiene la responsabilidad de regular la posesión de los datos personales en el gobierno federal y el sector privado de todo el país. No obstante esta disposición, el estado de Colima, en su Ley de Protección de Datos Personales, establece la normatividad en esta materia tanto para el sector público como para el privado; lo mismo sucede en Tlaxcala con su Ley de Acceso a la Información Pública y Protección de Datos Personales.

a) Sujetos obligados

Las 32 leyes de las entidades federativas y la LFTAIPG consideran a los poderes Ejecutivo, Legislativo y Judicial, a los órganos autónomos y, en el caso de 31 estados, a los municipios, como sujetos obligados a la normatividad en protección de datos personales. En ese contexto, partiendo del hecho de que todas las instituciones de interés público deben proteger los datos personales que poseen, es oportuno resaltar que sólo 12 legislaciones consideran a los partidos políticos como obligados directos y tres como indirectos.

Además, las leyes de Chiapas e Hidalgo no exigen a las entidades paraestatales, desconcentradas, empresas de participación estatal, fideicomisos públicos, o cualquier otro que ejerza gasto público a proteger los datos de las personas.

El siguiente cuadro resume la situación de los sujetos obligados en las legislaciones del país.

Cuadro 1. Sujetos obligados en las legislaciones.

Entidad	Ejecutivo	Legislativo	Judicial	Autónomos	Municipios	Partidos Políticos		*	Particulares
						Directos	Indirectos		
LFTAIPG	SÍ	SÍ	SÍ	SÍ	NO	NO	NO	SÍ	NO
LFPDPPP	NO	NO	NO	NO	NO	NO	NO	NO	SÍ
1. AGS	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
2. B.C.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
3. B.C.S.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
4. CAMP	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
5. CHIS	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	NO	NO
6. CHIH	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
7. COAH	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
8. COL	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	SÍ
9. D.F.	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO	SÍ	NO
10. DGO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
11. EDO MÉX	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
12. GTO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
13. GRO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	NO
14. HGO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO	NO
15. JAL	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
16. MICH	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
17. MOR	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
18. NAY	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	NO
19. N.L.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
20. OAX	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
21. PUE	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
22. QRO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
23. Q ROO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
24. S.L.P.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
25. SIN	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
26. SON	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
27. TAB	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
28. TAMPS	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
29. TLAX.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ
30. VER.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
31. YUC.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO
32. ZAC.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
TOTAL DE LEYES	**33**	**33**	**33**	**33**	**31**	**12**	**3**	**31**	**3**

* Entidades paraestatales, desconcentrado, empresas de participación estatal, fideicomisos públicos, o cualquier otro que ejerza gasto público.
Fuente: InfoDF, Dirección de Datos Personales.

b) Reconocimiento de los derechos ARCO

La mayoría de las leyes del país coinciden en la definición de los datos personales como *la información concerniente a una persona física identificada o identificable*. Varias de ellas agregan que puede ser información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo; por ejemplo, las características físicas, morales, emocionales, el origen étnico o racial, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, el patrimonio, ideología y opiniones políticas, creencias y convicciones religiosas y filosóficas, estado de salud, preferencia sexual, huella digital, el ADN, número de seguridad social, etcétera. Algunos de estos datos se consideran sensibles, dado que afectan *a la esfera más íntima de su titular, o cuya utilización indebida puede dar origen a discriminación o conlleve un riesgo grave para éste,*[2] como el origen étnico o racial, las creencias y convicciones de tipo religioso, filosófico, moral y político, el estado de salud, la preferencia sexual, etc.; razón por la cual tienen que ser especialmente protegidos.

Los gobiernos de todos los niveles deben resguardar este tipo de datos que poseen en sus archivos o expedientes, pero también están obligados a dar acceso a los titulares de éstos y, en su momento, a rectificarlos si son inexactos, inadecuados o excesivos, o cancelarlos cuando su tratamiento no se ajuste a lo dispuesto a la ley, y a bloquearlos cuando el dueño de esta información se oponga al tratamiento que pueda dárseles, si es que los datos fueron recabados sin su consentimiento. Al Acceso, Rectificación, Cancelación y Oposición de datos personales se les conoce como "derechos ARCO". En las siguientes páginas, se ofrece una sinopsis de las características que debe observar la normatividad en materia de protección de datos personales y las leyes que cumplen con éstas. Para ello, referimos un universo de 34 legislaciones, una por cada entidad federativa y, en el caso de la federación, se consideran las dos leyes en sus respectivos ámbitos de aplicación. El cuadro que se expone a continuación, resume el reconocimiento que dan a los derechos ARCO las legislaciones de las entidades y la federación:

[2] Artículo 3, fracción VI, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Cuadro 2. Reconocimiento de los derechos ARCO en el país.

ENTIDAD	ACCESO	RECTIFICACIÓN	CANCELACIÓN	OPOSICIÓN
LFTAIPG	SÍ	SÍ	SÍ	NO
LFPDPPP	SÍ	SÍ	SÍ	SÍ
1. Aguascalientes	SÍ	SÍ	SÍ	SÍ
2. Baja California	SÍ	SÍ	SÍ	SÍ
3. Baja California Sur	SÍ	SÍ	NO	NO
4. Campeche	SÍ	SÍ	NO	SÍ
5. Chiapas	SÍ	SÍ	SÍ	SÍ
6. Chihuahua	SÍ	SÍ	SÍ	NO
7. Coahuila	SÍ	SÍ	SÍ	SÍ
8. Colima	SÍ	SÍ	SÍ	SÍ
9. Distrito Federal	SÍ	SÍ	SÍ	SÍ
10. Durango	SÍ	SÍ	SÍ	SÍ
11. Estado de México	SÍ	SÍ	SÍ	SÍ
12. Guanajuato	SÍ	SÍ	SÍ	SÍ
13. Guerrero	SÍ	SÍ	SÍ	SÍ
14. Hidalgo	SÍ	SÍ	SÍ	SÍ
15. Jalisco	SÍ	SÍ	SÍ	NO
16. Michoacán	SÍ	SÍ	SÍ	SÍ
17. Morelos	SÍ	SÍ	SÍ	NO
18. Nayarit	SÍ	SÍ	SÍ	NO
19. Nuevo León	SÍ	SÍ	SÍ	SÍ
20. Oaxaca	SÍ	SÍ	SÍ	SÍ
21. Puebla	SÍ	SÍ	NO	NO
22. Querétaro	SÍ	SÍ	NO	NO
23. Quintana Roo	SÍ	SÍ	NO	NO
24. San Luis Potosí	SÍ	SÍ	NO	NO
25. Sinaloa	SÍ	SÍ	SÍ	NO
26. Sonora	SÍ	SÍ	SÍ	NO
27. Tabasco	SÍ	SÍ	SÍ	NO
28. Tamaulipas	SÍ	SÍ	SÍ	NO
29. Tlaxcala	SÍ	SÍ	SÍ	SÍ
30. Veracruz	SÍ	SÍ	SÍ	NO
31. Yucatán	SÍ	SÍ	SÍ	NO
32. Zacatecas	SÍ	SÍ	SÍ	SÍ
Total de legislaciones	34	34	28	18

Fuente: InfoDF, Dirección de Datos Personales.

Como se puede observar, todas las legislaciones del país incluyen en sus contenidos el reconocimiento de los derechos de *acceso* y *rectificación* de datos personales.

En el caso de la *cancelación*, 28 legislaciones consideran este derecho; únicamente los estados de Baja California Sur, Campeche, Puebla, Querétaro, Quintana Roo y San Luis Potosí no lo hacen. Y 18 entidades reconocen el derecho de *oposición*; en la federación, sólo es posible ejercerlo en el ámbito privado y en el Poder Judicial, mientras que en Querétaro sólo se puede ejercer para oponerse a la publicación de información de procesos jurisdiccionales.

En total, son 17 legislaciones Estatales que observan todos los derechos ARCO.

c) Quiénes pueden ejercer los derechos ARCO

Los *titulares* de los datos personales pueden ejercer sus derechos ARCO en la federación y las 32 entidades federativas. El *representante legal o tutor* del titular de los datos podrá ejercer los derechos en lugar de éste en 24 entidades y el gobierno federal; en el caso de Chihuahua, Guerrero, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala, y Veracruz no es posible delegar esta facultad en ellos.

En Durango, Jalisco y Oaxaca también los *familiares del titular* podrán, en su nombre, ejercer los derechos ARCO. En Jalisco, Oaxaca, Quintana Roo y San Luis Potosí, además del titular o su representante, podrá hacerlo quien *acredite tener derechos subjetivos*.

Durango, Guanajuato, Jalisco, Oaxaca y Tlaxcala establecen *disposiciones específicas en caso de fallecimiento del titular* de los datos; esto significa que las personas que acrediten un vínculo jurídico o la sucesión testamentaria podrán ejercer los derechos. Y en nueve estados (Aguascalientes, Durango, Guanajuato, Jalisco, Morelos, Oaxaca, Quintana Roo, Tlaxcala y Yucatán) y la federación, podrá ejercer los derechos quien *acredite tener interés jurídico*.

Cabe señalar que en las dos leyes de la federación, Baja California, Baja California Sur, Campeche, Chiapas, Coahuila, Colima, Distrito Federal, Estado de México, Hidalgo, Michoacán, Nayarit, Nuevo

León, Puebla, Querétaro y Zacatecas, se establecen expresamente mecanismos que aseguren que sólo el titular o su representante legal podrá ejercer los derechos ARCO.

Por otro lado, de las 17 legislaciones que reconocen el ejercicio de estos cuatro derechos, excepto Chiapas y Durango el resto han establecido procedimientos específicos para ejercer cada uno de ellos.

d) Principios generales

Todas las leyes de protección de datos personales y derechos ARCO deben establecer y definir los principios por los que se regirán, por ejemplo, los de licitud, finalidad, consentimiento, lealtad, información, proporcionalidad, calidad, confidencialidad, disponibilidad, seguridad y temporalidad.

En la mayoría de las legislaciones actuales, estos principios sólo son referidos, mas no definidos.

El cuadro 3 sintetiza el panorama sobre la situación de los principios en las legislaciones vigentes.

Cuadro 3. Principios observados por las legislaciones del país.

ENTIDAD	LICITUD	CONSENTIMIENTO	INFORMACIÓN	CALIDAD DE LOS DATOS	FINALIDAD	LEALTAD	PROPORCIONALIDAD	RESPONSABILIDAD	CONFIDENCIALIDAD	SEGURIDAD	TEMPORALIDAD	DISPONIBILIDAD
LFTAIPG	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
LFPDPPP	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
1. AGS	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
2. B.C.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	NO	SÍ
3. B.C.S	SÍ	SÍ	NO	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	SÍ	SÍ
4. CAMP	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
5. CHIS	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
6. CHIH	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
7. COAH	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
8. COL	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
9. D.F.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
10. DGO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
11. EDO. MÉX	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
12. GTO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
13. GRO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
14. HGO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
15. JAL	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
16. MICH	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
17. MOR	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
18. NAY	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
19. N.L.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
20. OAX	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
21. PUE	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ
22. QRO	SÍ	NO	NO	NO	NO	NO	NO	NO	SÍ	SÍ	NO	SÍ
23. Q. ROO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ
24. S.L.P.	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
25. SIN	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
26. SON	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
27. TAB	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
28. TAMPS	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
29. TLAX	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
30. VER	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
31. YUC	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ
32. ZAC	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
TOTAL DE LEYES	34	33	26	33	32	28	32	32	34	34	29	34

Fuente: InfoDF, Dirección de Datos Personales.

Del cuadro anterior destaca lo siguiente:

- Los principios de *licitud, confidencialidad, seguridad y disponibilidad* son observados en todas las leyes.

- Querétaro es el único estado que no incluye el principio del *consentimiento*.

- Ocho estados no consideran el principio de *información*, éstos son: Baja California Sur, Campeche, Estado de México, Morelos, Puebla, Querétaro, San Luis Potosí y Sinaloa.

- Con excepción del estado de Querétaro, todas las demás legislaciones comprenden la *calidad de los datos* en su contenido.

- Los principios de *finalidad, proporcionalidad* y r*esponsabilidad* no son considerados en Baja California Sur y Querétaro.

- Las leyes de Baja California, Chiapas, Chihuahua, Nuevo León, Querétaro y Tamaulipas no contienen el principio de *lealtad*.

- Finalmente, las legislaciones de Baja California, Puebla, Querétaro, Quintana Roo y Yucatán no hacen referencia al de *temporalidad*.

Cabe destacar que las leyes de Aguascalientes, Coahuila, Colima, Distrito Federal, Durango, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Oaxaca, Sonora, Tabasco, Tlaxcala, Veracruz y Zacatecas contienen todos los principios mencionados. En contraste, la ley de Querétaro sólo incluye cuatro de éstos.

Un principio esencial es el del *consentimiento* del titular para el tratamiento de sus datos. Las leyes y lineamientos en la materia lo definen como la *manifestación de la voluntad libre, expresa o inequívoca, específica e informada, con la cual el titular de los datos otorga su consentimiento para el tratamiento de* éstos y, en su caso, para su transmisión, a menos que concurra algunas excepciones previstas en la ley. El consentimiento es libre cuando es obtenido sin la intervención de vicio alguno de la voluntad; es expreso o inequívoco cuando existe una acción manifiesta que implique su otorgamiento,

de manera que no haya lugar a dudas; es específico cuando se otorga para una finalidad; y es informado cuando se otorga con conocimiento de las finalidades para las que se utilizarán.[3]

31 entidades y la federación, en sus dos leyes, reconocen el principio de consentimiento; sin embargo, solamente la LFPDPPP, Coahuila, Colima, Distrito Federal, Guanajuato, Guerrero, Michoacán, Nuevo León, Oaxaca, Puebla y Tlaxcala prevén la posibilidad de revocarlo.

En las dos leyes de la federación y 24 entidades más, se especifican los elementos que debe incluir la leyenda para informar al titular de los datos sobre el tratamiento que recibirán los datos recabados.

El cuadro que se muestra a continuación, ofrece un panorama completo de los elementos que deben estar contenidos en la leyenda de cualquier formato que se utilice para recabar el consentimiento del titular.

Esta leyenda también cumple con otro principio: el de información, para enterar a las personas el propósito de brindar sus datos y el tratamiento que se les dará:

[3] Véase numeral 19, fracción II, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal; y Carbonell, Miguel, Davara, Isabel y Luna, Issa, *Ley de Protección de Datos Personales para el Distrito Federal Comentada*, InfoDF, pp. 54 y 55.

Cuadro 4. Contenido de la leyenda.

Entidad	Responsable del sistema (datos adicionales)	Finalidad del tratamiento	Posibilidad de limitar el uso o divulgación de los datos	Derechos ARCO	Transferencias de datos	Notificación sobre cambios al aviso de privacidad	Consideraciones para datos sensibles	Otros
LFTAIPG	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	NO
LFPDPPP	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
1. AGS	SÍ	SÍ	NO	SÍ	SÍ	NO	NO	NO
2. B.C.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ
3. CHIS	SÍ	SÍ	SÍ	NO	SÍ	NO	NO	NO
4. CHIH	SÍ	SÍ	NO	SÍ	SÍ	NO	NO	NO
5. COAH	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ
6. COL	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ
7. D.F.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ
8. DGO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ
9. GTO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	NO
10. GRO	SÍ	SÍ	NO	SÍ	SÍ	NO	NO	NO
11. HGO	SÍ	SÍ	SÍ	NO	SÍ	NO	NO	NO
12. JAL	SÍ	SÍ	NO	SÍ	SÍ	NO	NO	NO
13. MICH	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ	NO
14. NAY	SÍ	SÍ	NO	SÍ	NO	NO	NO	NO
15. N.L.	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ
16. OAX	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO	NO
17. Q ROO	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ
18. SON	SÍ	SÍ	NO	SÍ	NO	NO	NO	NO
19. TAB	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	NO
20. TAMPS	SÍ	SÍ	NO	SÍ	NO	NO	NO	NO
21. TLAX	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
22. VER	SÍ	SÍ	NO	SÍ	NO	NO	NO	NO
23. YUC	SÍ	SÍ	NO	SÍ	SÍ	NO	NO	NO
24. ZAC	SÍ	SÍ	NO	SÍ	NO	NO	NO	NO
TOTAL DE LEYES	26	26	14	24	21	3	7	9

Fuente: Elaboración del autor, con base en información proporcionada por la Dirección de Datos Personales del InfoDF.

En el cuadro se observa que las 26 legislaciones ofrecen información sobre el responsable del sistema de datos personales y la finalidad del tratamiento que se les dará; Sobre la posibilidad de limitar el uso o divulgación de datos, 12 entidades federativas y la federación, en sus dos leyes, lo hacen patente.

Con excepción de Chiapas e Hidalgo, las otras 24 legislaciones establecen que las leyendas deberán orientar sobre la posibilidad de ejercer los derechos ARCO. El número de entidades que informan a quién se transferirán los datos son 19 y la federación en ambas leyes.

La LFPDPPP y los estados de Tabasco y Tlaxcala adicionan que deberán notificarse los cambios al aviso de privacidad. La LFPDPPP, el Distrito Federal, Durango, Michoacán, Quintana Roo, Tabasco y Tlaxcala tienen consideraciones especiales para datos sensibles. Y nueve leyes incluyen en su leyenda otros rubros adicionales a los mencionados.

Aun y cuando es importante obtener el consentimiento del interesado para tratar sus datos, las leyes establecen excepciones, toda vez que, en ocasiones específicas, será inevitable tratarlos sin tal consentimiento.

Las causales de excepción al consentimiento son heterogéneas; existen nueve contempladas en legislaciones de 28 entidades federativas y las dos de la federación. El siguiente cuadro resume las excepciones contenidas en cada una ellas:

Cuadro 5. Excepciones al principio de consentimiento.

Entidad	Previsión legal	Fuentes de acceso público	Datos disociados	Cumplimiento de obligaciones derivadas de una relación jurídica entre el titular y el responsable	Casos de emergencia (precisar)	Atención médica	Resolución de autoridad competente	Proteger los intereses jurídicamente tutelados del titular	Realizar una acción en función del interés público
LFTAIPG	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	NO
LFPDPPP	SÍ	NO	SÍ	SÍ	NO	NO	SÍ	NO	SÍ
1. AGS	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	NO
2. B.C.	SÍ	SÍ	NO	NO	NO	NO	SÍ	NO	NO
3. CHIS	SÍ	NO	SÍ	NO	NO	NO	SÍ	NO	SÍ
4. COAH	SÍ	SÍ	NO	SÍ	NO	SÍ	SÍ	NO	SÍ
5. COL	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ
6. D.F.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
7. DGO	SÍ	SÍ	NO	SÍ	NO	SÍ	NO	NO	SÍ
8. EDO MÉX	SÍ	SÍ	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ
9. GTO	NO	SÍ	NO	NO	SÍ	SÍ	SÍ	NO	SÍ
10. GRO	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	NO	SÍ
11. HGO	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	NO
12. JAL	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	NO	SÍ
13. MICH	SÍ	SÍ	NO	NO	NO	NO	SÍ	NO	SÍ
14. MOR	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ
15. NAY	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ
16. N.L.	SÍ	SÍ	NO	SÍ	NO	SÍ	NO	NO	SÍ
17. OAX	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ
18. PUE	SÍ	NO	NO	NO	NO	SÍ	SÍ	NO	SÍ
19. Q ROO	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	NO	SÍ
20. S.L.P.	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ
21. SIN	SÍ	SÍ	SÍ	SÍ	NO	NO	SÍ	NO	SÍ
22. SON	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	NO	SÍ
23. TAB	SÍ	NO	SÍ	SÍ	NO	SÍ	SÍ	NO	SÍ
24. TAMPS	SÍ	NO	SÍ	NO	NO	NO	SÍ	NO	SÍ
25. TLAX	SÍ	NO	SÍ	SÍ	NO	NO	NO	NO	SÍ
26. VER	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	NO	SÍ
27. YUC	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	SÍ	SÍ
28. ZAC	SÍ	NO	SÍ	NO	NO	SÍ	SÍ	NO	SÍ
TOTAL DE LEYES	**29**	**11**	**23**	**18**	**5**	**23**	**27**	**3**	**26**

Fuente: Elaboración del autor, con base en información proporcionada por la Dirección de Datos Personales del InfoDF.

Otro principio que es necesario considerar es el de la seguridad. Todas las legislaciones establecen medidas de seguridad que deberán ser observadas por los sujetos obligados. La seguridad consiste en garantizar que sólo el personal autorizado tiene acceso a la información, ya sea el responsable de los sistemas de datos o los usuarios.[4]

Los tipos de medidas de seguridad que contemplan las legislaciones son: física, administrativa y técnica.

[4] Carbonell, Miguel, Davara, Isabel y Luna, Issa, *Ley de Protección de Datos Personales para el Distrito Federal Comentada*, InfoDF, pág. 58.

Cuadro 6. Medidas de seguridad.

ENTIDAD	FÍSICA	ADMINISTRATIVA	TÉCNICA
LFTAIPG	SÍ	NO	NO
LFPDPPP	SÍ	SÍ	SÍ
1. AGS	SÍ	NO	NO
2. B.C.	SÍ	NO	NO
3. B.C.S	SÍ	NO	NO
4. CAMP	SÍ	NO	NO
5. CHIS	SÍ	SÍ	SÍ
6. CHIH	SÍ	NO	NO
7. COAH	SÍ	SÍ	SÍ
8. COL	SÍ	NO	NO
9. D.F.	SÍ	SÍ	SÍ
10. DGO	SÍ	NO	NO
11. EDO. MÉX	SÍ	NO	NO
12. GTO	SÍ	NO	NO
13. GRO	SÍ	NO	NO
14. HGO	SÍ	NO	NO
15. JAL	SÍ	NO	NO
16. MICH	SÍ	SÍ	SÍ
17. MOR	SÍ	NO	NO
18. NAY	SÍ	NO	NO
19. N.L.	SÍ	SÍ	SÍ
20. OAX	SÍ	NO	NO
21. PUE	SÍ	NO	NO
22. QRO	SÍ	NO	NO
23. Q. ROO	SÍ	NO	NO
24. S.L.P.	SÍ	NO	NO
25. SIN	SÍ	NO	NO
26. SON	SÍ	NO	NO
27. TAB	SÍ	NO	NO
28. TAMPS	SÍ	NO	NO
29. TLAX	SÍ	NO	NO
30. VER	SÍ	NO	NO
31. YUC	SÍ	NO	NO
32. ZAC	SÍ	SÍ	SÍ
Total de legislaciones	34	7	7

Fuente: Elaboración del autor, con base en información proporcionada por la Dirección de Datos Personales del InfoDF.

Es necesario aclarar que la Ley del Distrito Federal clasifica las medidas de seguridad de la siguiente manera: física; lógica y de

desarrollo y aplicaciones, de cifrado y comunicación y redes. Por otro lado, en Coahuila, Colima, Distrito Federal, Michoacán, Morelos y Nuevo León se establecen las medidas de seguridad de acuerdo con el tipo de datos que se recaben en los sistemas.

Pero sólo en el Distrito Federal y Nuevo León se especifican que las medidas se clasificarán en los siguientes niveles: básico, medio y alto.

Los registros de sistemas de datos

Otro aspecto relevante es el del registro de sistemas de datos, que tiene una importancia central porque permite identificar los ámbitos de responsabilidad, facilita el ejercicio de los derechos ARCO y la facultad de inspección del órgano garante. El sistema de datos personales puede definirse como: *conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permitan el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso.*[5] Los sistemas pueden ser físicos, lógicos y jurídicos:

- Físicos.- Se refieren a los sistemas en papel y/o a la ubicación geográfica del sistema.
- Lógico.- Se determinan por la configuración lógica del sistema de información.
- Jurídico.- Se definen por la naturaleza de los datos y la finalidad con la que éstos son tratados.[6]

Las legislaciones de 16 entidades regulan la existencia de un registro. El siguiente cuadro contiene los elementos que, de acuerdo con la ley de estas 16 entidades, deben inscribirse en el registro de los sistemas:

[5] Numeral 3, fracción XVIII, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

[6] Carbonell, Miguel, Davara, Isabel y Luna, Issa, *Ley de Protección de Datos Personales para el Distrito Federal Comentada*, InfoDF, pág. 286.

Cuadro 7. Elementos inscritos en el registro de los sistemas de datos.

Entidad	Nombre	Finalidad	Fundamento de existencia	Población objetivo	Procedimiento de recolección	Datos que se recaban	Cesiones o transferencias	Responsable del sistema	Funcionarios que realizan el tratamiento	Personal externo que realiza el tratamiento
1. AGS	SÍ	SÍ	SÍ	NO	NO	NO	NO	NO	NO	NO
2. B.C.	NO	SÍ	SÍ	NO	NO	NO	NO	NO	NO	NO
3. CAMP	NO	SÍ	SÍ	NO	NO	SÍ	SÍ	NO	NO	NO
4. CHIS	NO	SÍ	SÍ	SÍ	NO	NO	NO	NO	NO	NO
5. COAH	NO	SÍ	SÍ	NO	NO	SÍ	NO	NO	NO	NO
6. COL	SÍ	SÍ	SÍ	NO	NO	NO	NO	NO	NO	NO
7. D.F.	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
8. GTO	SÍ	SÍ	SÍ	NO	NO	NO	SÍ	NO	NO	NO
9. GRO	NO	SÍ	SÍ	NO	NO	NO	NO	SÍ	NO	NO
10. JAL	SÍ	SÍ	SÍ	NO	NO	NO	NO	NO	NO	NO
11. N.L.	SÍ	SÍ	SÍ	NO	NO	SÍ	NO	SÍ	SÍ	NO
12. OAX	SÍ	SÍ	SÍ	NO	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
13. SLP	NO	SÍ	SÍ	NO	NO	NO	NO	NO	NO	NO
14. TLAX	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
15. VER	SÍ	SÍ	SÍ	NO	NO	NO	SÍ	NO	NO	SÍ
16. ZAC	SÍ	SÍ	SÍ	NO	NO	NO	SÍ	NO	NO	SÍ
TOTAL DE LEYES	**10**	**16**	**16**	**3**	**3**	**6**	**7**	**5**	**4**	**5**

Fuente: Elaboración del autor, con base en información proporcionada por la Dirección de Datos Personales del InfoDF.

Como se puede observar en el cuadro, la *finalidad* del tratamiento y el *fundamento de existencia* están contenidos en las 16 legislaciones. Y sólo el Distrito Federal y el estado de Tlaxcala incluyen todos los elementos en su registro de los sistemas de datos.

Retos para consolidar el derecho a la protección de datos en el país

Aún queda mucho por hacer para consolidar el ejercicio del derecho a la protección de los datos personales en todo el país.

En particular, destacan los siguientes retos:

- Reconocer el derecho a la protección de los datos personales como un derecho independiente al de acceso a la información pública.

- Establecer límites entre este derecho y el de acceso a la información pública (incluir la prueba de interés público como una restricción a la divulgación de datos personales).

- Fortalecer el derecho a la protección de datos personales, tanto a nivel federal, como en cada una de las entidades del país.

Todas las entidades de la República deben tomar las medidas para consolidar este derecho en México y ofrecer a los ciudadanos, de manera plena, la protección y el acceso, rectificación, cancelación y oposición de sus datos personales. Entre otras, destacas las siguientes tareas pendientes:

- Impulsar la creación de leyes especializadas en la protección de datos personales en cada entidad federativa, con el fin de proteger, de manera eficiente, la privacidad de sus gobernados.

- Apoyar y contribuir, con acciones concretas y específicas, a la adopción de medidas de seguridad suficientes, para garantizar el tratamiento legítimo y seguro de los datos personales.

- Promover y facilitar un eficaz ejercicio de los derechos ARCO.

- Fomentar la observancia de los principios y deberes que se establezcan en las leyes especializadas en protección de datos personales.

- Capacitar a los servidores públicos en materia del derecho a la protección de datos personales.

- Dotar a los órganos garantes con las facultades suficientes para garantizar el derecho a la protección de los datos personales en posesión de las autoridades públicas estatales y municipales.

- Implementar estrategias de coordinación entre los órganos garantes del derecho de acceso a la información pública y el IFAI, para propiciar la plena vigencia del derecho a la protección de datos personales en todo el territorio nacional.

La protección de datos personales en el Distrito Federal

Con la publicación de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en mayo de 2008, la protección de datos personales adquirió especial relevancia en esta Entidad, toda vez que ocho de sus artículos limitan al derecho de acceso a la información pública cuando se trata de proteger los datos privados de las personas.

En octubre de ese mismo año, se publicó la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF), con el propósito de *establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos* de esta entidad,[7] de una forma más especializada y completa. En congruencia con lo anterior, el entonces Instituto de Acceso a la Información Pública del Distrito Federal, ahora Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), elaboró los *Lineamientos para la Protección de Datos Personales en el Distrito Federal*, publicados en la Gaceta Oficial el 26 de octubre de 2009.

[7] Artículo 1 de la LPDPDF.

La publicación de esta normatividad estuvo orientada a consolidar la protección de datos personales en posesión de las autoridades y el ejercicio de los derechos ARCO entre los habitantes de esta entidad federativa. Por tal motivo, es importante reconocer las relaciones y distinciones que existen entre el derecho de acceso a la información y el de protección de los datos personales:

- En primer término, es necesario que la protección de datos permanezca en ambos tipos de normatividad para lograr una interpretación armónica de ambas leyes.

- La protección de datos no debe ser utilizada como obstáculo para dar paso al interés público de conocer información socialmente relevante.

- Se debe establecer la prueba de daño, para limitar el acceso a la información pública, y la prueba de interés público, cuando se trate de limitar la protección de los datos personales.

- Es conveniente realizar estudios de ponderación de derechos.

Registro de sistemas de datos

Como se apuntó anteriormente, los sistemas de datos son el conjunto organizado de datos personales en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, clasificados de manera que se pueda acceder a ellos en cualquiera que fuere la modalidad de su creación o almacenamiento.

De acuerdo a lo establecido en el artículo 8 de la Ley de Protección de Datos Personales para el Distrito Federal, todos los sistemas de datos personales en posesión de los entes públicos deben estar inscritos en el registro que para tal efecto habilite el Instituto. Para el cumplimiento de esta obligación, el InfoDF creó la aplicación informática denominada *Registro de Sistemas de Datos Personales* (RESDP).

Esta plataforma informática está desarrollada especialmente para que todos los entes obligados del Distrito Federal estén en posibilidades de registrar y actualizar los sistemas de datos que manejan vía Internet.

Al 31 de octubre de 2011, habían sido inscritos 1,338 sistemas de datos personales, de un total de 117 entes obligados registrados en el padrón.[8] Con el objetivo de verificar si ya estaban inscritos ante el Instituto la totalidad de los sistemas de datos personales en posesión de los entes obligados, el Instituto se dio a la tarea de realizar un estudio diagnóstico para verificar que la obligación establecida en el artículo 8 de la Ley de Datos Personales para el Distrito Federal fuera cumplida por los entes públicos.

En la realización del estudio diagnóstico se estudió el marco normativo aplicable al Ente Público, además se revisaron los portales de transparencia en donde se publica el listado de información que detentan los entes, de acuerdo con las atribuciones y responsabilidades que les competen y de conformidad con las disposiciones aplicables, así como los programas y servicios que ofrecen y los respectivos formatos que son utilizados en la realización de los trámites y requisición de servicios.

Esta información se publica en el Portal de Transparencia de cada Ente Público (sujeto obligado en términos de la Ley de Transparencia) en cumplimiento a lo dispuesto en los artículos 13 y 14 fracciones I, III, XX y XXI de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

De la revisión realizada, se identificaron 944 sistemas en posesión de los entes públicos que no habían sido inscritos en el RESDP.

Además, dentro de los sí registrados, se detectaron 76 duplicados y 170 improcedentes. Esto da un total neto de 2,036 sistemas, que resultan de la suma de 1,338 sistemas inscritos y los 944 no registrados, menos los 76 duplicados y los 170 improcedentes.

El siguiente cuadro da un panorama completo por órgano de gobierno.

[8] Cabe aclarar que la Agencia de Protección Sanitaria del Gobierno del Distrito Federal, el Consejo para Prevenir y Eliminar la Discriminación de la Ciudad de México y el Fideicomiso Fondo de Apoyo a la Educación y el Empleo de las y los Jóvenes del Distrito Federal fueron incorporados al Padrón de Sujetos Obligados a la LPDPDF durante el periodo de evaluación, por lo tanto, no se consideran en el reporte que se expone en este artículo.

Cuadro 8. Evaluación preliminar de los sistemas de datos personales a octubre de 2011.

Órgano de Gobierno	Sistemas de Datos Personales				Total	Total Neto	% de Inscripción	% de Subregistro
	Inscritos	No registrados	Duplicados	Improcedentes				
Administración Pública Centralizada	246	300	41	0	587	505	41%	59%
Delegaciones Políticas	391	278	20	145	834	504	45%	55%
Desconcentrados, Descentralizados, Paraestatales y Auxiliares	594	267	13	9	883	839	68%	32%
Órgano Legislativo	2	16	0	0	18	18	11%	89%
Órgano Judicial	19	20	0	8	47	31	35%	65%
Órganos Autónomos	74	44	2	8	118	108	59%	41%
Partidos Políticos	12	19	0	0	31	31	39%	61%
TOTAL	1,338	944	76	170	2,518	2,036	54%	46%

Fuente: InfoDF, Dirección de Datos Personales.

Como se observa en el cuadro, al 31 de octubre sólo el 54% de los sistemas de datos personales estaba registrado en el RESDP; es decir, casi la mitad de los sistemas que operan los entes obligados en el Distrito Federal no habían sido registrados aún ante el Instituto.

A partir de estos resultados el Instituto se dio a la tarea de trabajar de manera coordinada con los entes públicos para asesorarlos en el cumplimiento de la obligación establecida en el artículo 8 de la Ley.

Cuadro 9. Evaluación preliminar de los sistemas de datos personales a diciembre de 2011.

Órgano de Gobierno	Sistemas de Datos Personales				Total	Total Neto	% de Inscripción	% de Subregistro
	Inscritos	No registrados	Duplicados	Improcedentes				
Administración Pública Centralizada	389	52	2	0	443	505	88%	12%
Delegaciones Políticas	466	166	0	145	777	504	74%	26%
Desconcentrados, Descentralizados, Paraestatales y Auxiliares	653	55	1	8	717	708	92%	8%
Órgano Legislativo	87	0	0	0	87	87	100%	12%
Órgano Judicial	22	3	0	8	33	25	88%	5%
Órganos Autónomos	91	5	1	8	105	96	95%	0%
Partidos Políticos	29	0	0	0	29	29	100%	0%
TOTAL	1,737	281	4	169	2,191	2,018	86%	14%

Fuente: InfoDF, Dirección de Datos Personales.

A partir de este trabajo de acompañamiento, al 9 de diciembre del 2011, el cumplimiento se incrementó y sólo quedaban pendientes por inscribir el 14% de los sistemas de datos personales en posesión de los entes públicos.

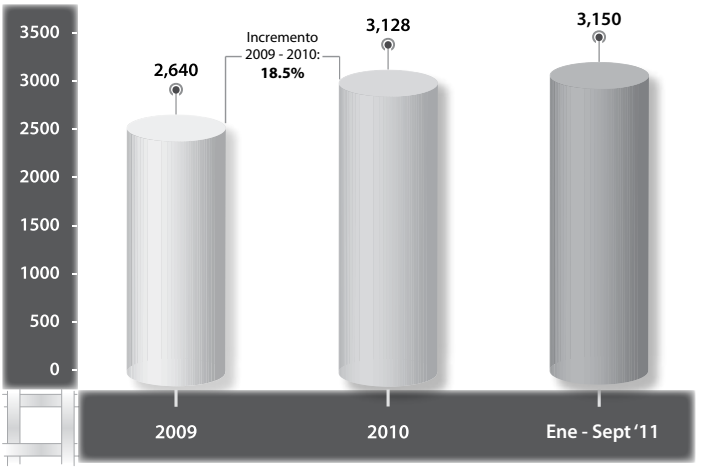
La media de cumplimiento de los 21 entes obligados de la administración pública centralizada fue del 88%; en el caso de las delegaciones, era de 74%; de los organismos desconcentrados, descentralizados, paraestatales y auxiliares, el promedio fue de 92%; el órgano Judicial, integrado por el Consejo de la Judicatura del D.F. y el Tribunal Superior de Justicia del D.F., tenía una media de cumplimiento del 88%; el Legislativo, conformado por la Asamblea Legislativa del D.F. y la Contaduría Mayor de Hacienda de la ALDF, registró un 100% y los órganos autónomos presentaron un 95%; por último, los partidos políticos promediaron un 100% de sistemas inscritos.

Solicitudes de derechos ARCO

En el año de 2009, los entes obligados del Distrito Federal recibieron un total de 2,640 solicitudes ARCO de datos personales. Para 2010, hubo un incremento del 18.5%, lo que representó un total de 3,128 solicitudes.

De enero a septiembre de 2011, las solicitudes recibidas han sido de 3,150. Las solicitudes totales de 2009 hasta el tercer trimestre de este año, son de 8,918.

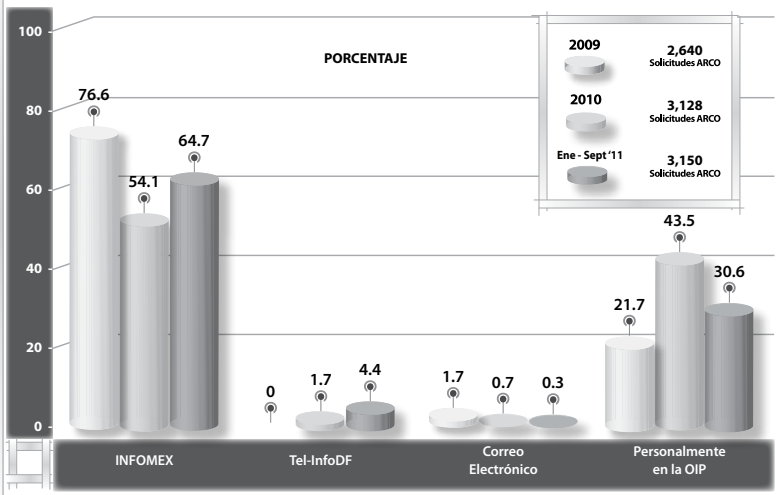
Gráfica 1. Solicitudes ARCO recibidas (2009 - septiembre 2011).



Fuente: InfoDF, Dirección de Evaluación y Estudios.

Respecto a los medios de presentación de las solicitudes, la siguiente gráfica revela los porcentajes de la forma en que éstas han llegado a los entes obligados:

Gráfica 2. Medios de presentación de solicitudes ARCO.



Fuente: InfoDF, Dirección de Evaluación y Estudios.

El sistema INFOMEX es el instrumento por el que, preferentemente, se presentan las solicitudes ARCO; aunque se nota un alto porcentaje en el trámite de manera presencial ante la oficina de información pública.

En los tres ejercicios que se comparan, el Ejecutivo es el órgano que recibe la mayor parte de las solicitudes; por ejemplo, en 2009, concentró el 94.3%; en 2010, el 92.0%; y al tercer trimestre de 2011, el 92.0%.

Como se observa en el cuadro siguiente, son los organismos desconcentrados, descentralizados, paraestatales y auxiliares los que mayormente reciben las peticiones de los ciudadanos con respecto a los derechos ARCO.

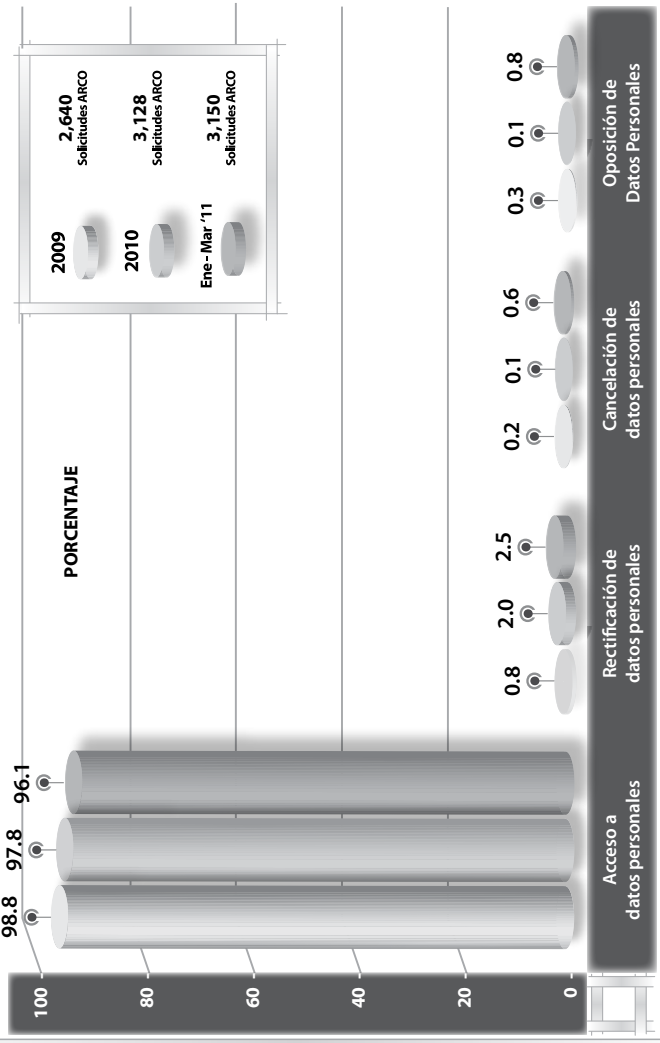
Cuadro 10. Solicitudes ARCO recibidas por órgano de gobierno.

ÓRGANO DE GOBIERNO	2009		2010		Ene-Sept'11	
	ARCO	%	ARCO	%	ARCO	%
Ejecutivo	2,490	94.3%	2,876	92%	2,898	92%
Administración Pùblica Central	721	27.3%	1,119	35.8%	1,427	45.3%
Desconcentrados, Descentralizados, Paraestatales y Auxiliares	1,452	55%	1,372	43.9%	1,186	37.7%
Delegaciones Políticas	317	12%	385	12.3%	285	9%
Judicial	14	0.5%	48	1.5%	43	1.4%
Legislativo	21	0.8%	65	2.1%	54	1.7%
Autónomo	28	1.1%	125	4%	143	4.5%
Partidos Políticos en el Distrito Federal	87	3.3%	14	0.4%	12	0.4%
Total	2,640	100%	3,128	100%	3,150	100%

Fuente: InfoDF, Dirección de Evaluación y Estudios.

Como se observa en la gráfica siguiente, la gran mayoría son en ejercicio del derecho de *acceso* a datos personales.

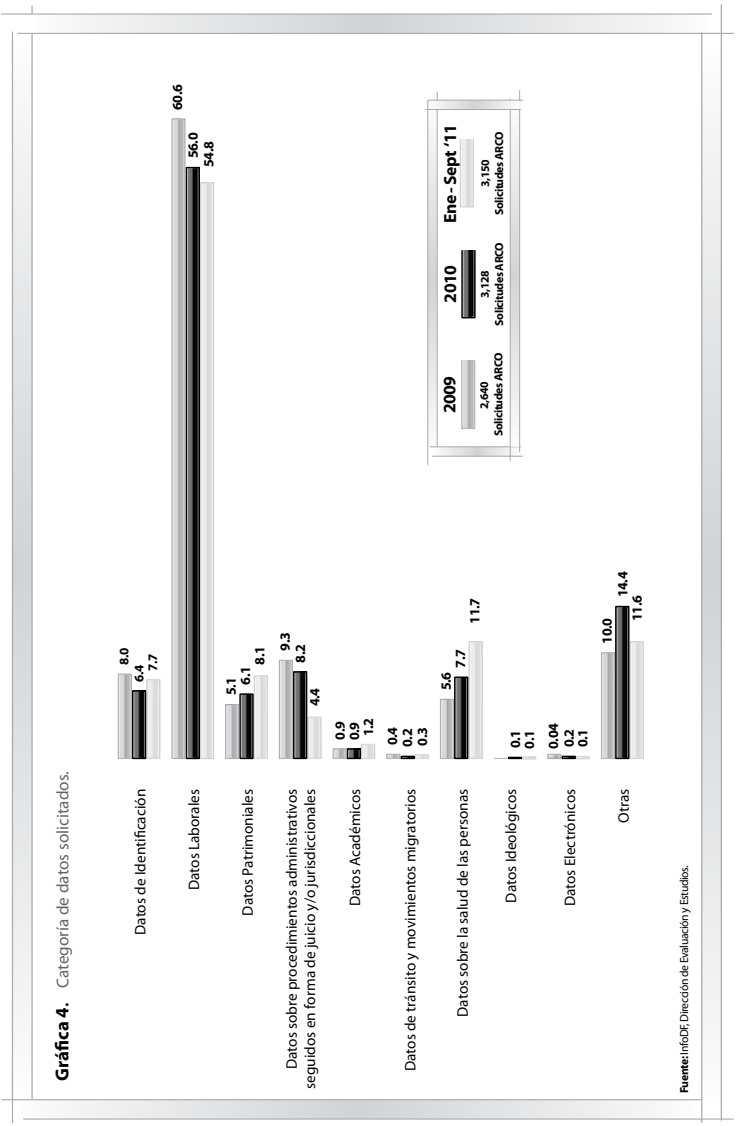
Gráfica 3. Derecho objeto de la solicitud ARCO.



Fuente: InfoDF, Dirección de Evaluación y Estudios.

Por otro lado, vale la pena informar sobre el tipo de datos que requieren los habitantes de esta entidad en sus solicitudes ARCO. Por supuesto, es comprensible que la mayor parte esté relacionada con el ámbito laboral.

Gráfica 4. Categoría de datos solicitados.



Fuente: InfoDF, Dirección de Evaluación y Estudios.

Los entes obligados con el mayor número de solicitudes al tercer trimestre de 2011, son:

Cuadro 11. Entes obligados con mayor número de solicitudes (enero - septiembre 2011)

Entes obligados	ARCO	%
1. Secretaría de Salud	855	27.10%
2. Policía Auxiliar	594	18.90%
3. Instituto de Vivienda del Distrito Federal	157	5.00%
4. Caja de Previsión de la Policía Auxiliar del Distrito Federal	150	4.80%
5. Secretaría de Seguridad Pública	121	3.80%
6. Procuraduría General de Justicia del Distrito Federal	75	2.40%
7. Oficialía Mayor	63	2.00%
8. Delegación Venustiano Carranza	53	1.70%
9. Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal	52	1.70%
11. Asamblea Legislativa del Distrito Federal	51	1.60%
12. Junta Local de Conciliación y Arbitraje del Distrito Federal	48	1.50%
13. Contraloría General del Distrito Federal	44	1.40%
14. Secretaría de Transportes y Vialidad	42	1.30%
15. Sistema de Transporte Colectivo	34	1.10%
16. Secretaría de Gobierno	33	1.00%
17. Tribunal Superior de Justicia del Distrito Federal	32	1.00%
18. Consejería Jurídica y de Servicios Legales	31	1.00%
19. Delegación Iztapalapa	27	0.90%
Total	**2,462**	**78.20%**

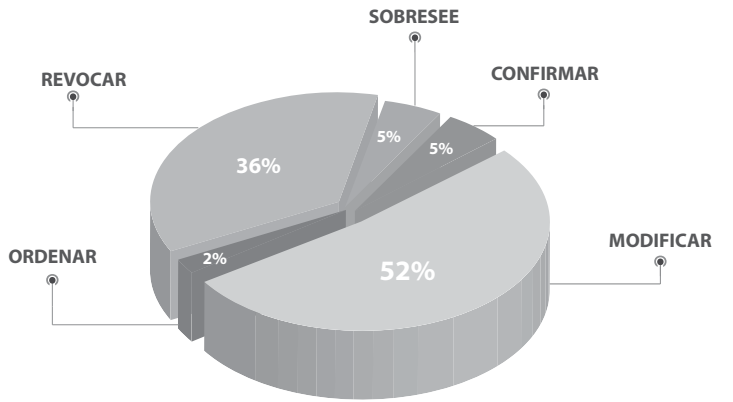
Fuente: InfoDF, Dirección de Evaluación y Estudios.

Estas 18 instituciones y dependencias concentran el 78.2% de las solicitudes ARCO.

Recurso de revisión

El artículo 38 de la LPDPDF determina que el interesado que se considere agraviado por la resolución definitiva que recaiga a su solicitud de acceso, rectificación, cancelación u oposición, o ante la omisión de respuesta, podrá interponer recurso de revisión ante el InfoDF. En este caso, las oficinas de información pública deben orientar al particular sobre su derecho de interponer el recurso y la forma y plazo para hacerlo. El InfoDF, con conocimiento de causa y con acceso a la información contenida en los sistemas de datos, deberá resolver el recurso; resolución que será definitiva, inatacable y obligatoria, tanto para los entes obligados como para los particulares (artículo 39 de la LPDPDF). Al respecto, la gráfica que se presenta a continuación contiene los porcentajes del sentido de las resoluciones aprobadas por el Pleno del Instituto, de enero de 2010 a septiembre de 2011, en materia de recursos de revisión de datos personales.

Gráfica 5. Sentido de las resoluciones del Pleno del InfoDF a los recursos de revisión.



Conclusiones

En el Distrito Federal, se ha trabajado para crear las leyes y las normas secundarias suficientes para garantizar a sus habitantes el ejercicio de su derecho a la protección de datos personales y los llamados derechos ARCO. El diagnóstico realizado por el InfoDF en los entes obligados, respecto del cumplimiento de la normatividad en la materia, deja claro que faltan cosas por hacer para consolidar la práctica de estos derechos entre los funcionarios públicos y la población.

Se han detectado problemas en la identificación de sistemas de datos personales, preexistentes a la entrada en vigor de la Ley de Protección de Datos Personales (GODF, 3 octubre de 2008); confusión sobre el origen, competencia, atribución y resguardo de los datos personales contenidos en los sistemas; dudas en la identificación de datos personales y las categorías de éstos; y dificultad sobre el contenido, finalidad, uso y destino de los sistemas de datos personales. Para responder a esta problemática, el InfoDF continuará con el asesoramiento a los entes obligados en la identificación e inscripción de sus sistemas en el Registro Electrónico de los Sistemas de Datos Personales y dará el acompañamiento institucional para resolver, en conjunto, las dudas y conflictos que se vayan presentando; al mismo tiempo que aplicará las medidas de prevención y corrección que le faculta la normativa, para asegurar la debida protección de los datos en los sistemas físicos y electrónicos, tal como lo prevé la propia norma.

Finalmente, es importante señalar algunos conceptos que deben prevalecer para compaginar el derecho de acceso a la información con el de protección de datos personales; por ejemplo:

- En caso de conflicto en el ejercicio de los derechos de acceso a la información y de protección de datos, se debe asegurar el máximo nivel de armonía.

- Es conveniente definir roles complementarios en la regulación de ambos, con la protección de datos como común denominador.

- Se deben establecer ambos derechos como independientes uno del otro, en legislaciones por separado, pero complementarias.

- Las excepciones para revelar información deben ser claras y, en ningún caso, los datos sensibles pueden ser objeto de difusión.

- En virtud de que es difícil establecer cuál derecho prevalece sobre el otro, deben ser cuidadosamente considerados los intereses en juego, tanto públicos como privados.

Con el reconocimiento constitucional del derecho a la protección de datos personales y la creación de Leyes especiales en la federación y en cuatro estados (Colima, el Distrito Federal, Oaxaca y Guanajuato) se han realizado avances importantes. Sin embargo, es necesario crear leyes especiales en cada entidad federativa con el objetivo continuar avanzando en la dirección correcta en la defensa de otros derechos como el derecho a la vida privada, al honor y a la no discriminación, sin generar inercias negativas que contrarresten los avances alcanzados en materia de transparencia y acceso a la información.

Referencias

Araujo Carranza, Ernesto (2009), *El Derecho a la Información y la Protección de Datos Personales en México*, Porrúa, 292 pp.

Carbonell, Miguel (Coordinador), Davara, Isabel y Luna, Issa, (2010), *Ley de Protección de Datos Personales para el Distrito Federal Comentada*, InfoDF e IIJ-UNAM, 322 pp.

Gómez-Robledo, Alonso y Ornelas Núñez, Lina (2006), *Protección de Datos Personales en México: el Caso del Poder Ejecutivo Federal*, UNAM, 111 pp.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG). Publicación DOF el 11 de junio de 2002, última reforma el 5 de julio de 2010.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Publicación DOF el 5 de julio de 2010.

Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes (LTAIPAgs). Publicación POE el 22 de mayo de 2006, última reforma el 8 de agosto de 2011.

Ley de Transparencia y Acceso a La Información Pública para el Estado de Baja California (LTAIPBC). Publicación POE el 1° de octubre de 2010.

Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California Sur (LTAIPBCS). Publicación POE el 12 de marzo de 2010

Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche (LTAIPCamp). Publicación POE el 21 de julio de 2005, última reforma el 15 de julio de 2009.

Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas (LTIPChis). Publicación POE el 12 de octubre de 2006, última reforma el 17 de noviembre de 2010.

Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua (LTAIPChih). Publicación POE el 15 de octubre de 2005, última reforma el 2 de octubre de 2010.

Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila (LAIPyPDPCoah). Publicación POE el 2 de septiembre de 2008, última reforma el 26 de junio de 2009.

Ley de Protección de Datos del Estado de Colima (LPDPCol). Publicación POE el 21 de junio de 2003.

Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF). Publicación GODF el 3 de octubre de 2008.

Ley de Transparencia y Acceso a la Información Pública del Estado de Durango (LTAIPDgo). Publicación POE el 13 de julio 2008.

Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios (LTAIPEdo.mex). Publicación POE el 30 de abril de 2004, última reforma el 2 de agosto de 2011.

Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato (LPDPGto). Publicación POE el 19 de mayo de 2006.

Ley número 374 de Transparencia y Acceso a la información Pública del Estado de Guerrero (LTAIPGro). Publicación POE 15 de junio de 2010.

Ley de Transparencia y Acceso a la Información Pública Gubernamental del Estado de Hidalgo (LTAIPHgo). Publicación POE el 29 de diciembre de 2006.

Ley de Transparencia y Acceso a la información del Estado de Jalisco (LTAIJal). Publicación POE el 6 de enero de 2005, última reforma el 24 de marzo de 2011.

Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo (LTAIPMich). Publicación POE el 7 de noviembre de 2008, última reforma el 16 de julio de 2009.

Ley de Información Pública, Estadística y Protección de Datos Personales del Estado de Morelos (LIPEPDPMor). Publicación POE el 27 de agosto de 2003, última reforma el 21 de mayo de 2009.

Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit (LTAIPNay).Publicación POE el 22 de diciembre de 2007, última reforma el 29 de mayo de 2010.

Ley de Transparencia y Acceso a la Información del Estado de Nuevo León (LTAINL). Publicación POE el 19 de julio de 2008, última reforma el 5 de agosto de 2011.

Ley de Protección de Datos Personales del Estado de Oaxaca (LPDPOax).

Publicación POE el 23 de agosto de 2008.

Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla (LTAIPPbla). Publicación POE el 16 de agosto de 2004, última reforma el 18 de julio de 2008.

Ley Estatal de Acceso a La Información Gubernamental en el Estado de Querétaro (LAIGQro). Publicación POE el 27 de septiembre de 2002, última reforma el 3 de septiembre de 2010.

Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo (LTAIPQR). Publicación POE el 31 de mayo de 2004, última reforma 10 de diciembre de 2010.

Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí (LTAIPSLP). Publicación POE el 18 de octubre de 2007, última reforma el 28 de diciembre de 2010.

Ley de Acceso a la Información Pública del Estado de Sinaloa (LAIPSin). Publicación POE el 26 de abril de 2002, última reforma el 20 de agosto de 2008.

Ley de Acceso a la Información Pública del Estado de Sonora (LAIPSon). Publicación POE el 25 de febrero de 2005, última reforma el 14 de agosto de 2007.

Ley de Transparencia y Acceso a la Información Pública Del Estado de Tabasco (LTAIPTab). Publicación POE el 10 de febrero de 2007, última reforma el 26 de diciembre de 2007.

Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas (LTAIPTamps). Publicación POE 26 de diciembre de 2007, última reforma el 21 de diciembre de 2010.

Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala (LAIPyPDPTlax).Publicación POE el 12 de enero de 2007, última reforma el 26 de abril de 2011.

Ley 848 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave (LTAIPVer). Publicación POE el 27 de febrero de 2007, última reforma el 5 de julio de 2011.

Ley de Acceso a la Información Pública para el Estado y los Municipios de Yucatán (LAIPYuc). Publicación POE el 31 de mayo de 2004, última reforma el 18 de agosto de 2008.

Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas (LAIPZac). Última reforma publicada en el POE el 29 de junio de 2011.

Desarrollo legislativo en materia de datos personales en las entidades federativas, la importancia de una lesgislación especial en el ámbito estatal

Luis Gustavo Parra Noriega

Luis Gustavo Parra Noriega

Abogado por la Escuela Libre de Derecho, tiene una Maestría en Administración y Gerencia Pública por el Instituto Nacional de Administración Pública y la Universidad de Alcalá de Henares, España y realizó estudios de Doctorado en Ciencia Política y Administración, en la Universidad Autónoma de Madrid.

Actualmente, como Diputado local en el Congreso del Estado de México, es Presidente de la Comisión Especial para la Protección de Datos Personales. Entre otros trabajos legislativos recientemente presentó la Iniciativa de Ley de Protección de Datos Personales en Posesión de Entes Públicos del Estado de México y Municipios.

Como Diputado Federal durante la LX Legislatura del Congreso de la Unión, impulsó las reformas a los artículos 6º, 16 y 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de Transparencia, Acceso a la Información y protección de datos personales; además, presentó la iniciativa de Ley Federal de Protección de Datos Personales en Posesión de Particulares, hoy ley vigente.

De 2003 a 2006 fue Diputado Local en el Congreso del Estado de México. Como integrante de la LV Legislatura fue autor de las iniciativas de Ley de Transparencia y Acceso a la Información Pública en el Estado de México y del Reglamento de Transparencia del Congreso Local en ese Estado.

Introducción

Para atender sus funciones públicas, la autoridad, requiere contar con bases de datos de sus gobernados, toda vez que sería imposible brindar un servicio de salud, educativo, en materia de procuración o impartición de justicia, sin contar con datos personales de los titulares involucrados en algún trámite o procedimiento que se siga ante una autoridad. Sin embargo, la actividad de recolección y tratamiento de datos personales por parte de la autoridad, debe respetar en todo momento los principios y derechos que los titulares de los datos tienen en materia de protección de datos personales. La posesión de datos personales conlleva un riesgo importante para los titulares de los datos quienes se ven amenazados a ser objeto de su uso indebido. El desarrollo de la tecnología ha permitido que exista un alto grado de capacidad de almacenamiento de los ordenadores, así como de fórmulas que permiten correlacionar la información existente a velocidades inimaginables, que en cuestión de segundos pueden elaborar perfiles bien definidos de las personas en base a su información personal.

Y es justamente el uso indebido de los datos personales, lo que puede tener consecuencias graves para una persona que pueden ir desde la provocación de actos de molestia al titular de los datos, consistente en el envío ilimitado de información no solicitada; pasando por actos de discriminación, toda vez que mediante el cruce de información de una persona, se puede configurar un perfil respecto de sus gustos, creencias, afinidades o que decir de su estado de salud o mental, que pueden influir negativamente al momento de solicitar se le proporcione un servicio o adquiera un bien; hasta la comisión de delitos graves como el secuestro o el robo de identidad. El uso perverso de la información puede crear problemas muy serios que han convertido a la persona en un ser vulnerable que vive con la amenaza latente de ser observado en forma permanente.

En consecuencia, los datos sometidos a tratamiento deben ser utilizados en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre ellos. Por lo cual es necesario que en la recopilación y tratamiento de datos se observen ciertos principios que garanticen plenamente seguridad en el manejo de los mismos.

Estado actual del derecho a la protección de datos personales en México

En nuestro país se ha dado un importante desarrollo legislativo en materia de protección de datos personales, haciendo una clara distinción en aquella protección de datos que se encuentran en posesión de particulares y los que poseen los entes públicos para el desarrollo de sus funciones, siendo éstos últimos a los que me referiré en este artículo. Actualmente, en nuestro país, contamos con una Ley Federal de Protección de Datos Personales en Posesión de Particulares y la protección de datos en posesión de entes públicos se encuentra regulada, en ámbito federal, en la Ley Federal de Transparencia y Acceso a la Información Pública. A nivel local las leyes locales de transparencia prevén un capítulo especial sobre protección de datos personales. Los estados de Colima, Guanajuato, Oaxaca y el Distrito Federal, cuentan con una ley especial de protección de datos personales y en el estado de Jalisco, la regulación de este tema, se encuentra contenida en el Código Civil de esa entidad.

Cuadro 1. Reconocimiento de los derechos ARCO en las legislaciones locales de transparencia o de datos personales.

	ACCESO	RECTIFICACIÓN	CANCELACIÓN	OPOSICIÓN
AGUASCALIENTES	SÍ	SÍ	SÍ	SÍ
BAJA CALIFORNIA	SÍ	SÍ	SÍ	SÍ
BAJA CALIFORNIA SUR	SÍ	SÍ	NO	NO
CAMPECHE	SÍ	SÍ	NO	SÍ
CHIAPAS	SÍ	SÍ	SÍ	SÍ
CHIHUAHUA	SÍ	SÍ	SÍ	NO
COAHUILA	SÍ	SÍ	SÍ	SÍ
DISTRITO FEDERAL	SÍ	SÍ	SÍ	SÍ
COLIMA	SÍ	SÍ	SÍ	SÍ
DURANGO	SÍ	SÍ	SÍ	SÍ
GUANAJUATO	SÍ	SÍ	SÍ	SÍ
GUERRERO	SÍ	SÍ	SÍ	SÍ
HIDALGO	SÍ	SÍ	SÍ	SÍ
JALISCO	SÍ	SÍ	NO	NO
MÉXICO	SÍ	SÍ	SÍ	NO
MICHOACÁN	SÍ	SÍ	SÍ	SÍ
MORELOS	SÍ	SÍ	SÍ	NO
NAYARIT	SÍ	SÍ	NO	NO

Antecedentes legislativos en México

La primera ley en nuestro país que reguló como tal la protección de datos personales, fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental,[1] cuya aprobación fue unánime por parte de todos los Grupos Parlamentarios de la LVIII Legislatura del Congreso de la Unión. Esta Ley establece como uno de sus objetivos: *Garantizar la protección de los datos personales en posesión de los sujetos obligados.*

La citada Ley, consideró por regla general a los datos personales como información confidencial; le impuso a los sujetos obligados diversos deberes para su debida protección, basados en los principios en la materia; previó un procedimiento para su acceso y corrección por parte de los particulares, así como un recurso para el caso de la negativa por parte de la autoridad, al acceso y corrección solicitado por los particulares.

La *Exposición de Motivos de la Iniciativa de Ley Federal de Transparencia y Acceso a la Información*, que dio origen a la Ley vigente estableció que:

> Como último principio, y como parte del objeto de la Ley, se señala la protección de datos personales. Existe una clara relación entre el derecho de acceso a la información y la protección de datos personales, no porque se trate forzosamente de dos realidades contrapuestas, sino porque la regulación de ambas debe ser complementaria. En efecto, la publicidad de la información debe respetar el derecho de privacidad que corresponde a los datos personales de cualquier individuo. Para lograr la correcta armonía entre uno y otro derecho, deben especificarse lo más posible sus alcances.[2]

[1] Publicada en el Diario Oficial de la Federación el martes 11 de junio de 2002.

[2] Iniciativa de Ley Federal de Transparencia y Acceso a la Información Pública, presentada por el Ejecutivo Federal. Gaceta Parlamentaria número 892, martes 4 de diciembre de 2001.

En la citada iniciativa se advertía que el derecho de acceso a la información pública y el de protección de datos personales, eran de tal magnitud, que su diseño, contenido y alcances merecía una regulación independiente y especial, sin embargo, reconocía que, en tanto no se expidiera una ley en materia de protección de datos personales, el tema sería regulado en la Ley de Transparencia que se estaba presentando, lo cual quedó expresado en los siguientes términos:

> Existe la conciencia de que cada uno de estos derechos es de tal magnitud, que requeriría de una ley especial que regule su objeto y establezca su diseño institucional, por esta razón y mientras no se expida una ley en materia de datos personales, la iniciativa que se presenta incluye un capítulo específico relativo a este tema, en el que se recogen los principios fundamentales al respecto y que puede servir de base para la legislación futura.

Las entidades federativas y el Distrito Federal iniciaron el desarrollo legislativo de las leyes de transparencia en las cuales, siguiendo a la federal, se reguló la protección de datos personales. En el año 2007 todos los Estados y el Distrito Federal, ya contaban con su propia ley en la materia.

Sin embargo, al analizar las leyes existentes, se advirtió que prevalecía una heterogeneidad marcada la cual generaba que en cada entidad del país se regulara en forma diferente tanto el derecho de acceso a la información como el de protección de datos personales, es decir, los requisitos, procedimientos, supuestos de información reservada, plazos, sanciones, etcétera, eran diferentes dependiendo de la entidad federativa de que se tratara, lo cual generó una situación no deseable pues se trataba de un mismo derecho, pero con condiciones de ejercicio diferentes en cada Estado (López Ayllón, 2009).

Reforma al artículo 6 constitucional

Ante la heterogeneidad normativa y teniendo como antecedentes la Declaración de Guadalajara y la Iniciativa Chihuahua,[3] surgió la iniciativa de reforma al artículo 6º constitucional, cuyo dictamen,[4] elaborado por una comisión redactora integrada por legisladores de diferentes Grupos Parlamentarios de la Cámara de Diputados, se refirió a la necesidad de promover la reforma en los siguientes términos:

> …La rutina democrática que posibilita pedir información a los gobiernos sin limitaciones, luego de 33 leyes de transparencia en la Federación y los Estados, ha adquirido las más variadas tonalidades, pues los procedimientos y los arreglos institucionales, los límites, la apertura, la tecnología disponible y los documentos accesibles son muy distintos, por lo tanto la pregunta obligada es: ¿Puede un derecho fundamental tener tantas versiones como gobiernos, jurisdicciones administrativas y soberanías? ¿Puede un derecho diferenciar a los mexicanos de modo tan subrayado, dependiendo de la entidad federativa, del lugar de residencia o del nacimiento de una persona?

El dictamen previó una limitación al derecho de acceso a la información, consistente en la protección de la vida privada y los datos personales. Así esta información no estaría sujeta al principio de publicidad, pues se valoró que pondría en grave riesgo otro derecho fundamental que es el de la intimidad y la vida privada. La reforma estableció una reserva de ley, en el sentido de que corresponderá a ésta, determinar los términos de la protección y las excepciones a este derecho. De forma tal que es viable que cierta información privada o datos personales, adquieran un valor público y en consecuencia puedan ser divulgados a través de los mecanismos que determine la ley, lo cual quedó expresado en los siguientes términos:

[3] Disponible en: http://www.ifai.org.mx/Eventos/articulo6.

[4] Dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública con Proyecto de Decreto que reforma el artículo 6º de la Constitución Política de los Estados Unidos Mexicano en Gaceta Parlamentaria, Cámara de Diputados, número 2207-II, martes 6 de marzo de 2007.

> Este es el caso, por ejemplo, de los registros públicos de la propiedad, de los salarios de los funcionarios públicos o bien de la regulación del ejercicio del consentimiento del titular de la información para que ésta pueda ser divulgada. En otras palabras, existen circunstancias en que, por ministerio la ley, los datos personales podrán ser divulgados sin el consentimiento del titular.
>
> En otros casos, la ley deberá prever la posibilidad de que, algunos datos personales, puedan ser divulgados cuando un órgano jurisdiccional o administrativo determine que existen razones particulares que justifiquen su divulgación, previa garantía de audiencia del implicado. De cualquier forma, las autoridades deberán realizar una cuidadosa ponderación que justifique el hecho de que una información que pertenece al ámbito privado, puede ser divulgada por así convenir al interés público.[5]

Por otra parte, la reforma estableció que el acceso y rectificación de datos personales, no pueden estar condicionados; no se debe requerir al gobernado identificación alguna, ni acreditación de un interés.

En consecuencia, el hecho de no requerir acreditación de interés alguno en el ejercicio de estos derechos implica que únicamente se requerirá acreditar la identidad de su titular para su acceso y la procedencia de su rectificación, en su caso. La misma fracción establece el principio de gratuidad en el de acceso o rectificación de los datos personales. Resulta pertinente precisar que este principio se refiere a los procedimientos de acceso o rectificación de datos personales, no así a los eventuales costos de los soportes en los que se entregue la información (por ejemplo soportes magnéticos, copias simples o certificadas), ni a los costos de entrega por mecanismos de mensajería cuando así lo solicite el particular. Los medios de reproducción y los costos de envío tienen un costo, no así la información.

Las reformas al artículo 6º constitucional, referentes al derecho a la protección de datos personales, quedaron expresadas de la siguiente forma:

[5] Idem.

> Artículo 6. …
> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> I. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> II. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
> ...

Reforma del artículo 16 Constitucional

Con la reforma al artículo 6º constitucional, por primera vez se hace referencia en la Carta Magna a la protección de datos, sin embargo es importante resaltar que se hace como un límite al derecho de acceso a la información, por lo que posteriormente el legislador aprobó la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, la cual tuvo como propósito consolidar el derecho a la protección de datos personales en nuestro país, apuntalando la estructura edificada a través de la fracción segunda del artículo sexto constitucional y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales, y de acuerdo al dictamen[6] de la Cámara de Diputados, que dio origen a esta reforma: *reconociendo la existencia del mismo respecto de los datos personales en poder de particulares*.

La reforma al artículo 16 de nuestra Constitución Política, reconoció al máximo nivel de nuestra pirámide normativa, la existencia de un

[6] Dictamen de la Comisión de Puntos Constitucionales con Proyecto de Decreto por el que se adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos en Gaceta Parlamentaria, Cámara de Diputados, número 2653-II, jueves 11 de diciembre de 2008.

nuevo derecho distinto y fundamental dentro del catálogo de garantías: el derecho a la protección de datos personales. Este nuevo derecho presenta caracteres propios que le dotan de una naturaleza autónoma, de tal forma que su contenido esencial lo distingue de otros derechos fundamentales:

La citada reforma publicada en el Diario Oficial de la Federación el primero de junio de dos mil nueve quedó aprobada en los siguientes términos:

> Artículo 16 …
> Toda persona tiene derecho a la protección de sus datos personales, el 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 públicas o para proteger los derechos de terceros.
> …

La reforma da contenido al derecho a la protección de datos personales, se reconoce al gobernado el derecho a disponer de manera libre, informada y específica sobre el tratamiento de los datos personales que le conciernan, sobre la base del consentimiento del titular de los datos personales. Derivado de la reforma, el ciudadano tiene el derecho de exigir la protección de sus datos personales, a través de los derechos de acceso, rectificación, cancelación y oposición, conocidos por su acrónimo ARCO en la doctrina en el ámbito internacional y a los que me referiré más adelante. Se deja a la ley secundaria establecer 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 públicas o para proteger los derechos de terceros.

En el dictamen por el que se aprobó la citada reforma al artículo 16 constitucional, hicimos referencia a que el derecho a la protección de datos personales consiste en la protección a la persona, en relación con la utilización que se dé a su información personal, tanto por entes públicos como privados; asimismo, se refirió a que *la estructura*

propuesta serviría de punto de partida para cualquier regulación que se emita en torno al derecho a la protección de datos, tanto en el ámbito público como en el privado.

Reforma al artículo 73 constitucional

Por lo que se refiere a la protección de datos personales en posesión de entes privados, desde la LVII Legislatura del Congreso de la Unión, legisladores de todos los Grupos Parlamentarios presentaron Iniciativas para regular la protección de datos personales, sin embargo ante la falta de un precepto constitucional que facultara al Congreso de la Unión para legislar en materia de datos personales, la dictaminación de la propuesta en Comisiones no prosperaba.

Ante esa situación, presenté la Iniciativa de reforma al artículo 73 de la Constitución General, a efecto de dotar de atribuciones al Congreso de la Unión, para legislar en materia de protección de datos personales en posesión de particulares.[7]

En la Iniciativa se reconoció que el Congreso de la Unión, en términos de nuestro esquema de división de competencias entre los órdenes de gobierno del Estado mexicano, no contaba con facultades expresas para legislar sobre la materia, y el establecimiento de marcos legislativos diversos en materia de protección de datos personales, por parte de las entidades federativas, podía dispersar el esfuerzo estatal por tutelar los aspectos más sensibles de la información personal, en perjuicio de los titulares de los mismos, establecer condiciones que restringieran el comercio entre las propias entidades federativas, y resultar contrario a los lineamientos adoptados por los organismos internacionales de los cuales forma parte el Estado mexicano.

Por lo tanto, las razones que sustentaron que la ley para proteger los datos personales en posesión de los particulares, tuviera un ámbito de aplicación nacional, fueron por una parte, la necesidad de unificar la tutela de un derecho fundamental en todo el país, en cuanto a derechos, principios y procedimientos de tutela, evitando de esta

[7] Iniciativa que reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Publicada en la Gaceta Parlamentaria número 2221-I, de fecha martes 27 de marzo de 2007 y publicada en el Diario Oficial de la Federación de fecha jueves 30 de abril de 2009.

manera su respeto y protección asimétricos al expedirse tantas leyes como entidades federativas tiene la República mexicana; y por otro lado, se tomó en cuenta que la materia de comercio es federal, de conformidad con nuestra Ley fundamental.

Finalmente la iniciativa prosperó y fue reformado por los órganos que integran el Poder Reformador de la Constitución el artículo 73 de nuestra Carta Magna, estableciéndose la competencia para que el Congreso de la Unión se constituyera en fuente normativa en materia de datos personales en posesión de particulares, de la siguiente forma:

> Artículo 73. El Congreso tiene facultad:
> I. a XXIX-N...
> XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.
> ...

Al contar el Congreso de la Unión con la facultad para legislar en la materia, se presentó en la LX Legislatura la Iniciativa de Ley de Protección de Datos Personales en Posesión de Particulares,[8] la cual tuvo por objeto la protección de los datos personales contenidos en bases de datos en posesión de particulares, con la finalidad de garantizar el derecho al honor, imagen y vida privada de las personas.

En la LXI Legislatura, la iniciativa fue dictaminada junto con otras que fueron presentadas en diferentes Legislaturas y por diversos Grupos Parlamentarios.[9] Las iniciativas presentadas coincidían en establecer los principios y derechos en materia de protección de datos personales; hacían la propuesta de una autoridad que regulara dicha protección e hiciera efectivo el cumplimiento de esos principios y derechos; se regulaba un procedimiento para ejercer los derechos en la materia; y se establecían causales de responsabilidad y sanciones por el incumplimiento a las disposiciones contenidas. Finalmente, el

[8] Iniciativa de Ley de Protección de Datos Personales en Posesión de los Particulares presentada por el Dip. Gustavo Parra Noriega, Publicada en la Gaceta Parlamentaria, número 2607-III, martes 7 de octubre de 2008.

[9] Dictamen de la Comisión de Gobernación, con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicado en la Gaceta Parlamentaria número 2984-IV, jueves 8 de abril de 2010.

dictamen fue aprobado y publicada la Ley Federal de Protección de Datos Personales en Posesión de Particulares en el Diario Oficial de la Federación el 5 de julio de 2010.

Justificación de la creación de Leyes estatales de Protección de Datos Personales en posesión de Entes Públicos

La dispersión legislativa y la heterogeneidad que existe en la regulación del tema de datos personales en posesión de entes públicos en nuestro país,[10] advierte sobre la necesidad de legislar la materia en forma homogénea, con contenidos normativos que le den forma y contenido a los derechos y principios de protección de derechos personales. En el tema existen razones justificadas para expedir una ley independiente a la de transparencia que regule específicamente este derecho fundamental.

El derecho de acceso a la información pública y el de protección de datos personales, son dos derechos autónomos e independientes entre los cuales debe existir un sano equilibrio que permita que en algunas ocasiones en aras del interés público se divulgue determinada información de carácter personal.

El derecho a la protección de datos personales es un derecho diferente y distinguible del derecho de acceso a la información pública y constituye una limitación al derecho de acceso a la información pública.

Por otra parte, el derecho de acceso a la información pública se rige por principios y criterios distintos al de la protección de datos personales. El derecho de acceso a la información se rige por el principio de máxima publicidad, previsto en el artículo 6º párrafo segundo, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, por el cual *Toda información en posesión de cualquier*

[10] En el Estudio *Métrica de la Transparencia 2010*, elaborado por el Centro de Investigación y Docencia Económicas, CIDE, se advierte que existen problemas importantes en el diseño de la legislación en materia de datos personales, por lo que se trata de áreas de oportunidad para mejorar la legislación. Estudio disponible en: http://www.metricadetransparencia.cide.edu/metrica.html.

autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

Mientras que el derecho de protección de datos personales, se rige por el principio de máxima reserva, el cual implica que el gobierno debe de conocer el mínimo indispensable de sus gobernados para llevar a cabo sus funciones.

Es por lo anterior que resulta plenamente justificado que exista una legislación independiente y especial para la protección de los datos personales, el cual con las citadas reformas a los artículos 6º y 16 de nuestra Carta Magna, se perfila como un derecho fundamental, como un derecho humano que con la reciente reforma constitucional en materia de derechos humanos publicada en el Diario Oficial de la Federación el 10 de junio de 2011, adquiere una nueva concepción y reformulación. Con la reforma, el artículo 1º de la Constitución federal establece que:

> En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

En el diseño y contenido del derecho a la protección de datos personales en nuestro país, han influido diversos instrumentos internacionales con los que México ha asumido compromisos, tales como la Declaración de los Derechos del Hombre, el Convenio para la Protección de los Derechos y Libertades Fundamentales, el Pacto Internacional de los Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos. Por lo que a partir de la reforma constitucional en materia de derechos humanos, estos compromisos asumen una dimensión especial ante el reconocimiento y tutela de los derechos fundamentales contenidos en ellos. Y por otra parte, la reforma constitucional plantea un tema de especial importancia contenido en el tercer párrafo del citado artículo primero, el cual

prevé en materia de principios y obligaciones en materia de derechos humanos lo siguiente:

> Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

Sin duda, el derecho a la protección de datos personales es un derecho fundamental que se va a circunscribir bajo la nueva concepción de los derechos humanos y a todas luces podemos afirmar que para su tutela es conveniente que exista una legislación propia, distinta de la regulación del derecho de acceso a la información, que regule sus propios principios, derechos, procedimiento para su ejercicio, autoridad garante y régimen de responsabilidades.

A manera de ejemplo, en el Congreso del Estado de México, el derecho a la protección de datos personales, se encuentra regulado en la Ley de Transparencia y Acceso a la Información del Estado de México en un capítulo especial, el cual adolece de diversos elementos mínimos que deben regir en este tema, por lo cual, presenté el 11 de agosto del año en curso, la Iniciativa de Ley de Protección de Datos Personales en Posesión de entes públicos del Estado de México y Municipios, actualmente en estado de dictaminación, la cual contiene los principios, derechos, procedimiento, autoridad garante, medidas de seguridad y régimen de responsabilidades que deben contener las leyes que se expidan en la materia para estar a la vanguardia en la regulación de este derecho fundamental.

Mínimos normativos de las leyes estatales de protección de datos personales

Ámbito de competencia

Es necesario dejar en claro que tratándose de la protección de datos personales en posesión de entes públicos, la competencia correspondiente en su respectivo ámbito, a la federación y a las entidades federativas.[11] Por lo que respecta a la posesión de datos personales en posesión de los particulares, esta materia sólo puede ser regulada por el Congreso de la unión, en términos de lo previsto en nuestra Constitución federal en su artículo 73, fracción XXIX-O, el cual prevé la facultad del Congreso para legislar en materia de protección de datos personales en posesión de particulares.

Asimismo el artículo tercero transitorio de dicha reforma, estableció que:

> Tercero.- En tanto el Congreso de la Unión expide la ley respectiva a la facultad que se otorga en este Decreto, continuarán vigentes las disposiciones que sobre la materia hayan dictado las legislaturas de las entidades federativas, tratándose de datos personales en posesión de particulares.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, por lo que de acuerdo a establecido en nuestra Ley Fundamental, la legislación en materia de protección de datos personales en posesión de particulares es objeto exclusivo de esa Ley federal, en tanto la legislación estatal en materia de protección de datos personales, debe atender exclusivamente a aquellos datos personales que obran en poder de entes públicos. Es decir, la regulación que se de en los Estados y el Distrito Federal en materia de protección de

[11] Como ya se indicó en la sección II, la posesión de datos personales en posesión de particulares, la competencia es exclusiva del Congreso de la Unión, en virtud de la necesidad de unificar la tutela de un derecho fundamental en todo el país, en cuanto a derechos, principios y procedimientos de protección, evitando así su cumplimiento asimétrico al expedirse tantas leyes como entidades federativas tiene nuestro país.

datos personales, deberá abordar única y exclusivamente la tutela de los datos personales en posesión de entes públicos.

Principios en materia de protección de datos personales

Toda la legislación en materia de protección de datos personales, debe contar con principios que rijan el tratamiento de datos personales y en los cuales se oriente la protección de datos personales. Existen diversos principios que desde hace tiempo han sido reconocidos internacionalmente por importantes organismos internacionales como la OCDE y la APEC. Resulta esencial que las legislaciones locales prevean al menos los siguientes principios:

a) Principio del Consentimiento

El consentimiento es un principio exigido en la mayoría de las disposiciones legales que existen en la materia, se configura como una manifestación de voluntad libre, específica, informada e inequívoca mediante la que el interesado consiente el tratamiento de sus datos de carácter personal. Se considera la piedra angular o el eje central de las legislaciones en la materia, se trata del derecho que tiene el titular de los datos personales para decidir quién, cómo, cuándo y para qué se tratarán sus datos.

Las características que debe tener el consentimiento del titular es que debe ser libre, es decir obtenido sin la intervención de vicio alguno de la voluntad; específico, referido a una determinada finalidad; inequívoco al existir expresamente una acción que implique su otorgamiento; e informado, es decir, otorgado con el conocimiento de las finalidades para las que el mismo se produce.

El consentimiento es uno de los principios que legitima el tratamiento de datos de carácter personal de los interesados. Puede estar sometido a excepciones en virtud de obligaciones legales: en el caso de que el tratamiento de datos derive de una relación contractual; exista una situación de emergencia que pueda dañar potencialmente a un individuo en su persona o bienes; sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios,

mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos legales aplicables; o bien, cuando los datos figuren en fuentes de acceso público.

Repercute en que los Sujetos Obligados no podrán difundir o transmitir los datos personales contenidos en las bases de datos que tengan en el ejercicio de las funciones a su cargo, excepto que haya estado de por medio el consentimiento de los titulares de los datos.

Al regular este tema, debe preverse la revocación del consentimiento y el régimen de excepciones, sin que ello signifique efectos retroactivos respecto al tratamiento efectuado de los datos antes de la revocación.

b) Principio de Finalidad

Se refiere a que el tratamiento de datos personales sea llevado a cabo únicamente en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del responsable. De acuerdo a este principio, el tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. En caso de que el responsable pretenda tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

c) Principio de Proporcionalidad

El principio de proporcionalidad, se encuentra directamente relacionado al de finalidad, alude a que los datos sólo deberán ser los adecuados o necesarios para la finalidad que justifica el tratamiento. A la luz de este principio, el responsable deberá únicamente tratar datos proporcionales para la finalidad para la que se obtuvieron.

Este principio ha sido analizado por los distintos derechos regionales o nacionales desde dos perspectivas distintas, aunque complementarias: Por una parte, los datos sólo deberían ser los adecuados o necesarios para la finalidad que justifica el tratamiento; por otra, quien realiza el tratamiento de los datos deberá analizar las finalidades que justifican el tratamiento, de modo que sólo debería tratar la mínima cantidad de información necesaria para conseguir la finalidad que se persigue (principio de minimización).

d) Principio de Calidad

El Principio de Calidad de Datos, se refiere a que los datos que se recaben deberán ser pertinentes, adecuados y no excesivos para el fin que se pretenda en su tratamiento. El principio de calidad se encuentra vinculado con la veracidad y exactitud en la que se mantienen los datos personales. Se ve plasmado al establecerse que los datos personales contenidos en las bases de datos deberán ser exactos y actualizados; aquellos que sean inexactos o incompletos deber ser suprimidos y sustituidos o bien, completados por el responsable de la base de datos.

e) Principio de Información

Se refiere al derecho que tiene el titular de los datos personales de ser informado sobre la finalidad de la recolección de sus datos. Implica que el interesado tenga el control del tratamiento que se le darán a sus datos de carácter personal. Para dar cumplimiento al principio de información, debe estar prevista la obligación a cargo de las autoridades que posean bases de datos personales, de proporcionar la información a los titulares de los datos en forma clara y entendible, sobre el tratamiento que se dará a sus datos personales.

Se debe garantizar al titular de los datos que está plenamente informado sobre el tratamiento que se le dará a sus datos personales. Se le debe comunicar, entre otras cosas, de la existencia de un sistema o base de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información. Asimismo, se le debe informar del carácter obligatorio o facultativo de responder a las preguntas que le sean planteadas; de las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos; de la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por ley sean públicos; de la posibilidad de ejercitar los derechos y del nombre del responsable del sistema o base de datos personales.

f) Principio de Seguridad

La seguridad en materia de protección de datos es una de las cuestiones de mayor preocupación en el tratamiento de datos. Su

finalidad es impedir el acceso a los sistemas de datos personales a personas no autorizadas o bien, evitar el desvío de la información hacia sitios no previstos. A la luz de este principio, se debe garantizar que únicamente el responsable del sistema de datos personales o en su caso, los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

Los entes públicos deben establecer medidas de carácter técnico y organizativo para garantizar la confidencialidad e integralidad de cada sistema o base de datos personales que posean, con la finalidad de garantizar el pleno ejercicio de los derechos tutelados, frente a su alteración, pérdida, transmisión y acceso no autorizado.

Las medidas deben ser adoptadas de acuerdo al menor o mayor grado de protección que ameriten los datos personales, debiendo constar por escrito y ser comunicadas a la autoridad encargada de protección de datos de la entidad federativa, para su correspondiente registro. En este sentido se aconseja la elaboración del documento de seguridad que desarrolle las medidas de seguridad de índole técnica y organizativa a aplicar en cada caso.

g) Principio de Confidencialidad

Es un deber que debe observarse por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo. Consiste en garantizar que exclusivamente la persona interesada pueda acceder a los datos personales o, en su caso el responsable del sistema o base de datos personales para su tratamiento.

Derechos en materia de protección de datos personales

Los derechos de acceso, rectificación, cancelación y oposición, denominados derechos ARCO son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales. El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, prevé claramente los 4 derechos, los cuales constituyen la columna vertebral de la protección de datos personales.

En consecuencia se considera necesario que todas las legislaciones estatales prevean en la regulación que diseñen sobre este tema que nos ocupa los siguientes derechos:

El *derecho de acceso* corresponde a cualquier persona física para obtener información sobre sus datos de carácter personal sometidos a tratamiento. En el caso del *derecho de rectificación*, es procedente cuando los datos que sean tratados resulten inexactos, incompletos, inadecuados o excesivos, es decir, los datos tienen que cumplir con el principio de calidad. El *derecho de cancelación* es el derecho de solicitar el bloqueo de los datos personales cuando hayan sido objeto de tratamiento en violación a alguno de los principios en la materia. Finalmente, las personas tienen el *derecho a oponerse al tratamiento* de sus datos cuando hayan sido recabados sin su consentimiento.

De una revisión en las leyes locales de transparencia y las leyes de protección de datos que existen en los Estados, se observa una regulación asimétrica de los derechos de acceso, rectificación, cancelación y oposición, los llamados derechos "ARCO". La heterogeneidad prevalece en la regulación de los derechos de cancelación y oposición, para los cuales en muchos casos, su regulación no se prevé. En algunas entidades federativas como Tlaxcala, llegamos a encontrar hasta siete derechos en materia de protección de datos, tales como el de acceso, inclusión, complementación, rectificación, suspensión, reserva y cancelación de datos personales.[12]

Por lo que respecta al derecho de oposición, éste se encuentra regulado en varias entidades federativas como Campeche, Tlaxcala, Querétaro, Quintana Roo, Oaxaca y Sonora, como el derecho del titular de los datos a oponerse a la publicación de sus datos personales en resoluciones o sentencias que emita la autoridad judicial.

En algunas legislaciones como la de Oaxaca, Jalisco, Durango se regulan los datos personales de los fallecidos, tema que amerita una reflexión especial para el diseño de su legislación, ya que fue objeto de debates polémicos en el Instituto Federal de Acceso a la Información Pública y Protección de Datos, al resolver el recuso de

[12] Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala. Artículo 42, fracción IV. Disponible en al 15 de noviembre en http://www.ifai.org.mx/Vinculacion/directorioL.

revisión 3751/2009[13] ante la negativa de la Secretaría de Seguridad Pública de atender la solicitud de un particular que requería: *Solicitud de documentos que muestren la lista de prisioneros fallecidos en el Penal de Máxima Seguridad del Altiplano desde el año 2000*; así como *Solicitud de copia de los expedientes médicos de todos los prisioneros fallecidos desde el 2000 en el Penal de Máxima Seguridad del Altiplano*.

El caso dio lugar a un intenso debate entre los Comisionados del IFAI, en el que se llegó a una votación dividida que por una parte, confirmó la reserva de los nombres de los prisioneros fallecidos invocando el derecho al olvido y la afectación al derecho a la privacidad de los familiares, así como los potenciales efectos discriminatorios para ellos por la revelación de la información.

Y por otra parte, se instruyó al sujeto obligado a entregar en versión pública los expedientes clínicos de los prisioneros fallecidos, argumentando que existe un interés público en otorgar acceso a la información contenida en los expedientes clínicos, debido a que la divulgación de dicha información *da cuenta o puede arrojar luz sobre el actuar del sujeto obligado y permite contrastarlo con sus obligaciones legales relativas a la atención de salud y a la obligación de velar por la integridad física de los sujetos que le son entregados en custodia*.

Sin duda se trató de un caso que puso de manifiesto el dilema que existe entre el derecho de acceso a la información y la protección de datos personales y con el que podemos confirmar que el tema que nos ocupa, es un tema que presenta retos importantes y en el que resulta trascendental el estudio del caso en concreto.

[13] Recurso de Revisión Instituto Federal de Acceso a la Información y Protección de Datos. IFAI. Expediente 3751/2009. Disponible en al 15 de noviembre de 2011 en http://www.ifai.org.mx/Sesiones/Consulta.

Cuadro 1. Reconocimiento de los derechos ARCO en las legislaciones locales de transparencia o de datos personales.

	ACCESO	RECTIFICACIÓN	CANCELACIÓN	OPOSICIÓN
AGUASCALIENTES	SÍ	SÍ	SÍ	SÍ
BAJA CALIFORNIA	SÍ	SÍ	SÍ	SÍ
BAJA CALIFORNIA SUR	SÍ	SÍ	NO	NO
CAMPECHE	SÍ	SÍ	NO	SÍ
CHIAPAS	SÍ	SÍ	SÍ	SÍ
CHIHUAHUA	SÍ	SÍ	SÍ	NO
COAHUILA	SÍ	SÍ	SÍ	SÍ
DISTRITO FEDERAL	SÍ	SÍ	SÍ	SÍ
COLIMA	SÍ	SÍ	SÍ	SÍ
DURANGO	SÍ	SÍ	SÍ	SÍ
GUANAJUATO	SÍ	SÍ	SÍ	SÍ
GUERRERO	SÍ	SÍ	SÍ	SÍ
HIDALGO	SÍ	SÍ	SÍ	SÍ
JALISCO	SÍ	SÍ	NO	NO
MÉXICO	SÍ	SÍ	SÍ	NO
MICHOACÁN	SÍ	SÍ	SÍ	SÍ
MORELOS	SÍ	SÍ	SÍ	NO
NAYARIT	SÍ	SÍ	NO	NO
NUEVO LEÓN	SÍ	SÍ	SÍ	SÍ
OAXACA	SÍ	SÍ	SÍ	SÍ
PUEBLA	SÍ	SÍ	NO	NO
QUERÉTARO	SÍ	SÍ	NO	SI
QUINTANA ROO	SÍ	SÍ	NO	NO
SAN LUIS POTOSÍ	SÍ	SÍ	SÍ	NO
SINALOA	SÍ	SÍ	SÍ	NO
SONORA	SÍ	SÍ	SÍ	NO
TABASCO	SÍ	SÍ	SÍ	SI
TAMAULIPAS	SÍ	SÍ	SÍ	NO
TLAXCALA	SÍ	SÍ	SÍ	SÍ
VERACRUZ	SÍ	SÍ	SÍ	SÍ
YUCATÁN	SÍ	SÍ	SÍ	NO
ZACATECAS	SÍ	SÍ	SÍ	SÍ

Fuente: Elaboración propia con información del Instituto Federal de Acceso a la Información y Protección de Datos http://www.ifai.org.mx/Vinculacion/directorioL

SÍ: Se identificó regulación en la Ley de Transparencia o de protección de datos personales del Estado.
NO: No se identificó regulación en la Ley de Transparencia del Estado.

Transferencia de datos personales

Un aspecto importante a considerar en las legislaciones estatales en materia de protección de datos personales, es la transferencia o cesión de bases de datos, en las cuales es necesario prever que el responsable deberá comunicar a los terceros las finalidades a las que el titular sujetó el tratamiento, debiendo respetar el tercero esas finalidades y asumir las mismas obligaciones del responsable que hizo la transferencia de datos.

Es decir, se deben asegurar niveles semejantes de seguridad y protección de datos personales cuando se realice alguna transferencia de ellos.

De un análisis a la legislación estatal sobre esta materia, se advierte que existen variaciones importantes en la forma en que se encuentra regulado este tema en los estados, en algunos no se regula el tema y en otros como Tabasco[14] se establece que no se requerirá el consentimiento de los individuos para proporcionar los datos personales, entre otros casos cuando la información sea requerida para la prestación de un servicio contratado a particulares por los Sujetos Obligados. En este caso, la entrega de información se hará una vez que se haya cubierto una fianza y sólo se utilizará para los propósitos estrictamente señalados en el contrato. Una vez terminado el contrato particular devolverá los datos personales que para uso exclusivo y temporal le fueron otorgados por el Sujeto Obligado.

Límites o excepciones a los principios o derechos

Otro tema que es necesario regular en las leyes estatales para la protección de datos, se refiere a los límites o excepciones a los principios o derechos de protección de datos personales, los cuales se dan cuando se presentan situaciones en las que el tratamiento de datos es necesario, sin necesidad de consentimiento del interesado, en virtud de la protección de la seguridad nacional, el orden, la seguridad

[14] Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Artículo 58 fracción V. Disponible en http://www.ifai.org.mx/Vinculacion/directorioL.

y la salud públicos, así como los derechos de terceros. En cualquier caso, dichas situaciones deberán estar previstas en la ley.

Si analizamos la Ley Federal de Protección de Datos Personales en Posesión de Particulares, observamos que en ella se establecen diversos supuestos en los cuales no es necesario el consentimiento para el tratamiento de los datos personales, o los casos en que el responsable no está obligado a cancelar los datos o bien, se regulan aquellos supuestos en los cuales las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular. Algunos de los casos en los cuales dicha Ley Federal no exige el consentimiento para el tratamiento de datos personales, son los siguientes: cuando los datos figuren en fuentes de acceso público; los datos personales se sometan a un procedimiento previo de disociación; exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.

Entre los casos en los cuales en la referida Ley Federal se estima que el responsable no estará obligado a cancelar los datos personales encontramos: Cuando deban ser tratados por disposición legal; obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delito o la actualización de sanciones administrativas; sean necesarios para proteger los intereses jurídicamente tutelados del titular o bien; sean necesarios para realizar una acción en función del interés público.

Régimen de responsabilidades específico en materia de protección de datos personales

Otro tema importante a considerar en las legislaciones estatales en la materia que nos ocupa, es el referente al esquema de responsabilidades de los servidores públicos que tratan datos personales. En este caso,

deberán preverse conductas específicas que constituyan infracciones en la materia.

Las causales de responsabilidad deberán preverse en función de la transgresión a los derechos o principios en materia de protección de datos personales. Entre las causales que darían origen a responsabilidades encontramos las siguientes:

- No atender la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin que exista razón fundada;
- Declarar dolosamente la inexistencia de datos personales, cuando estos existan;
- Incumplir con el deber de confidencialidad;
- Transferir datos a terceros en contravención a la ley;
- Recabar datos en forma engañosa o fraudulenta; o,
- Vulnerar la seguridad de bases de datos.

Sobre este tema la mayor parte de las legislaciones locales prevén disposiciones específicas, sin embargo se llega a detectar que en algunos casos el régimen de responsabilidades se refiere al derecho de acceso a la información, siendo omiso en las causales de responsabilidad específicas en materia de protección de datos personales.

Mecanismos de defensa ante el Órgano Garante

Otro aspecto que resulta indispensable regular en las legislaciones estatales es el medio de impugnación (regularmente el llamado recurso de revisión), cuando el titular de los datos se considere agraviado por alguna resolución a su solicitud de acceso, rectificación, cancelación u oposición de datos. En este sentido, es necesario prever la orientación que los sujetos obligados deberán dar al titular sobre su derecho de interponer el recurso de revisión y el medio y plazo para interponerlo. Entre los casos por los cuales se prevé la impugnación ante el Órgano

garante encontramos, los siguientes: La falta de respuesta por parte del responsable de la base de datos; la entrega incompleta de las solicitudes de acceso a datos personales; y, la negativa injustificada para realizar la cancelación o rectificación de datos personales.

Además es importante que las resoluciones del órgano garante sean definitivas e inatacables para los sujetos obligados, así como establecer mecanismos que garanticen que los procedimientos serán expeditos.

Órgano garante con facultades adecuadas

Se recomienda que en las entidades federativas el órgano garante en materia de protección de datos personales sea el mismo que en materia de acceso a la información, pues es indispensable que exista una homogeneidad de criterios para evitar que la protección de los datos personales se constituya en un obstáculo para la transparencia y la rendición de cuentas.

El órgano garante debe tener autonomía y suficiencia presupuestaria y tener entre sus facultades, las de resolver los recursos de revisión, conciliar interés entre el titular de los datos y los sujetos obligados, emitir recomendaciones en las materia de la Ley, resolver las quejas por posibles violaciones a la Ley, promover la cultura de la protección de datos, entre otras. A continuación se detallan algunas de las facultades referidas.

a) Conciliación entre el titular de los datos y el sujeto obligado

Otro aspecto que se considera importante prever en las legislaciones locales que regulen el tema que nos ocupa es el de la conciliación. Entendida como un medio alterno para resolver algún conflicto entre el titular de los datos personales y el sujeto obligado. El Órgano garante deberá procurar la conciliación entre ambas partes y de llegarse a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes, debiendo el Órgano garante verificar el cumplimiento del acuerdo respectivo.

b) Facultad de Verificación del Órgano Garante

Es necesario que las leyes locales de datos personales, prevean facultades de verificación o inspección para los Órganos garantes con la finalidad de verificar el cumplimiento de la normatividad en materia de protección de datos personales; identificar violaciones a los derechos de acceso, rectificación, cancelación u oposición de datos personales; o bien, la detección del tratamiento ilícito de los datos personales. La verificación tendrá lugar, ya sea de oficio o a petición de parte.

De una revisión al tema en las leyes de transparencia de los estados o leyes locales sobre datos personales, se observa que en muchos estados no se prevé la facultad de verificación del Órgano garante, en algunos como el de Nayarit, se prevé la verificación de forma genérica y en otros como Michoacán, sólo en caso de que existan violaciones a la ley.

c) Registro de Datos Personales

Se considera importante establecer en la legislación de datos personales la existencia de un Registro de los sistemas de datos personales que obren en poder de los entes públicos con la finalidad de que los titulares de los datos personales tengan conocimiento de la existencia de las bases o sistemas de datos que poseen las autoridades y permitir el ejercicio de sus derechos ARCO. El registro debe comprender como mínimo la información siguiente: Finalidad del sistema de datos personales; naturaleza de los datos contenidos; nombre y cargo del responsable y de los usuarios del sistema de datos; forma de recolección y actualización de los datos; destino de los datos; tiempo de conservación de los datos personales; y, medidas de seguridad. Son pocas las entidades federativas que prevén la regulación de un Registro de Datos Personales, algunos como es el caso de Quintana Roo, no se refiere a un Registro como tal, sino a un listado de los sistemas de datos personales.[15]

[15] Ley de Transparencia y Acceso a la Información del Estado de Quintana Roo. Artículo 31. Disponible en http://www.ifai.org.mx/Vinculacion/directorioL

d) Medidas de seguridad de datos personales

La seguridad en el tratamiento de los datos de carácter personal es vital para garantizar de forma efectiva la privacidad de las personas, la autoridad responsable deberá mantener la integridad y exactitud de la información personal, estableciendo controles o medidas que impidan el acceso indebido a la información así como la pérdida total o parcial de los datos o su alteración.

Las medidas que se implementen para tal efecto deberán ser de carácter técnico, físico y organizativo, que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad.

La autoridad responsable de los sistemas de datos personales debe proteger los datos de carácter personal que sometan a tratamiento mediante la implementación de dichas medidas.

Además, el principio de seguridad implica la obligación de tomar todas aquellas medidas pertinentes para evitar el desvío de la información hacia sitios no previstos, así como tomar las medidas pertinentes para que de llegar a existir vulneraciones de seguridad en el tratamiento de datos, se informe de forma inmediata al titular, a fin de que éste pueda tomar las medidas correspondientes en la defensa de sus derechos.

La mayor parte de los Estados y el Distrito Federal, poseen disposiciones generales relativas a las medidas de seguridad, aunque es necesario que en las regulaciones estatales se haga referencia a cada una de ellas, haciendo referencia a las medidas de seguridad de carácter técnico, físico y organizativo.

Algunas legislaciones como la del Distrito Federal y Nuevo León, prevén en forma integral, diversos tipos de seguridad (física, lógica, de desarrollo y aplicaciones, de cifrado y de comunicaciones y redes), atendiendo a la naturaleza de los datos, estos niveles se traducen en medidas más bien de carácter informático cuya inclusión, si bien refleja que se trata de normatividades muy completas, no se considera indispensable en la ley. Lo que sí es necesario en la Ley es el establecimiento de plazos perentorios para implementar medidas de

seguridad y la facultad del órgano garante para emitir recomendaciones en esta materia, así como la facultad de inspección para verificar que los sujetos obligados cumplan con las recomendaciones emitidas.

e) Cultura de protección de datos personales

La promoción de la cultura de la protección de datos personales es indispensable para fortalecer el ejercicio de este derecho, lo cual se puede lograr a través del fortalecimiento en el trabajo de difusión y educación con todos los sectores de la población.

El derecho de protección de datos personales debe permear a todos los sectores de la población ya que éste no es privativo de unos cuantos, por lo que es necesario plantear desde el Poder Legislativo de cada entidad federativa aquellas reformas que permitan a todos los habitantes de nuestro país ejercer su derecho.

Otra propuesta legislativa de corte educativo en este tema consiste en la promoción de mecanismos de participación con instituciones educativas, a través de la investigación, difusión y docencia de materias cuyo contenido sea la protección de datos; así como la realización de cursos, seminarios, talleres en la materia; y la inclusión en los planes de estudios del derecho a la protección de datos personales visto como un derecho fundamental.

Conclusiones

La legislación en materia de protección de datos personales en nuestro país se encuentra en una etapa de plena construcción, aunque ya se cuenta con regulación constitucional y legal en el tema, en el ámbito federal, su regulación en los estados es asimétrica, cada estado prevé parámetros y formas de regulación heterogénea, lo cual genera que la protección de datos personales sea distinta dependiendo de la entidad federativa en la que nos encontremos, por lo que se considera necesario alinear la legislación que existe en la materia, de acuerdo a los principios y derechos que establecen los artículos 6º y 16 de la Constitución Política de los Estados Unidos Mexicanos, además respetando en todo momento las recientes reformas al artículo 1º

constitucional en materia de derechos humanos, al ser el derecho a la protección de datos personales, un derecho fundamental.

La protección de datos personales, plantea retos importantes tanto para el legislador como para la autoridad encargada de la aplicación de la ley, especialmente en temas en los que el derecho a la protección de datos personales presenta tensiones con otros derechos tales como el de seguridad pública, procuración e impartición de justicia, y es justamente en estos temas donde el legislador debe ser cuidadoso para diseñar una legislación que permita a la autoridad llegar a un sano equilibrio entre esos derechos.

El derecho fundamental a la protección de datos personales en posesión de entes públicos merece un diseño legislativo propio a través de una ley especial e independiente a la de transparencia y acceso a la información. El marco normativo local que se expida en la materia deberá contener regulados su ámbito de aplicación, los principios, derechos, procedimiento para ejercer su tutela, autoridad responsable, medidas de seguridad, transferencias y régimen de responsabilidades que son propios y característicos de los datos personales.

Referencias

Centro de Investigación y Docencia Económicas (2010) *Métrica de la Transparencia 2010*, estudio disponible al 10 de noviembre de 2011 en: http://www.metricadetransparencia.cide.edu/metrica.html.

Dictamen de la Comisión de Gobernación, con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicado en la Gaceta Parlamentaria número 2984-IV, jueves 8 de abril de 2010.

Dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública con Proyecto de Decreto que reforma el artículo 6º de la Constitución Política de los Estados Unidos Mexicano en Gaceta Parlamentaria, Cámara de Diputados, número 2207-II, martes 6 de marzo de 2007.

Dictamen de la Comisión de Puntos Constitucionales con Proyecto de Decreto por el que se adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos en Gaceta Parlamentaria, Cámara de Diputados, número 2653-II, jueves 11 de diciembre de 2008.

Iniciativa de Ley Federal de Transparencia y Acceso a la Información Pública, presentada por el Ejecutivo Federal. Gaceta Parlamentaria número 892, martes 4 de diciembre de 2001.

Iniciativa de Ley Federal de Transparencia y Acceso a la Información Pública, presentada por el Ejecutivo Federal. Gaceta Parlamentaria número 892, martes 4 de diciembre de 2001.

Iniciativa que reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Publicada en la Gaceta Parlamentaria número 2221-I, de fecha martes 27 de marzo de 2007 y publicada en el Diario Oficial de la Federación de fecha jueves 30 de abril de 2009.

Iniciativa de Ley de Protección de Datos Personales en Posesión de los Particulares presentada por el Dip. Gustavo Parra Noriega, Publicada en la Gaceta Parlamentaria, número 2607-III, martes 7 de octubre de 2008.

Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala. Artículo 42, fracción IV. Disponible al 15 de noviembre de 2011 en http://www.ifai.org.mx/Vinculacion/directorioL.

Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Artículo 58 fracción V. Disponible al 15 de noviembre de 2011 en http://www.ifai.org.mx/Vinculacion/directorioL.

Ley de Transparencia y Acceso a la Información del Estado de Quintana Roo. Artículo 31. Disponible al 15 de noviembre de 2011 en http://www.ifai.org.mx/Vinculacion/directorioL.

López Ayllón, Sergio (2009) *El acceso a la información como un derecho fundamental: La reforma al artículo 6º de la Constitución mexicana.* Instituto Federal de Acceso a la Información Pública, IFAI. México.

La protección de los datos personales

Eugenio Monterrey Chepov

Gregorio Castillo Porras

Eugenio Monterrey Chepov

Cursó su licenciatura en economía en el Centro de Investigación y Docencia Económicas, CIDE y Universidad del Valle de México, UVM. De octubre de 2010 a la fecha es Comisionado Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios (INFOEM), y ha sido Comisionado del mismo instituto desde agosto de 2008. Su experiencia laboral inicia en enero del 2000 como Asesor del Lic. Porfirio Muñóz Ledo, Candidato a la Presidencia de la República; de agosto a noviembre de ese año se desempeñó en la Comisión de Estudios para la Reforma del Estado; en 2001 fue investigador en el Fondo de Historia y Análisis Político, A.C.; en 2002 fue Secretario Técnico de Instituto Nacional de Estudios Históricos de la Revolución Mexicana de la Secretaría de Gobernación; de junio a agosto de 2002 formó parte como Asesor de la Unidad para la Promoción y Defensa de los Derechos Humanos de la Secretaría de Gobernación, posteriormente fungió como asesor del Subsecretario de Desarrollo Político de la Secretaría de Gobernación. En octubre de 2003 a octubre de 2005 es nombrado Coordinador de la Unidad de Enlace para la Transparencia y Acceso a la Información Pública de la Secretaría de Gobernación; de noviembre de 2005 a octubre de 2006 es Coordinador de la Unidad de Enlace para la Transparencia y Acceso a la Información Pública del Instituto Federal Electoral; de octubre de 2006 a octubre de 2008 se incorpora como asesor del Secretario de Finanzas del Gobierno del Estado de México y Coordinador de Transparencia de la Secretaría de Finanzas; de junio a julio de 2008 es Titular de la Unidad de Información, Planeación, Programación y Evaluación, así como Coordinador de Transparencia de la Secretaría de Finanzas.

Gregorio Castillo Porras

Secretario Particular del Comisionado Presidente del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Cursó la carrera de Abogado y Maestría en Derecho en la Escuela Libre de Derecho.

Introducción

La protección de los datos personales ejemplifica una de las formas más elocuentes de un derecho fundamental: el derecho a la privacidad y a la intimidad de las personas.

Poco se ha escrito en torno a este derecho fundamental consagrado en la Constitución General de la República. Lo anterior, sin demérito de la muy importante reforma constitucional en materia de derechos humanos publicada en junio de 2011. Con ella se establece un sistema de derechos humanos, en tanto que la incorporación del derecho a la intimidad y a la privacidad se ajusta a una prerrogativa, que data desde julio de 2007, con sendas ratificaciones en abril y junio de 2009.

Aunque paradójica, la aparición de este derecho fundamental va de la mano con la existencia de otro que presenta características diametralmente opuestas, sin el cual tal vez el éxito de dicha inserción constitucional no hubiera sido posible. Nos referimos al derecho de acceso a la información pública.

Esto se debe, en parte, al desconocimiento que existe sobre la materia de los datos personales y la circunstancia pragmática consistente en que resultaba mucho más sencillo aprobar una ley –la de transparencia, en este caso– que involucrara los dos derechos fundamentales.

El presente artículo pretende dar una explicación general sobre los orígenes y el concepto acerca de la protección de los datos personales, sin más finalidad que fijar parámetros teóricos que expliquen su naturaleza, utilizando referentes normativos del Estado de México. También se pretende deslindar a la protección de los datos personales respecto del acceso a la información pública, como ha acontecido en el ámbito federal y pudiese acontecer en las esferas locales de los Estados. Para lo cual se realizará una revisión de conceptos relevantes en la materia y se analizarán los temas clave a incluir en una ley especial que regule la protección de los datos personales.

El derecho fundamental a la privacidad e intimidad

Hablar de la protección de datos personales no sólo se refiere a un aspecto meramente de respeto, tanto de particulares como de instituciones públicas hacia los titulares de esos datos. Estamos frente a una expresión concreta del derecho fundamental a la privacidad e intimidad, término señalado por el jurista mexicano Carbonel (2009), que acuña el conjunto de prerrogativas y libertades de los individuos frente al ejercicio arbitrario o autoritario del Estado y sus agentes.

Por nuestra parte agregaríamos que sin esos derechos fundamentales, no se explica la construcción del Estado contemporáneo más allá de los elementos orgánicos o estructurales, sino que además exige un apartado dogmático, que los anglosajones llaman *Bill of Rights*.

En consecuencia, es claro que obviemos en el discurso y en la dogmática jurídica términos como el de garantías individuales, por mucho superado en el tiempo y en la doctrina. O, si se prefiere, darle la justa dimensión significativa a la voz *"garantía individual o constitucional",* frente a la de *"derechos fundamentales"*. En vista de ello, el ámbito de intimidad o la esfera de privacidad de los particulares es, sin duda, el espacio más cercano a la individualidad o, en un sentido más ontológico, a la esencia de una sustancia indivisa, única y propia.

Luego entonces ¿cómo no haber regulado o fijado en dispositivos jurídicos tan importante derecho como el de la privacidad e intimidad? Sin duda hay muchos y diversos argumentos, esencialmente de naturaleza histórica, que justifican esta ausencia en el ámbito de la normativa constitucional.

No es sino hasta la reforma al artículo 6º de la Constitución General de la República, publicada en el *Diario Oficial de la Federación* del 20 de julio de 2007, que se incluye por vez primera el derecho a la privacidad y a la intimidad.

Es cierto que el tema de los datos personales, y la protección que merecen, ya estaba legalmente contemplada en el ámbito federal desde 2002, a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, pero con dos limitantes:

- El tema de datos personales no estaba contemplado en la Constitución, a diferencia del acceso a la información que, aunque con deficiencias y una ineficacia real, estaba previsto en su artículo 6º desde 1977.

- Se trataba de un aspecto adicional encaramado en el tema políticamente más llamativo como el de transparencia.

En otro orden de ideas, también se discute la distinción o, por el contrario, la sinonimia entre privacidad e intimidad. Al respecto, estimamos que la diferencia existe, aunque es meramente gradual, y con mucha mayor *expertise* lo explica el profesor argentino Ernesto Garzón Valdéz:

> Conviene, pues, tener en cuenta que en el ámbito de la intimidad, según la interpretación aquí propuesta, es donde el individuo ejerce plenamente su autonomía personal; es el reducto último de la personalidad, es allí "donde soy lo que soy". En él, el individuo es soberano, como diría John Stuart Mill, en él decide las formas de su comportamiento social, privado o público, que es el que constituye el objeto propiamente dicho de la moral. (...)
> La privacidad es el ámbito donde pueden imperar exclusivamente los deseos y preferencias individuales. Es condición necesaria del ejercicio de la libertad individual. Parafraseando a Amartya Sen, podría decirse que la privacidad es la "esfera personal reconocida" que tendría que aceptar también todo liberal como punto de partida para la adopción de decisiones sociales que respondan a los ideales del liberalismo" (Garzón, 2003).

Esta cita nos permite llevar a cabo algunas conclusiones:

- La intimidad y la privacidad son conceptos con diferencias de grado, pero ambos conforman un derecho fundamental de respeto, no sólo frente al Estado, sino también frente a cualquier agente, particular o público.

- Frente a esta esfera de intimidad y de privacidad se ubica una diametralmente opuesta, no por ello ilícita: la de lo público.

> En dichas esferas aplican axiomas diferentes: mientras que la transparencia es la divisa de lo público, la confidencialidad lo es de la privacidad e intimidad. La distinción que Garzón Valdés (2003) refiere permite rescatar en la legislación mexicana una distinción entre datos personales *in genere* y datos sensibles, que permiten ubicar esas dos esferas: en el primer caso la privacidad y en el segundo la intimidad.

Con lo anterior, cerraríamos este análisis introductorio con una cita más que *ad hoc* de la autoría de Norberto Bobbio (1989):

> Si bien lo público/lo privado no resuelve el problema, hay una máxima: hay una zona en la que la publicidad deja de ser una virtud: esa zona es el espacio de la privacidad y de la intimidad individual. En este caso opera la máxima contraria: únicamente las sociedades permiten mantener a salvo de las miradas indiscretas a la esfera privada de todas y cada una de las personas que la integran, puedan edificar instituciones democráticas. (Bobbio, 1989).

El derecho a la protección de datos personales

Antecedentes en México

La protección de los datos personales tiene un origen legislativo dispar, sin que se haya definido su naturaleza de derecho fundamental hasta 2007. No obstante existen referencias normativas que parcialmente recogen ideas o aspectos de los datos personales, de la intimidad, de la privacidad, etcétera.

En un primer caso, lo más cercano a los datos personales es la regulación codificadora del Derecho Civil. De modo más concreto, en lo concerniente a los derechos de la personalidad significamos que las personas físicas –que no los individuos– tienen una esfera de derechos y obligaciones en el ámbito del Derecho Privado, y del Derecho Civil por excelencia. Tienen un nombre, un domicilio, edad legal (capacidad jurídica), un patrimonio, un estado civil y relaciones familiares, y con estos elementos se conforma la esfera civil que pudiera conformar hace muchos años lo más cercano a una especie de esfera de lo privado e íntimo.

Los derechos de la personalidad corresponden a todas y cada una de las personas físicas[1] y por lo mismo no son compartidos: identifican e individualizan a los titulares de esos derechos.

En otro ámbito del Derecho, la legislación penal pretendió proteger desde esta perspectiva valores jurídicos como la imagen personal, la reputación, la fama y el honor, mediante el establecimiento de delitos o tipos penales como la injuria, la difamación y la calumnia.

El Derecho Penal resulta insuficiente por dos razones: al igual que el Derecho Civil, la defensa de estos valores o bienes tutelados es tan sólo un segmento –por demás, subjetivo de valoración jurídica–, porque muchos de esos tipos penales han desaparecido bajo argumentos de derechos fundamentales como la libertad de expresión, entre otros.

Otro posible antecedente sobre la materia es poco conocido, aunque de bastante interés: la Ley Federal del Derecho de Autor, que desde 1996 consagró en su artículo 87[2] el derecho a la imagen física dentro de cierto tipo de obra autoral, como la fotográfica o audiovisual.

De alguna manera se pretendió proteger un dato personal como la imagen física. Sin embargo, es insuficiente tal regulación que, por otro lado, no es comprensible salvo por el tema de la obra fotográfica o audiovisual, que pudiera estimarse un dato personal como objeto de protección de la propiedad intelectual.

Puede sustentarse que el primer acercamiento a la intimidad y privacidad como derecho se dio a nivel federal con la Ley de Transparencia de 2002.

Como bien es sabido, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental regula en ese ámbito espacial de validez lo relativo al acceso y a la protección de los datos personales, con dos restricciones: la primera, consistente sólo en aquellos

[1] Se obvia comentar el caso de las personas morales o jurídico-colectivas.

[2] "Artículo 87. El retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso, o bien con el de sus representantes o los titulares de los derechos correspondientes. La autorización de usar o publicar el retrato podrá revocarse por quien la otorgó quién, en su caso, responderá por los daños y perjuicios que pudiera ocasionar dicha revocación…".

casos en los que la posesión de los datos personales recaiga única y exclusivamente en los llamados Sujetos Obligados por la Ley de Transparencia, esto es, sólo por instituciones públicas.[3]

La segunda comprende la medición de las leyes en términos de porcentajes, donde la Ley de Transparencia cuenta con un 80 a 85% de contenido normativo dedicado a transparencia, rendición de cuentas y acceso a la información pública, en tanto que el 15 y 20% restante se avoca a los datos personales.[4]

Finalmente, con las reformas constitucionales de 2007 y 2009 se consagró el derecho a la intimidad y a la privacidad. La reforma al artículo 6º constitucional, de julio de 2007, se dedicó a fijar los basamentos constitucionales del ejercicio del derecho de acceso a la información en todo el país, sin importar que se tratase de una instancia federal, estatal o municipal.

Aunque la fracción II del citado precepto fundamental colocó la primera piedra sobre la privacidad e intimidad al regular que "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes".

En ese mismo orden de ideas, la primera consagración constitucional del derecho a la privacidad e intimidad se realizó por vía de los datos personales. De manera afortunada, el Constituyente impactó de nueva cuenta en el texto fundamental con dos reformas en 2009, que definen de una vez y por todas al derecho a la privacidad y a la intimidad.

[3] Y ello tiene una explicación: frente a los innumerables trámites que los particulares realizan ante las diversas instancias de gobierno, existe una transmisión necesaria de datos personales.

[4] Y en realidad, este porcentaje minoritario se ve a la vez limitado precisamente por lo siguiente:
De nueva cuenta, esa regulación sobre datos personales sólo incide en el terreno de las instituciones públicas.
En materia de porcentajes, el que le corresponde a los datos personales tampoco es mucho porque la mayor parte de esa regulación mínima está dedicada al procedimiento de acceso a esos datos.
Y si bien nos va, encontraremos tan sólo algún precepto aislado sobre la protección de los datos personales.
Pero todo lo relativo a los principios que regulan esos datos como el de finalidad, consentimiento, entre otros, o bien, el tratamiento de las bases de datos, las medidas de seguridad, las traslaciones de las mismas, etcétera, etcétera, francamente se encuentran ausentes en esa normatividad.

La primera de esas reformas incidió en una nueva fracción al artículo 73 de la Carta Magna, al atribuir al Congreso de la Unión la facultad de legislar en materia de protección de datos personales en posesión de particulares.[5] Por otro lado, la segunda de las modificaciones a la Ley Fundamental fue incoada con la adición de un párrafo en el artículo 16 constitucional.[6]

Esto es, resulta verdaderamente importante el reconocimiento constitucional de los llamados derechos ARCO en materia de datos personales: acceso, rectificación, cancelación y oposición.

Antecedentes en América Latina

En el ámbito regional de América Latina, el tema del derecho a la privacidad y a la intimidad no es tan contundente como ocurre en Europa, tanto a título nacional como comunitario. El antecedente más inmediato sobre la protección de datos personales es la inclusión de una garantía jurisdiccional del derecho fundamental de acceso y rectificación de datos personales: el *Habeas Data*.

Las primeras referencias constitucionales de este mecanismo de protección se encuentran en la Ley Fundamental del Brasil, aunque hoy día esta institución jurídica ha encontrado importante eco en distintas legislaciones de América del Sur: Argentina, Colombia, Ecuador, Guatemala, Paraguay, Perú y Venezuela.

[5] Esto quiere decir que la enorme laguna de la protección de los datos personales en la esfera de lo privado quedó colmada, y volvió facultad exclusivamente federal este apartado de los datos personales. Y dejó a los Estados la regulación de los datos personales en posesión de las instituciones públicas locales y municipales. Lo anterior, debido al artículo tercero transitorio de la citada reforma que indicaba lo siguiente: "Tercero.- En tanto el Congreso de la Unión expide la ley respectiva a la facultad que se otorga en este Decreto, continuarán vigentes las disposiciones que sobre la materia hayan dictado las legislaturas de las entidades federativas, en tratándose de datos personales en posesión de particulares".

[6] El párrafo adicionado al artículo 16 estableció lo siguiente "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 públicas o para proteger los derechos de terceros".

Más allá de una concepción teórica y humanista, la inserción del *Habeas Data* respondió a una necesidad política y un contexto histórico latinoamericano: frente a los abusos de los regímenes dictatoriales en el uso y manejo de los datos personales de los civiles.

Adicionalmente, hay dos elementos que refuerzan el aspecto garantista de protección de este derecho fundamental, uno es el carácter de definitividad e inatacabilidad de las decisiones de los órganos garantes que recaen a los recursos de revisión, por lo que las instituciones públicas se ven impedidas de impugnar tales determinaciones.[7] El otro aspecto fortificante es la garantía de acceso a la justicia que los particulares tienen, en específico el Juicio de Amparo.

Por lo tanto, con todo y las peculiaridades del caso, puede afirmarse que en México se cuenta con una versión *sui generis* del *Habeas Data*.

[7] Aunque debe dejarse en claro que existen tendencias regresionistas que pretenden vulnerar el régimen de transparencia, como es el caso de la legislación del Estado de Campeche o la intentona de reforma a la Ley Federal de Transparencia de los entonces Senadores Fauzi Hamdan y Jorge Zermeño, entre otros casos, que han pretendido que los Tribunales de lo Contencioso-Administrativo o alguna instancia jurisdiccional revise las decisiones de los órganos garantes de transparencia. Lo cual, adicionalmente, demuestra la ignorancia que se padece sobre la naturaleza jurídica de los derechos de acceso a la información y a la vida privada e intimidad como prerrogativas fundamentales de última generación que no admiten formalismos ni rigideces propios del litigio jurisdiccional, sino que buscan mecanismos de protección procesal sencillos, rápidos y ágiles basados en los principios de oportunidad y eficacia en la entrega de la información pública o del acceso a los datos personales propios.

Antecedentes internacionales

En otro orden de ideas, la literatura en torno al derecho a la autodeterminación informativa, como suele denominarse en algunos países europeos, y que en el presente artículo hemos abordado como derecho fundamental a la privacidad e intimidad o protección de datos personales, adquirió el rango de prerrogativa fundamental en la construcción jurisprudencial o pretoriana del Tribunal Constitucional Federal alemán, en la conocida sentencia sobre la Ley del Censo. Dicha ley exigía tal cantidad de datos personales a los censados que vulneraba los derechos al libre desarrollo de la personalidad, la dignidad humana y la libertad de expresión. Los argumentos esenciales del Tribunal Constitucional Federal alemán para declarar la invalidez constitucional de dicha Ley fueron los siguientes:

- El valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre.

- Cobra significación especial la evolución moderna y de las nuevas amenazas que lleva aparejadas para la personalidad.

- La autodeterminación del individuo presupone conceder al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir.

De lo anterior, inferimos que la máxima instancia de justicia constitucional alemana creó, mediante jurisprudencia, el reconocimiento de la libre autodeterminación informativa de los individuos frente a posibles ataques o excesos de la autoridad en conocer parte de esa esfera de privacidad e intimidad, con dos consecuencias fundamentales: por un lado, la libre autodeterminación informativa se funda a la vez, en dos basamentos filosóficos de la naturaleza humana: el desarrollo de la personalidad y la dignidad humana, ambos considerados derechos fundamentales.

Por el otro, la protección de la libre autodeterminación informativa anticipa la protección de otros derechos fundamentales, pues conocer en exceso aspectos de la vida de los particulares pondría en riesgo, v.gr., la libertad de expresión y de reunión política, que al verse en

riesgo por haber dado a conocer la preferencia o ideología política o partidista, se vulnera un conjunto mayor de derechos fundamentales.

Por otro lado, aunque en Europa existe una normatividad extensa (Directivas) en el ámbito de la Unión Europea, ha sido esencialmente la jurisprudencia de los Tribunales Constitucionales tanto comunitarios como nacionales los que han formado la casuística pretoriana de la protección de los datos personales.

Datos personales y derechos ARCO

Una vez hecho el anterior recorrido sobre los antecedentes del derecho a la protección de los datos personales, es importante señalar las definiciones de los principales conceptos en esta materia. El primer punto a abordar corresponde a los datos personales, mismos que pueden definirse como se ha hecho en todas las legislaciones sobre la materia en México y en Europa: los datos personales es toda la información relativa a las personas físicas que permite identificarlas o hacerlas identificables. La definición es, sin duda, amplia pero es lo más cercano conceptualmente en razón de lo siguiente:

- La información derivada de los datos personales es generada a partir de las propias características de los particulares, provenientes de las esferas de intimidad y de privacidad.

- La definición es clara: sólo las personas físicas o, mejor dicho, los individuos, tienen datos personales y pueden ser titulares de los mismos. Por exclusión, las personas morales o jurídico-colectivas carecen de ellos.

- Y probablemente lo más relevante es que ese cúmulo de información sobre personas físicas tiene como finalidad identificarlas o hacerlas identificables. En un primer caso, la identificación es indudable: esa y ninguna otra persona más es la titular de los datos. En cambio, la identificabilidad sólo supone generar un universo acotado de ciertas personas que bien pudieran ser las titulares de los datos en cuestión.

Así, por ejemplo, las directivas de la Unión Europea en la materia son explícitas en torno a este elemento de la definición de los datos personales:

Directiva 95/46/CE. "Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Otro aspecto importante en la definición de los datos personales es la enumeración casuística y ejemplificativa de los mismos. En ese sentido, como lo hace también la mayoría de las legislaciones, los datos personales pueden ser: información numérica, alfabética, gráfica, fotográfica y acústica, entre muchos otros supuestos.[8]

Asimismo, estos datos personales admiten una regla general con dos excepciones que la confirman:

- Por regla general, todo dato personal es información confidencial.

- Excepcionalmente, hay datos personales que sin dejar de serlos no ameritan la protección de la confidencialidad, cuando por la disociación de datos o lo aislado de los mismos evitan la identificación o identificabilidad de la persona. Por ejemplo, el nombre de las personas es un dato personal por excelencia, pero en sí mismo considerado y no vinculado a otros datos personales, en principio no le asiste la confidencialidad.

- Del mismo modo, como excepción algunos datos personales dejan no sólo de gozar de confidencialidad, sino que se convierten en información pública incluso hasta de oficio. Y el ejemplo más claro de ello es el tema de datos de identificación y patrimonio de servidores públicos.

[8] Los datos personales deben ser considerados casuísticos pues, por ejemplo, en algunos casos de órganos garantes estatales en México se ha resuelto, por ejemplo, como datos personales el perfil alimenticio. Esto es, si derivado de una factura de pago por concepto de alimentos se determina la clase de éstos, pudiera inferirse un estado de salud (comida para diabéticos), gustos alimenticios (comida gourmet o chatarra), régimen (comida dietética), entre otros.

Los derechos Acceso, Rectificación, Cancelación y Oposición (conocidos como derechos ARCO por el acrónimo) constituyen el núcleo fundamental del derecho a la protección de los datos personales. La primera referencia a estos derechos se encuentra en un proyecto de Ley Modelo de Transparencia que el entonces Instituto Federal de Acceso a la Información Pública elaboró en 2008 y que los contempló de la siguiente manera:

> CAPÍTULO II. Derechos de acceso, rectificación, cancelación y oposición
>
> Derechos ARCO
> Artículo 72. Los derechos de acceso, rectificación, cancelación y oposición de datos personales son derechos independientes. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el interesado o su representante legal acrediten su identidad o representación, respectivamente.

Los derechos ARCO, pueden ser ejercitados por:

a) El titular de los datos personales, debidamente identificado.

b) El representante legal del titular, debidamente acreditada la representación.

Por tanto, cuando el ejercicio de cualquiera de los cuatro derechos mencionados pretenda ser llevado a cabo por un tercero distinto al titular, o que carezca de la representación legal suficiente, le será negado el derecho en cuestión.

Además, el ejercicio de estos derechos se rige por un principio de independencia entre cada uno de ellos, es decir, que el acceso, la rectificación, la cancelación y la oposición son prerrogativas independientes cuyo ejercicio no se condiciona a los otros como requisito previo o condición *sine qua non*.

El resultado del ejercicio de cualquiera de estos derechos esencialmente tiene dos posibilidades: el cumplimiento a cualquiera

de los cuatro derechos, asimismo, existe el supuesto por el cual, aunque los datos personales existan, no existen condiciones jurídicas para cumplimentar esos derechos, pues la autoridad tiene título legal suficiente para el manejo de esos datos personales.

En todo caso un acto denegatorio es un acto de autoridad que debe estar debidamente fundado y motivado, por respeto a los artículos 14 y 16 constitucionales, que establecen garantías de seguridad jurídica a favor de los particulares que se vean afectados en sus derechos fundamentales.

Conviene ahora explicar cada uno de estos cuatro derechos.El derecho de acceso a datos personales corresponde a todo individuo *per se* o por medio de representante legal, para solicitar y obtener gratuitamente información sobre sus datos de índole personal sometidos a tratamiento, el origen de dichos datos, así como las transmisiones o comunicaciones realizadas o que se prevén hacer de los mismos.

El derecho de acceso a datos personales supone la posibilidad del titular o representante legal de conocer dichos datos desde una mera consulta *in situ* o simple visualización y hasta el otorgamiento de copias certificadas.

Dicha información comprenderá todos los datos personales con los que se cuente del titular, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre su origen, los cesionarios de los datos y la especificación de los usos concretos y finalidades para los que se almacenaron.

El derecho de rectificación es la prerrogativa de todo individuo como titular o por medio de representante legal para que se modifiquen los datos personales que resulten inexactos o incompletos, por lo que impone un deber a las instituciones públicas y privadas que cuenten con bases de datos personales de mantener los principios de revisión constante y actualización de dichas bases de datos para evitar la exigencia de la rectificación.

El derecho de cancelación es la prerrogativa de todo individuo como titular o a través de representante legal para que se supriman los datos

personales que resulten ser inadecuados o excesivos, lo cual permitirá el bloqueo de los datos, con la posibilidad de conservarse solamente para efectos de responsabilidades en un negligente o inadecuado uso y manejo de bases de datos personales.

Deberá considerarse, además, que la cancelación no podrá realizarse si existe disposición legal que establezca un plazo obligatorio de conservación de los datos.

El derecho de oposición es la prerrogativa a todo individuo, como titular o por medio de representante legal, para que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo, siempre y cuando medie causa justificada. Al parecer, este derecho de oposición refleja de manera contundente el principio de consentimiento en el uso y manejo de datos personales.

Sin embargo, deberá considerarse que habrá casos excepcionales en los que el consentimiento es innecesario para el manejo de los datos personales. Por ejemplo, estos casos excepcionales están incluidos en el artículo 52 de la Ley de Transparencia del Estado de México.

Para ejemplificar de modo accesible un caso de ejercicio del derecho de oposición puede señalarse el derecho de todo individuo a oponerse por los efectos jurídicos que pueden tener a la publicación de sus nombres en litigios laborales o fiscales que les puedan perjudicar como empleados "riesgosos" o deudores morosos.

Principios rectores de la protección de los datos personales

Salvo –nuevamente– los casos federal y del Distrito Federal, pocas legislaciones recogen los principios que pueden considerarse como universales en torno al uso, manejo y tratamiento de datos personales. Sin duda, algunos de esos principios son recogidos en forma dispersa en las legislaciones locales.

Los principios rectores de los datos personales no sólo son normas jurídicas que se imponen como obligaciones para quienes estén en posesión de esos datos (instituciones públicas o particulares),

sino también son tales: es decir, principios en el sentido que la argumentación jurídica les ha dado a partir de las doctrinas de Alexy (2006) o de Ronald Dworkin.[9]

Esto es, diría Alexy (2006), los problemas de una jerarquía de los valores jurídicamente relevantes se han discutido con frecuencia. Se ha mostrado que no es posible un orden que conduzca en cada caso a un resultado –a tal orden habría que llamarlo orden estricto–. Un *orden estricto* solamente sería posible si el peso de los valores o de los principios y sus intensidades de realización fueran expresables en una escala numérica, de manera calculable. El programa de semejante orden cardinal fracasaría ante los problemas de una medición del peso y de la intensidad de realización de los principios jurídicos o de los valores jurídicos. En ese sentido, creemos que los principios rectores de los datos personales representan un orden estricto de valoración frente a cualquier duda en el uso y manejo de los datos.

Aunque sin duda, cuando haya conflicto entre los propios principios rectores habrá que aplicar las reglas de ponderación que señala Alexy en su obra.

Por otra parte, Dworkin señala que los principios hacen referencia *a la justicia y la equidad*. Mientras las normas se aplican o no, los principios dan razones para decidir en un sentido determinado, pero, a diferencia de las normas, su enunciado no determina condiciones de aplicación. El contenido material del principio –su peso específico– determina cuándo se debe aplicar en una situación determinada.

Los principios –además– informan las normas jurídicas concretas de tal forma que la literalidad de la norma puede ser desatendida por el juez cuando viola un principio que en ese caso específico se considera importante.

En consecuencia, los principios rectores de los datos personales tienen que llevar un orden estricto en la valoración de quienes recojan, usan, manejan, tratan, transmiten o ceden datos personales y, ante una disparidad con la norma jurídica, informan de un contenido de

[9] DWORKIN, Ronald. Los derechos en serio, Prólogo de Alberto Calsamiglia, Colección Biblioteca Fundamental.

mayor envergadura que deberá de observarse aún en contra de la misma simplicidad de la norma técnica de Derecho.

Estos principios, además de los derechos ARCO, en caso que no se observen, generan violentaciones al derecho fundamental de los particulares a una vida privada y un espacio de intimidad, y pueden ser sancionables esas conductas atentatorias a tales esferas de desarrollo de la personalidad de los individuos.

Los principios rectores que pueden estimarse en materia de datos personales, más allá de las distintas nomenclaturas que la doctrina o las legislaciones les puedan dar, son los siguientes:

a) Principio de calidad de los datos personales.

b) Principio de consentimiento e información.

c) Principio de protección especial de datos sensibles.

d) Principio de seguridad de los datos personales.

e) Principio de confidencialidad estricta.

f) Principio de comunicación de datos personales.

A continuación explicaremos brevemente cada uno de estos principios con algunas ejemplificaciones prácticas y referencias normativas.

a) *El principio de calidad* de los datos personales atañe, en términos de argumentación jurídica, a una idea de racionalidad y proporcionalidad en el uso y manejo de esos datos. Dicho en otro sentido, en evitar un uso o manejo excesivo de los datos, principalmente en la recolección u obtención de los mismos. Es una medida prudencial y de pertinencia de quien recoge los datos y el uso que les va a dar, con base en las finalidades que motivaron su uso o recolección.

Por ende, este principio deberá resguardarse mediante las siguientes medidas meramente enunciativas:

- Los objetivos y finalidades que se pretenden alcanzar con la recolección y/o uso de los datos deben ser explícitos e indubitables, esto es, ¿para qué se requieren esos datos personales?

- Los titulares de los datos pueden cuestionar en todo momento si el recolector o responsable de la base de datos se conducen con pertinencia y prudencia ante un posible exceso o abuso que violenten la proporcionalidad y racionalidad de los datos personales.

- Debe existir compatibilidad entre los datos requeridos y la finalidad de la recolección o uso.

- En el caso de instituciones públicas, se deberá constatar que tienen las atribuciones legales para requerir los datos, de lo contrario existirá una actuación extralimitada. Por ejemplo, será incomprensible que una instancia de desarrollo social pretenda pedir a un órgano electoral el padrón de electores, para dar cumplimiento a sus finalidades de política social.

- Asimismo, la recolección de los datos personales debe responder a parámetros de exactitud y veracidad, pues el titular tiene en todo tiempo el derecho de rectificación de datos. Lo cual, como se ha visto en párrafos anteriores, se traduce en una obligación de los poseedores de los datos de una permanente revisión y actualización de éstos.

- De igual modo, ante una posesión excesiva o innecesaria de datos, el titular puede ejercer el derecho de cancelación.

Una de las principales preocupaciones que ha generado la existencia del principio de calidad de los datos personales, es el mal uso que las corporaciones tanto públicas como privadas puedan dar a los datos personales que el titular les proporcionó. Por ejemplo, en el ámbito de lo público los padrones de beneficiarios de programas sociales se basan en datos personales, lo cual no significa que le dé derecho a las instituciones de política social de hacer propaganda electoral o proselitismo en aras de los beneficios obtenidos. O bien, en lo privado, la obtención de datos personales necesarios para el otorgamiento de

un crédito bancario, no le otorga derecho a la institución financiera de utilizarlos para el envío de correos electrónicos con propaganda de otros servicios financieros. En ese sentido, la Ley de Transparencia del Estado de México señala, como ejemplo normativo del principio de calidad de los datos personales el siguiente:

> Artículo 52. (...)
> En ningún caso los datos personales podrán ser utilizados para fines electorales o de proselitismo por partido político alguno, y sólo se emplearán para los fines previstos en esta Ley o en la especial en la materia.

b) *El principio de consentimiento e información* consiste en que cualquier recolección, uso, manejo y transmisión de datos personales debe hacerse del conocimiento del titular, y éste deberá manifestar de modo indubitable y expreso la voluntad o el asentimiento de proporcionarlos. Por lo tanto, se torna en obligación para quienes recogen los datos requerir el consentimiento a los titulares, e informarles el uso y finalidad de la recolección. Por lo general, se utilizan leyendas o formatos en que aparece una advertencia para los titulares del uso que se dará a sus datos, así como un espacio en que mediante firma o selección de una afirmativa expresen el consentimiento. En todo momento, el titular podrá ejercer los derechos ARCO, según sea el caso, para constatar que no se defraudó el principio de información y, hasta es posible estimar que con el ejercicio del derecho de acceso pudiera ratificarse el consentimiento del titular de los datos. De igual modo, es importante informarle a los titulares en qué base de datos personales obran sus propios datos. En el caso del Estado de México se ha establecido una leyenda para cumplir con el principio de información, misma que aparece en los Lineamientos para el Manejo, Mantenimiento, y Seguridad de los Datos Personales que se Encuentran en Posesión del Poder Ejecutivo del Estado de México, las Dependencias y Organismos Auxiliares, los Fideicomisos Públicos y la Procuraduría General de Justicia, como Sujetos Obligados de la Ley de Transparencia y Acceso a la Información Pública del Estado de México, misma que cumple los requisitos de ley respecto del deber de informar a los titulares de los datos acerca del tratamiento y destino de que serán objeto.

Asimismo, hemos visto en párrafos anteriores que la ley de Transparencia del Estado de México,[10] al igual que la mayoría de las leyes estatales, contiene implícito el principio de consentimiento, al establecer excepciones al mismo. Esto es, no se requiere el consentimiento del titular de los datos bajo ciertas circunstancias, que siempre serán excepcionales y estrictas, tales como:

- Por razones de atención médica urgente o sanidad pública.
- Por razones estadísticas, siempre que se disocien los datos y se impida con ello la identificación o identificabilidad de los titulares.
- Por mandamiento judicial.
- Por razones contractuales con terceros, siempre que se garantice la confidencialidad de los datos mediante penas convencionales, responsabilidades legales y garantías económicas como fianzas.
- Por razones de fuentes de acceso público, como registros civiles o de la propiedad y comercio.
- Por razones de la legalidad de las atribuciones de instituciones públicas.[11]
- Y en general, cuando una ley expresamente lo establezca, pero siempre deberá establecerse esa excepción en una ley formal y material y no en una norma jurídica de rango menor al de la ley en el sentido antes descrito.

[10] Artículo 52 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Dicho precepto tiene correlativo en el artículo 22 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[11] Existe un caso muy interesante en torno a datos biométricos como el iris ocular o la huella dactilar como registro de entrada y salida de empleados públicos en términos de horario laboral. En una sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo español que data de 2007 se estableció que: *"(…) cumplir con el control horario es una obligación inherente a la relación que une a los funcionarios con la Administración, no siendo necesario obtener previamente su consentimiento ya que el artículo 6.2 de la LOPD lo excluye en estos casos. Asimismo, no hay norma que prohíba el recurso a la tecnología escogida para realizar el control del cumplimiento del horario de trabajo. Su novedad o complejidad no la convierten en lesiva de los derechos fundamentales invocados".*

Finalmente, el principio de consentimiento es de interpretación estricta y casuística, esto es, la obtención del consentimiento sólo es para los efectos para los cuales fue informado el titular y sólo para ese caso. Por lo que si los efectos se amplían o se requiere un uso adicional se volverá a pedir el consentimiento del titular de los datos personales.

c) *El principio de protección especial de datos sensibles* se relaciona con aquellos que tengan que ver con lo que podríamos denominar intimidad física e ideológica, como lo es el estado de salud físico y/o mental, la vida y preferencia sexual, la etnicidad, así como las creencias religiosas y políticas. La naturaleza de sensibilidad de estos datos, además de lo dicho, se vincula necesariamente con otros derechos fundamentales como lo son el libre albedrío decisorio sobre el cuerpo, la libertad de expresión y la libertad religiosa. Por ende, todos los principios rectores de los datos personales se vuelven mucho más estrictos que de lo habitual correspondería. Así, por ejemplo, estimamos que no bastaría una simple leyenda de formato en la recolección de los datos como la que hemos transcrito líneas arriba, sino que debe existir una declaración escrita y expresa del consentimiento del titular. Esta protección especializada y rigurosa obedece sobre todo a la base de la dignidad humana y al principio de no discriminación y ante un pasado histórico más o menos reciente de violaciones de lesa humanidad en razón de pertenencias étnicas, religiosas o políticas durante el siglo XX. Una norma de la Ley de Transparencia del Estado de México parece recoger este sentido —aunque de modo desafortunado— en una franca confusión entre lo que es la información pública de oficio y la protección de datos sensibles, al tratarse de padrones de beneficiarios siempre que difundir dicha información no genere discriminación:

> Artículo 12. Los Sujetos Obligados deberán tener disponible en medio impreso o electrónico, de manera permanente y actualizada, de forma sencilla, precisa y entendible para los particulares, la información siguiente:
> (…)
> VIII. Padrones de beneficiarios de los programas desarrollados por el Estado y los municipios, así como información disponible sobre el diseño, montos, acceso y ejecución de los programas de subsidio, siempre y cuando la publicación de estos datos no produzca discriminación. Esta disposición sólo será aplicable en

> aquellos programas que por su naturaleza y características permitan la integración de los padrones de referencia; (…).[12]

Tal disposición genera polémica, pues bien podría argumentarse que todo programa de desarrollo social atiende grupos vulnerables, y que dar a conocer el nombre de los beneficiarios pudiera generar discriminación. Hay casos muy claros y contundentes, como por ejemplo, un padrón de beneficiaros de medicamentos para la atención del VIH. Pero el caso ya no es tan prístino cuando sólo se atiende revertir los efectos de la pobreza en comunidades menesterosas ¿ser pobre puede generar discriminación? En fin, la polémica está por resolverse.

Por otro lado, la citada Ley atiende el tema de los datos sensibles y la protección especial que exigen, además de ratificar el principio de calidad de los datos personales en la siguiente disposición:

> Artículo 26. Los sujetos obligados deben sistematizar la información que contenga datos personales en archivos seguros y confiables bajo su resguardo y responsabilidad. Solamente podrá obligarse a los sujetos obligados a proporcionar la información personal para proteger la seguridad pública o la vida de las personas; dicha información será la estrictamente necesaria y no contendrá datos que puedan originar discriminación, sobre su origen racial o étnico, preferencia sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, su participación el alguna asociación o a la afiliación a una agrupación gremial.
> En lo no previsto, los sujetos obligados estarán a lo dispuesto en la Ley especial.

d) *El principio de seguridad* de los datos personales atañe esencialmente al poseedor de la base de datos con un conjunto variopinto de medidas protectoras de aquéllos.

[12] El subrayado es nuestro.

Tales medidas van desde disposiciones, garantías y sanciones jurídicas, hasta de naturaleza técnica como respaldos, claves y contraseñas, uso de equipos de cómputo *ad hoc*, y reglas internas de designación de responsables y usuarios de las bases de datos, horarios de uso, entre muchas otras.

Las medidas de seguridad deberán ser acordes a diversos factores: la tecnología en que se encuentra la base de datos, el tipo de datos personales en posesión y los riesgos de exposición por agentes externos personales o físicos. El artículo 25 Bis de la Ley de Transparencia del Estado de México establece escuetamente algunas medidas de seguridad de protección de datos personales:

> Artículo 25 Bis. Los sujetos obligados son responsables de los datos personales y, en relación con estos, deben:
> I. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y evite su alteración, pérdida, transmisión y acceso no autorizado; y
> II. Capacitar a los servidores públicos en relación a la protección de los datos personales.

Vinculadas las bases de datos a finalidades tributarias o de servicios de salud pública y seguridad social. Y finalmente, el nivel alto que corresponde a datos sensibles de los cuales ya hemos hecho referencia.

Asimismo, es relevante destacar algunos conceptos en torno a este principio de seguridad de los datos personales. Elementos que podemos agrupar en objetivos, subjetivos y procesales, bajo el entendido de que los primeros tienen que ver con el elemento material sobre el cuales se ejercen y aplican las medidas de seguridad y protección, en tanto los segundos a los actores responsables del uso y manejo de esas bases de datos. Y los procesales a las medidas propiamente dichas, de las cuales amerita atención especial el proceso de disociación.

Así, el elemento objetivo del principio de seguridad es, precisamente la base de datos personales. Misma que puede comprenderse como el conjunto organizado y sistematizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso.

De acuerdo a la práctica administrativa de instituciones públicas y corporaciones privadas, las bases de datos pueden ser esencialmente de dos tipos: electrónicas o automatizadas y no automatizadas o físicas. Estos últimos recaen esencialmente en la documentación impresa en papel que conforman expedientes.

En lo relativo a los elementos subjetivos o personales destacan tres: *a)* el responsable de la base de datos, *b)* el responsable del tratamiento de la base de datos y *c)* los usuarios de la base de datos. El responsable de la base de datos puede entenderse como la persona física o jurídico-colectiva, tanto de Derecho Público como de Derecho Privado, que tiene a cargo la responsabilidad de la finalidad, contenido y uso de la base.

El responsable del tratamiento de la base de datos es, igualmente, la persona física o jurídico-colectiva, tanto de Derecho Privado como de Derecho Público, que da tratamiento a la base de datos personales por cuenta del responsable de la misma. Esto es, quien en los hechos y directamente se responsabiliza del manejo efectivo de las bases de datos y hay que reconocer que en lo específico recae en un servidor público o en un empleado privado. En algunos casos, el responsable de la base de datos puede contratar a un tercero para que le preste el servicio de responsable de tratamiento de la base de datos, por lo que no necesariamente puede recaer esta tarea en una unidad administrativa o área de trabajo interna del responsable de la base de datos.

Finalmente, el usuario de la base de datos será el personal (servidores públicos o empleados privados) dependiente de los responsables de las bases y que tendrán acceso a ellas derivado de las funciones que tienen a cargo. Por último, el elemento procesal que deseamos destacar es el procedimiento de disociación, que representa una medida de seguridad consistente en el uso y manejo de los datos, de manera que al descomponer los vínculos asociativos se impide la identificación o identificabilidad de los titulares de los datos. Con esta disociación lo que en realidad se logra es despersonalizar al dato o quitarle dicha naturaleza y por lo tanto no ha menester de medidas protectoras para esos datos disociados.Por ejemplo, como se ha comentado, en la estadística no se requiere el consentimiento de los datos personales, puesto que la disociación que se realiza impide la identificación del titular.

e) *El principio de confidencialidad estricta* se traduce en una restricción o inhibición a cualquier tercero distinto al titular, que impide conocer los datos personales de éste. Asimismo, la confidencialidad es una forma de clasificar la información; es prácticamente permanente, sólo superable cuando existe el consentimiento expreso del titular de publicitar sus datos personales; y tiene varias vertientes:

- Como clasificación de información que en el caso mexicano, tanto a nivel federal como en todas las entidades federativas, debe expresarse mediante un acuerdo o acta del Comité de Información (órgano colegiado de las instituciones públicas) que con la debida fundamentación y motivación por ser un acto de autoridad, se niega cualquiera de los derechos ARCO a un tercero que no es el titular de los datos personales en cuestión.

- Como listado de bases de datos, que, por ser confidenciales, sólo se da a conocer como información pública de oficio una mera enunciación de cuántas y cuáles bases de datos tiene en posesión, o ha generado una institución pública o una corporación privada.

- Como deber profesional de secrecía a cargo de los responsables de bases, responsables de tratamiento, usuarios de bases y, en general cualquier tercero que por razón indistinta tenga acceso o conocimiento de los contenidos de las bases.

- Como cláusula contractual, sobre todo en casos en que terceros prestan servicios a los responsables de las bases y que, por tanto, se comprometen a: *a)* mantener la confidencialidad de los datos contenidos en la base, *b)* asumir responsabilidad jurídica en caso de violentar esa confidencialidad, *c)* pagar penas convencionales y *d)* garantizar mediante fianza u oro mecanismo de respaldo jurídico-económico el deber de secrecía.

- Como registro y autorización de bases de datos ante la competencia de los órganos garantes de esa confidencialidad.

f) *El principio de comunicación o transmisión de datos personales*, consistente en la cesión de éstos a un tercero, pero es indispensable que tal transmisión tenga un fin lícito entre las partes de la transmisión,

y tenga que ver con las atribuciones y competencia del transmisor y del receptor.

Asimismo, resulta *sine qua non* el consentimiento previo de los titulares de los datos y el principio de información sobre las razones, necesidad y finalidades de esa transmisión de datos personales. De nueva cuenta, hemos visto ya el supuesto del artículo 52 de la Ley de Transparencia del Estado de México, que prevé casos excepcionales de transmisiones de datos personales sin la necesidad del consentimiento del titular. Ahora bien, entiéndase como transmisión de datos, tan sólo una de diversas acciones u operaciones que abarcan, además de dicha cesión, la recolección, almacenamiento, uso y manejo de datos personales.

A todo este conjunto de acciones y operaciones –que bien puede ser automatizadas/electrónicas o no automatizadas/físicas– se denomina tratamiento de datos personales. En los Lineamientos de Bases de Datos Personales del Estado de México que ya se refirieron en un apartado anterior de este artículo, se define a ese tratamiento de datos personales como:

> CUARTO. Para efectos de la aplicación de los presentes Lineamientos, se entenderá por:
> (…)
> VI. Manejo o Tratamiento. Operaciones y procedimientos de cualquier índole que permitan recabar, registrar, reproducir, conservar, organizar, modificar, corregir, sustituir, rectificar, suprimir, transmitir y eliminar datos personales de las bases de datos de los sujetos obligados;
> (…).

Aunque en nuestra opinión una mejor definición que pudiera enriquecer el concepto es la siguiente propuesta:

> Tratamiento de datos personales. A cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, aprovechamiento, cesión, difusión, transferencia,

interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al titular el acceso, rectificación, cancelación u oposición de sus datos.

Por una Ley de Protección de Datos Personales en Posesión de Instituciones Públicas

Como se explicó en el apartado de antecedentes, hemos visto cómo en las leyes de transparencia se incorporó el tema de datos personales en posesión de instituciones públicas, y que a partir de 2009 se federalizó en los casos de datos personales en posesión de particulares. Como se ha comentado, la necesidad de incorporar pocos elementos en materia de datos personales radicaba en mantener condiciones de éxito parlamentario, para la aprobación de las respectivas leyes de transparencia, y no generar una doble discusión frente a dos iniciativas temáticamente distintas. Más aún, cuando no había comprensión suficiente de los datos personales para iniciar la aventura legislativa de una norma *ad hoc*.

Si bien la incorporación de los datos personales a las leyes de transparencia insertó la semilla de un derecho novedoso en México, también permitió la germinación de un aspecto insoslayable que conforma la necesidad de contar con una ley específica en el rubro.

Esta primera semilla, insistimos, colocó al tema en el interés de académicos y autoridades. Por primera vez se reguló el derecho a la privacidad y a la intimidad, que pocas noticias se había tenido en la literatura jurídica y legislativa en México. Por ello, vale la pena cuestionar: ¿Por qué son diferentes los dos derechos que consagran las leyes de transparencia? Ante todo, porque en sí mismos se trata de dos derechos distintos, con sus propias dinámicas y naturaleza: por un lado, el derecho de acceso a la información pública y, por el otro, el derecho a la privacidad e intimidad.

El primero de esos derechos tiene una clara vocación de transparentar el ejercicio del poder público, de escrutar la gestión de los servidores públicos, de conocer documentalmente las razones que llevaron a la toma de decisiones del gobierno. Por eso es público, no sólo porque el gran sujeto obligado es el Estado, sino porque el contenido informativo

que se desea conocer es de difusión abierta y de disposición a cualquier individuo, prácticamente sin ninguna limitación.

En tanto, el segundo de esos derechos radica en el ámbito de la vida ajena al Estado y su injerencia: el mundo de lo privado, el de los particulares, ese valladar al cual ni siquiera, diría Jeremy Bentham, ni los ojos del mismo rey pueden penetrar la más modesta casa del más modesto de sus súbditos. Y ese fuero interno y ese espacio exclusivo de la vida de cada individuo, contrario a lo que sucede con el acceso a la información, debe contenerse, resguardarse y comprimirse en la confidencialidad casi absoluta.

Como se observa, entre el acceso a la información y los datos personales opera una relación de oposición, esto es, que entre ambos derechos les aplica inversamente los principios que les rigen:

- El acceso a la información tiene como prédica el principio de máxima publicidad. El derecho a la privacidad e intimidad tiene como eje transversal el principio de máxima protección.

- Las restricciones al acceso a la información pública bajo la forma de reserva son temporales. Las restricciones de acceso a la información privada e íntima son prácticamente perennes.

- El acceso a la información pública está permitido a cualquier individuo. El acceso a los datos personales exclusivamente al titular de éstos o su representante legal debidamente acreditado.

- El acceso a la información pública confronta al Estado. El derecho a la privacidad y a la intimidad no sólo frente al Estado, sino también frente a los particulares.

En fin, como se ha expresado, son dos derechos opuestamente diferentes, cuyo único punto de convergencia es el procedimiento de acceso a la información que contiene a la vez datos personales, y que es información en posesión o generada por una institución pública.

A la anterior conclusión, cabría entonces preguntar: ¿el procedimiento de acceso a datos personales debe separarse de la Ley de Transparencia? La respuesta es sí, porque a pesar de formar parte de un procedimiento

ante el Estado, la sustancia mantiene los contenidos propios e independientes de la materia de los datos personales y del derecho a la privacidad e intimidad, los que no pueden restringirse a los contenidos normativos de las leyes de transparencia. Es decir, se amerita de una regulación propia que responda a la naturaleza particular del derecho a la privacidad e intimidad.

Esto ha sido excepcionalmente considerado en las siguientes legislaciones, independientes de las leyes de transparencia y acceso a la información:

- La Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- La Ley de Protección de Datos Personales del Estado de Colima.
- La Ley de Protección de Datos Personales para el Distrito Federal.
- La Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato.
- El Capítulo III, del Libro Segundo del Código Civil del Estado de Jalisco, relativo a la Información Privada.
- La Ley de Protección de Datos Personales del Estado de Oaxaca.

Sin embargo, deben acotarse y dimensionar adecuadamente estas excepciones:

De las seis leyes, tres (Distrito Federal, Guanajuato y Oaxaca) cuentan con una Ley de Protección de Datos Personales, pero sólo en el ámbito de lo público. Esto es, separan de sus respectivas Leyes de Transparencia el acceso y protección a datos personales en posesión de instituciones públicas.

En esas entidades federativas no hay leyes de protección de datos personales en posesión de particulares. Y no hay necesidad de que se expidan, en virtud de la reforma constitucional de 2009 al artículo 73 de la Carta Magna, al Artículo Tercero Transitorio del Decreto de dicha reforma constitucional y a la expedición de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

De las seis excepciones, una (Jalisco) le da un tratamiento parcializado, al incorporar como parte de los atributos de la personalidad jurídica la información privada. Por lo que no debe estimarse como la mejor fórmula legislativa de regular la protección de datos personales. De esas seis excepciones, dos (la Federación y Colima) regulan separadamente la protección de datos personales respecto de las leyes de transparencia, comprendiendo tanto a instituciones públicas como a particulares, en su calidad de poseedores de datos personales. Aunque es Colima la entidad pionera en regular el tema en forma separada, lo hace mediante una ley escueta que no comprende todos los rubros que se estiman indispensables en la regulación de esta materia. Por otro lado, en atención al Artículo Tercero Transitorio de la reforma constitucional citada, la Ley colimense quedó abrogada ante la "federalización" de esa materia, y sólo quedó el recurso de legislarla, cuando los datos personales obren en posesión de las instituciones estatales y municipales de dicha entidad. En el caso de la Federación debe señalarse que si bien la regula y se apropió de la materia de protección de datos personales en posesión de los particulares, también lo es que mantiene esta materia cuando opera en las instituciones públicas dentro de la misma Ley Federal de Transparencia.

Por lo que se ve, hay tres niveles en la regulación de los datos personales en México: dos responden a una autonomía legislativa sobre el tema, aunque uno ya no es posible en el nivel estatal por ser materia exclusivamente federal:

- El primer nivel regula el acceso y la protección de los datos personales en la misma ley que comprende el régimen de transparencia y el acceso a la información pública. En datos personales sólo en lo que respecta a la posesión de los mismos por parte de las instituciones públicas.

- El segundo nivel es el que corresponde a la separación del acceso y protección de los datos personales en una ley propia, pero sólo en lo relativo a instituciones públicas poseedoras de información confidencial, como es el caso del Distrito Federal, Guanajuato y Oaxaca. El caso de Jalisco por sus propias consideraciones queda fuera de esta categoría.

- El tercer nivel consiste en dos leyes: una de transparencia y acceso a la información pública generada o en posesión de las instituciones estatales, y otra ley de acceso y protección de datos personales en posesión de esas mismas instituciones y de particulares, como fue el caso de la Ley del Estado de Colima, abrogada al asumir la Federación la competencia exclusiva en la protección de datos personales en posesión de particulares.

Para finalizar el artículo, vale la pena fijar las bases mínimas para expedir una ley de protección de datos personales en posesión de instituciones públicas. A manera de propuesta y bajo las bases más elementales de Derecho Comparado, se estiman como elementos mínimos para una ley de este tipo que incluya solamente a las instituciones públicas, los siguientes:

- Un apartado de disposiciones generales en el que se establezca el cumplimiento de la misma por parte de las instituciones públicas poseedoras de datos personales.

- Un glosario que defina la naturaleza de la materia de datos personales y del derecho a la privacidad e intimidad, en aras de una mejor comprensión de la materia regulada por dicha ley.

- Los principios rectores de la materia.

- Los derechos de los particulares, y en específico, los llamados derechos ARCO: acceso, rectificación, cancelación y oposición.

- La regulación sustantiva y de trámite de sistemas y bases de datos personales, y el manejo, tratamiento, traslado y diversas operaciones que se realicen en torno a las bases, con inclusión de bases electrónicas o las que se encuentren en formatos impresos, archivados o catalogados.

- La regulación procesal de los derechos ARCO.

- El establecimiento de una autoridad garante de estos derechos, que la tendencia y la comparación jurídica en México encaminan hacia el órgano garante de transparencia.

- Los procedimientos de verificación y cumplimiento de la Ley.
- Y, finalmente, las infracciones y sanciones aplicables.

Referencias

Alexy, Roberto (2006). *Theorie der Juristischen Argumentation. Die Theorie des rationalen Diskurses Die Theorie der Juristischen Begründ*. Existe traducción al español bajo el título Derecho y Razón Práctica. DIBS FONTAMARA.

Bobbio, Norbert (1989) *Estado, gobierno y sociedad: Por una teoría general de la política*. Colección Breviarios, No. 487, Fondo de Cultura Económica, Traducción de José F. Fernández Santillán, México.

Carbonell Sánchez, Miguel (2009) *Los Derechos Fundamentales en México*. Edit. Porrúa, México, 2009, 1150 pp.

Dworkin, Ronald (1993) *Los derechos en serio*, Prólogo de Alberto Calsamiglia, Colección Biblioteca Fundamental.

Garzón Valdéz, Ernesto (2003) . *Lo íntimo, lo privado y lo público*, en Claves de Razón Práctica, No. 137. Madrid, Noviembre.

La seguridad como una pieza clave en el rompecabezas de la protección de datos personales

Lina Ornelas Núñez

Samantha Alcalde Urbina

Lina Ornelas Núñez

Es egresada de la Facultad de Derecho de la Universidad de Guadalajara y es maestra en Derecho Internacional por la Universidad Libre de Bruselas.

Ha trabajado desde hace mas de 12 años en el sector público en México y Europa, en particular para la Comisión Europea y las Secretarías de Economía y Gobernación, en la que fungió como Directora General Adjunta en la Unidad para la Promoción y Defensa de los Derechos Humanos.

Actualmente, coordina subgrupos de trabajo de la Red Iberoamericana de Protección de Datos Personales, es miembro del Consejo Editorial de la Revista de Protección de Datos de la Comunidad de Madrid "Data Protection Review"; miembro de la Asociación Internacional de Profesionales de Privacidad; coautora del capítulo sobre México del libro "Privacidad y Derechos Humanos 2005, 2006 y 2007" publicado por la organización Electronic Privacy Information Center, (EPIC); así como del libro "Protección de datos personales en México: El caso del Poder Ejecutivo". En 2011 publicó como compiladora junto con Carlos Gregorio el libro "Protección de Datos Personales de Menores en las Redes Sociales Digitales. También ha publicado numerosos artículos académicos en la materia.

Se desempeñó desde 2003, como Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información y Protección de Datos, en el que a partir de mayo de 2011 fue nombrada Directora General de Autorregulación en materia de protección de datos personales.

Samantha Alcalde Urbina

Es egresada de la Licenciatura en Derecho por la Universidad Iberoamericana, Campus Santa Fé, Ciudad de México. Por más de 6 años ha trabajado en la Administración Pública Federal, en particular, en Aeropuertos y Servicios Auxiliares y actualmente en el Instituto Federal de Acceso a la Información y Protección de Datos.

En el Instituto Federal de Acceso a la Información y Protección de Datos ha participado en el grupo redactor de la iniciativa de la Ley Federal de Protección de Datos Personales en posesión de los Particulares y su Reglamento. En 2010, publicó el artículo Las redes sociales y la protección de datos personales en menores: perspectiva y retos, en la Revista Documentación número 20 de la Fundación Ciencias de la Documentación.

Desde septiembre de 2011, se desempeña como Subdirectora de Registro de la Dirección General de Autorregulación del Instituto Federal de Acceso a la Información y Protección de Datos.

> Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas, ni entiendes la tecnología.
>
> Bruce Schneider

La doble cara de las tecnologías de la información y del conocimiento

Actualmente, las Tecnologías de la Información y del Conocimiento (en adelante, TIC) hacen posible acceder, manipular y almacenar un número ilimitado de información, -incluyendo datos personales-, lo cual ha representado para las instituciones gubernamentales federales, estatales y municipales una serie de beneficios económicos y sociales.

Es posible afirmar que cada vez más las instituciones gubernamentales se respaldan en este tipo de herramientas para la consecución de sus tareas cotidianas en beneficio de la ciudadanía y buen gobierno, imprimiendo a éstas un toque de agilidad, eficiencia y satisfacción al ciudadano, al tiempo de cumplir a cabalidad con sus atribuciones legales.

Un ejemplo de lo anterior, fue el reconocimiento que este año efectuó la publicación *Information Week* México[1] al Hospital General Dr. Manuel Gea González como una de las 40 instituciones más innovadoras del sector público del 2011.[2]

[1] Esta revista se caracteriza por promover la transformación de las instituciones gubernamentales en México, al reconocer cada año la capacidad e innovación en el uso de herramientas o soluciones de TIC. La selección de los proyectos ganadores se basó en el análisis de su descripción y la congruencia con los resultados obtenidos, así como el impacto alcanzado tanto al interior de la institución como al exterior, es decir, a la ciudadanía a la que sirve, considerando factores como el tiempo de implementación, la inversión realizada, así como las desviaciones que se hubieran presentado en la planeación de estos dos rubros.

Mayor información al respecto, en el siguiente vínculo de Internet: http://www.linkedin.com/news?viewArticle=&articleID=906167389&gid=1778459&type=member&item=79995357&articleURL=http%3A%2F%2Fwww%2Enetmedia%2Einfo%2Fnewsletter%2F2011%2Fnetmedia%2Finnovadoraspublico-2011%2Ehtm&urlhash=oqXH&goback=%2Egde_1778459_member_79995357.

[2] Para conocer otras instituciones federales reconocidas por la revista *Information Week* México, consultar el siguiente vínculo de Internet: http://www.linkedin.com/news?viewArticl

La institución de salud logró agilizar el proceso de solicitud de estudios en línea, así como visualizar los mismos gracias a la integración de un sistema de almacenamiento y distribución de imágenes, así como de un sistema de información en el departamento de imagenología en la arquitectura de sistemas de gestión hospitalaria.

Lo anterior, significa un nuevo modelo de atención a los pacientes, quienes ya no tienen que esperar por los resultados de sus estudios. Por su parte, el hospital experimentó una reducción considerable en la impresión de papel, es decir, menos costos y más eficiencia en la oferta de servicios de salud pública.

Un ejemplo más, es la ambiciosa meta de la Secretaría de Seguridad Pública del Distrito Federal de identificar que la policía esté disponible dónde y cuándo se requiere. Para lo cual, la ciudad se organizó en 918 cuadrantes en los cuales la operación policial es monitoreada y ejecutada a través del Sistema de Geoposicionamiento Policial (SGP), que supervisa mediante geocercas que los policías estén en su área geográfica de responsabilidad, reportándose todas las desviaciones en tiempo real a cada director de cuadrante.

Entre muchas otras funciones, el SGP también genera archivos electrónicos con la posición geográfica de los radios asignados a patrullas y personal en tierra, los cuales se reproducen para poder visualizar la trazabilidad de movimientos de los policías. Se trata del primer sistema electrónico de control de operación policial a nivel nacional, proyecto que también fue reconocido por la revista *Information Week* México este año.[3]

Mientras estas tecnologías abaratan y facilitan el almacenamiento de grandes cantidades de información que son imprescindibles para la gestión gubernamental, constantemente los archivos o bases de datos

eID=906167389&gid=1778459&type=member&item=79995357&articleURL=http%3A%2F%2Fwww%2Enetmedia%2Einfo%2Fnewsletter%2F2011%2Fnetmedia%2Finnovadoraspublico-2011%2Ehtm&urlhash=oqXH&goback=%2Egde_1778459_member_79995357

[3] Para conocer otras instituciones estatales reconocidas por *Information Week* México, consúltese el siguiente vínculo en Internet:
http://www.linkedin.com/news?viewArticle=&articleID=906167389&gid=1778459&type=member&item=79995357&articleURL=http%3A%2F%2Fwww%2Enetmedia%2Einfo%2Fnewsletter%2F2011%2Fnetmedia%2Finnovadoraspublico-2011%2Ehtm&urlhash=oqXH&goback=%2Egde_1778459_member_79995357

gubernamentales están expuestas a ataques de seguridad que pueden devenir en accesos no autorizados, robo, alteración, transferencias ilícitas, copias no autorizadas o fugas de información; misma que ha sido obtenida de los ciudadanos, almacenada; transmitida y utilizada cotidianamente.

A primera vista, la afirmación anterior puede ser considerada como el "simple" extravío de información gubernamental durante el traslado de documentos o archivos oficiales por negligencia, pasando por la venta de bases de datos al mejor postor, o hasta intrusiones no deseadas y uso incorrecto de la información vulnerada.

Ejemplo de lo anterior, fue la denuncia que en abril de 2010 hizo el periódico El Universal sobre la venta de bases de datos en el barrio de Tepito con información personal de millones de mexicanos actualizada al año 2009 a un precio de 12,000 dólares.[4] Entre los productos ofertados a través de memorias externas se encontraban: el padrón electoral del país, o el registro de todos los vehículos y licencias de conducir, números de teléfonos públicos o datos de policías por mencionar algunos (González, 2010).

Las vulneraciones de seguridad ocurren en los gobiernos de todos los países, hay claros ejemplos de ataques a la seguridad a la información gubernamental y por citar tan solo un ejemplo, en Reino Unido se publicaron en noviembre de 2011 varias declaraciones sobre los ciberataques efectuados contra dependencias gubernamentales británicas, incluido un severo asalto a la red del Ministerio de Relaciones Exteriores.

Al respecto, Iain Lobban, Director del Centro Gubernamental de Comunicaciones (GCHQ),[5] señaló que los ataques constituían una amenaza para el bienestar económico de ese país. Por su parte, el

[4] La Comisionada Presidenta del IFAI, en su momento, hizo llegar sendos oficios a las Secretarías de Estado responsables del resguardo de algunas de estas bases de datos para pedirles que revisaran sus procesos de seguridad y el deslinde de responsabilidades. Asimismo, el oficio daba vista al Ministerio Público por la posible comisión de delitos en materia de vulneraciones de seguridad.

[5] La GCHQ, es un órgano de supervisión similar a la Agencia de Seguridad Nacional de los Estados Unidos, que se ocupa de operaciones relacionadas con la recopilación de información y códigos en ataques cibernéticos.

Secretario de Relaciones Exteriores, William Hague, declaró al periódico *Times* que Gran Bretaña sufre alrededor de 600 ataques "maliciosos" contra sus sistemas gubernamentales por día; mientras los criminales podían obtener detalles de tarjetas de crédito robadas a británicos en Internet por sólo 70 peniques.[6]

En noviembre de 2009, en Reino Unido el Ministerio de Defensa admitió haber perdido 500 archivos altamente sensibles con información que describe relaciones extra-maritales, deudas y uso de drogas del personal de la fuerza aérea.[7]

En junio de 2008, el Comisionado de Información de Eslovenia sancionó al alcalde de la región de Borovnica y a su abogado porque el primero le vendió al segundo los datos personales de electores que solicitaban se llevara a cabo un referéndum.[8]

A finales de 2007, el gobierno británico admitió la pérdida de un disco informático que contenía el nombre y número de cuenta bancaria de millones de personas que reciben subsidios en Gran Bretaña, cuando era enviado por correo de una oficina gubernamental a otra (Piñar, 2010).

Así, podríamos citar innumerables ejemplos para darnos cuenta que cualquier situación imaginable es actualmente posible, a tal grado de afirmar que los fallos de seguridad en los archivos gubernamentales no sólo pueden repercutir en la continuidad de las operaciones de dichas instituciones o la detección de fallas mayores en los propios sistemas de información que sean irreversibles o con altos costos de reparación, generando afectaciones directas o indirectas en la esfera de otros derechos y libertades fundamentales de las personas, concretamente en la privacidad de éstas.

[6] Holden, Micahel y Pipen, Elizabeth, U.K. Cyber attacks on government happen 600 times per day. Disponible en el siguiente vínculo de Internet: http://www.huffingtonpost.com/2011/10/31/uk-cyber-attacks_n_1067084.html.

[7] Fuente: BBC News.

[8] Fuente: Oficina del Comisionado de Información de la República de Eslovenia.

El derecho a la protección de datos personales como un mecanismo de defensa a nuestra privacidad

Con el desarrollo vertiginoso de las TIC existen constantes violaciones a la privacidad de las personas, y de manera particular, se da el fenómeno de accesos, usos y transmisiones indiscriminadas y no autorizadas de información personal, que como fue posible observar en los ejemplos anteriores estos fenómenos también se hacen presentes en los archivos gubernamentales.

Así, el uso de las Tecnologías de la Información y sus implicaciones para la vida de las personas dieron origen a un nuevo derecho relacionado con la protección de los datos personales.

Para definir la naturaleza del derecho a la protección de datos personales, conviene citar lo que señala magistralmente la Sentencia del Tribunal Constitucional Español 292/200 al respecto[9]. A manera de contexto, la *litis* de esta sentencia del 30 de noviembre del 2000, versa sobre el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal del 13 de diciembre de 1999. De manera paralela en que la sentencia se pronuncia sobre la inconstitucionalidad de estas disposiciones, entre los argumentos se van sentando las bases jurídicas que tajantemente reconocen un nuevo derecho fundamental:

> […] En cambio, el derecho fundamental a la protección de datos personales persigue garantizar a la persona un poder de disposición y control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. [E]sta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso

[9] El texto completo de la sentencia se puede consultar en el siguiente vínculo de Internet: http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf.

> o divulgación indebidas de dicha información. Pero ese poder de disposición no vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.
> [...]
>
> El derecho a la protección de datos personales atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.
> [...]
>
> [énfasis añadido]

De esta manera, *el derecho a la protección de datos personales se erige como el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.*

También se le conoce como el derecho a la autodeterminación informativa que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaban, manejan y utilizan sus datos personales.

Concretamente, de acuerdo con los instrumentos y estándares internacionales y la legislación nacional y estatal aplicable al sector público y privado en la materia, es posible afirmar que los deberes de hacer a que se refiere la sentencia española se concretan en una serie de obligaciones comúnmente conocidas como *principios de protección de datos personales*, los cuales consisten en:

- Obtener la autorización del titular de los datos para el aprovechamiento de su información (principio de consentimiento).
- Informar al titular de los datos personales el uso que se le dará a los mismos, así como los términos y condiciones que distinguen

el tratamiento a que será sometida su información (principio de información o transparencia).

- No utilizar medios engañosos o fraudulentos para obtener los datos personales (principio de lealtad).

- Tratar los datos personales respetando la legislación nacional e internacional (principio de licitud).

- Restringir el tratamiento de la información personal al cumplimiento de finalidades determinadas y legítimas (principio de finalidad).

- Usar sólo los datos personales que resulten estrictamente necesarios con relación a las finalidades previstas (principio de proporcionalidad).

- Mantener los datos personales actualizados (principio de calidad).

- Limitar el periodo de conservación de la información personal tratada al mínimo necesario y suprimir ésta cuando hayan concluido las finalidades que dieron origen al tratamiento (principio de calidad).

- Implementar medidas y controles de seguridad que garanticen la confidencialidad e integridad de los datos personales (deber de seguridad).

- Guardar la confidencialidad de la información personal en todas las fases del tratamiento de ésta (deber de confidencialidad).

- Adoptar las medidas necesarias para cumplir con los principios y obligaciones en materia de protección de datos personales, así como rendir cuentas al titular en caso de incumplimiento (principio de responsabilidad).

De manera complementaria a estas obligaciones de hacer o no hacer impuestas al responsable del tratamiento de los datos personales, el derecho a la protección de datos personales también otorga una gama

de poderes jurídicos que garantizan a la persona el poder de decisión y control que tiene sobre su información, y actúan como complemento del deber del responsable de velar por el efectivo cumplimiento de las obligaciones que le son impuestas por la ley, permitiéndole conocer aquellos casos en los que el tratamiento pudiera no resultar ajustado a los mismos.

Entre estas prerrogativas del individuo se encuentran los *derechos ARCO* que se refieren a la posibilidad de:

- Acceder a los datos personales y solicitar cualquier tipo de información relacionada con las generalidades o características del tratamiento a que están siendo sometidos los datos personales del titular.

- Rectificar la información personal que resulte ser inexacta o incompleta.

- Cancelar los datos personales que no están siendo tratados conforme a los principios, deberes y obligaciones establecidas en la ley.

- Oponerse al tratamiento de los datos personales cuando concurra una razón legítima derivada de una situación personal del titular, o bien, para el tratamiento de una finalidad en específico.

Es así, que esta serie de principios (obligaciones) y derechos ARCO que dan contenido al derecho a la protección de datos personales, actúan coordinada e integralmente para garantizar la efectiva protección de la privacidad de las personas, con relación al tratamiento de su información.

Lo que se traduce, en que el titular de la información sea quien detente única y exclusivamente ese poder de control y disposición que tiene sobre sus datos personales, y por consiguiente, tenga la libertad de elegir qué datos, cuándo y a quién comunica los mismos -autodeterminación informativa-.

La seguridad como una pieza clave en el rompecabezas de la protección de datos personales

Si bien las disposiciones normativas en materia del ejercicio de derechos ARCO y la observancia de los principios de licitud, consentimiento, calidad, proporcionalidad, información, lealtad y responsabilidad, son importantes, de nada o poco serviría que un responsable de tratamiento cumpla con todo lo anterior, si no se otorgan garantías suficientes en materia de seguridad de la información.

Cuando a una persona le roban el coche o la cartera, se puede percatar de ello casi de inmediato, sin embargo, cuando nos roban nuestros datos personales no es tan evidente.

La implementación de medidas y controles de seguridad aplicables a los archivos o bases de datos personales se constituyen en el gran candado que resguarda y acompaña todo ciclo de tratamiento de información personal.

Ahora bien, imagine las piezas de un rompecabezas que generalmente se pueden clasificar en "piezas centrales" y "piezas de las orillas y esquinas". Haciendo una analogía, si diéramos una función clave a estas piezas dentro del mundo y entramado de la protección de los datos personales, las piezas centrales del rompecabezas se equipararían a los principios y derechos mencionados en el apartado anterior, mientras que todas y cada una de las piezas de las orillas y esquinas al delinear y establecer el contorno y límite del rompecabezas, se erigirían como el escudo protector que enmarca las piezas centrales.

En este sentido, como ya se afirmó, de poco sirve el cumplimiento de los principios de protección de datos personales o la habilitación de mecanismos que permitan el ejercicio de los derechos ARCO, sin la existencia de medidas de seguridad cuya función sea expresamente evitar el robo, fuga, pérdida, modificación, alteración, venta ilegal, acceso o transmisión no autorizada de la información personal. Siguiendo la analogía, sería inútil la existencia de las piezas centrales de un rompecabezas si no hay un muro de contención sobre el cual se erijan.

En la actualidad, la información se ha convertido en el activo fundamental para las instituciones gubernamentales que al igual que las instalaciones, capital humano y recursos financieros, debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por las propias instituciones.

En el sector público el riesgo de sufrir la pérdida de información -incluyendo datos personales-, bien sea producto de la voluntad de un agente pernicioso o bien resultado del caso fortuito, siempre está presente y latente. Es una realidad, que las vulneraciones de seguridad generan altos costos para las institucionales, además de afectaciones colaterales hacia la ciudadanía si la pérdida de información se trata de datos personales.

Es así, que la seguridad en el tratamiento de la información personal es de vital importancia y se ha convertido en una pieza clave para garantizar de forma efectiva la privacidad de las personas, estableciendo controles específicos que impidan el acceso indebido a la información personal tratada manteniendo su carácter confidencial.

Al mismo tiempo, la garantía de la privacidad exige también que se mantenga la integridad y disponibilidad de los datos personales, de tal manera, que la implementación de medidas y controles que la información esté completa (íntegra) y la recuperación de los datos en caso de producirse un ataque, vulneración o fallo de seguridad que ponga en riesgo la continuidad de las operaciones gubernamentales, o bien, la privacidad de las personas (disponibilidad y redundancia).

A efecto de evitar cualquier vulneración o incidente que pueda comprometer la seguridad de los datos personales o cualquier otra información (de seguridad nacional por ejemplo), las institucionales gubernamentales están obligadas a implementar acciones y controles específicos de carácter administrativo, físico y técnico que resulten necesarios y adecuados en rubros como:

- La gestión y resguardo de soportes físicos y electrónicos.
- El uso de bitácoras para el registro de accesos y operaciones cotidianas.

- La gestión de incidentes.
- El acceso a las instalaciones y a los "*data center*" o centros de procesamiento de datos.
- El establecimiento de controles de acceso y privilegios de las personas autorizadas para acceder, consultar, modificar o realizar cualquier operación con la información.
- El traslado de datos personales de forma segura.
- Los procedimientos de respaldo y recuperación de datos.
- El plan de contingencia.
- La realización periódica de revisiones o auditorías.
- La capacitación al personal.
- La construcción de una cultura institucional de seguridad integral.

Por otra parte, es importante destacar que el nivel de complejidad de las medidas y controles de seguridad a implementar dependerá de factores como el riesgo existente, la naturaleza y tipo de datos personales sometidos a tratamiento, del estado de la técnica o desarrollo tecnológico, del contexto en que se efectúe el tratamiento y las obligaciones que exija la legislación aplicable.

Por ejemplo, las medidas deberían extremarse en los casos de tratamientos de datos personales de carácter sensible, o bien, si el tratamiento permite delimitar un perfil claro de la situación familiar y económica de las personas, pudiendo incluso obtenerse conclusiones no conocidas conscientemente por el propio individuo, como sucede en las bases de datos relacionadas con programas sociales de subsidio, para evitar que tal información pueda llegar a manos de un tercero mal intencionado.

Por otro lado, diversos consultores y agencias en seguridad informática recomiendan los siguientes marcos de referencia o

estándares para asegurar la protección efectiva de la información, incluyendo datos personales y de los insumos informáticos en toda organización:

Estándar	Finalidad
NORMA MEXICANA NMX-I-27001-NYCE-2009 Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de la seguridad información - Requisitos.	Esta Norma Mexicana es aplicable a todo tipo de organización (empresas, organismos y entes públicos, entidades sin ánimo de lucro o cualquier otra). Se distingue por señalar los requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad Informática documentado, en el marco de los riesgos empresariales generales de la organización.
NORMA MEXICANA NMX-I-27002-NYCE-2009 Tecnología de la Información - Técnicas de seguridad - Código de buenas prácticas para la gestión de la seguridad de la información.	Esta Norma Mexicana establece una serie de recomendaciones para la administración de la seguridad de la información, que pueden servir de utilidad en la implementación o mantenimiento de un sistema de gestión de la seguridad de la información dentro de una organización.
ISO/IEC 27001 (2005) Information technology - Security techniques - Information Security management systems - Requirements.	Este estándar diseña un modelo para gestionar la seguridad de la información, modelo que también es aplicable fuera de los sistemas informáticos.
ISO/IEC 27002:2005 Information trechnology - Security Techniques - Code of practice for information security management.	Es una guía de buenas prácticas que describe los controles recomendables en cuanto a seguridad de la información.

Asimismo, es necesario contar con personal certificado en rubros específicos de la seguridad de la información, puede resultar de gran valía y ayuda en la implementación de una política integral de seguridad al interior de la organización:

Certificación	Finalidad
CISSP (Certified Information Systems Security Professional)	Certificación de alto nivel profesional otorgada por la International Information Systems Security Certification Consortium con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información.
CISA (Certified Information Systems Auditor)	Certificación para auditores en sistemas respaldada por la Asociación ISACA, Information Systems Control Association .
CISM (Certified Information Security Management)	Certificación para administradores de seguridad de la información respaldada por la ISACA

Finalmente, el deber de confidencialidad que tiene toda persona involucrada en el tratamiento de información personal es la contrapartida necesaria de la seguridad en el tratamiento. Resultaría insuficiente la implementación de medidas tendentes a evitar el robo, fuga, pérdida, modificación, alteración, venta ilegal, acceso o transmisión no autorizada de la información personal, si las personas (empleados, prestadores de servicios o terceros) que intervienen en el tratamiento no actúan con la debida cautela y discreción sobre la información personal que tratan durante el desarrollo de su actividad o una vez que han concluido las actividades del tratamiento.

Una situación que ocurre de manera frecuente, es que las contraseñas de los equipos que tienen accesos privilegiados para ciertos servidores públicos, se encuentran a la vista de cualquiera al ser pegados en pequeñas papeletas adheribles y con colores llamativos. Otra mala práctica es que los equipos portátiles no tienen canceladas las entradas a dispositivos USB y pueden sacarse de los lugares de trabajo sin ser revisados por personal de seguridad. Así, el deber de confidencialidad se erige como la obligación dirigida a quienes intervienen en cualquier fase del tratamiento de datos personales de guardar y respetar la confidencialidad de los mismos, obligación que subsistirá aún después de finalizar el tratamiento.

Los Lineamientos de Protección de Datos Personales y su modelo de seguridad

Los Lineamientos de Protección de Datos Personales[10] (en adelante, los Lineamientos) son disposiciones administrativas de carácter general y obligatorio que tienen por objeto establecer las políticas generales y procedimientos que deben observar las dependencias y entidades de la Administración Pública Federal, para garantizar a toda persona la facultad de decisión sobre el uso y destino de su información, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos de la persona. Si bien, la seguridad de los datos debe preverse en todos los sujetos regulados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, esto no se ha desarrollado de manera armónica en cada uno de ellos. El Poder Ejecutivo Federal es el que cuenta con los mayores avances en este tema. De manera particular, cabe destacar algunas de las principales obligaciones de seguridad que prevén los Lineamientos en mención:

- La expedición de un documento de seguridad que contenga las medidas administrativas, físicas y técnicas aplicables a los archivos y bases de datos en posesión de las Dependencias y Entidades en el ámbito de la Administración Pública Federal, siendo de observancia obligatoria para todos los servidores públicos, prestadores de servicios contratados y personas externas que tengan acceso a la información personal o al sitio donde se encuentre ésta.[11]

- El establecimiento de procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación de las bases de datos.

- La actualización de información.

[10] Los Lineamientos de "Protección de Datos Personales" fueron publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

[11] El Trigésimo cuarto de los Lineamientos describe puntualmente el contenido del documento de seguridad.

- La habilitación de procedimientos de creación de copias de respaldo y de recuperación de datos.

- El uso de bitácoras que registren las acciones cotidianas que se llevan a cabo con los sistemas de información gubernamentales.

- El establecimiento de procedimientos de notificación, gestión y repuesta de incidentes.

- El diseño y habilitación de mecanismos de auditorías o rastreabilidad de operaciones.

- El control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales.

- El diseño de planes de contingencia que garanticen la continuidad de la operación, así como la realización de pruebas de eficiencia de los mismos.

Como se puede observar, las acciones y medidas de seguridad en su conjunto permiten atender todos aquellos puntos vulnerables de los sistemas de información, así como monitorear las operaciones a efecto de que los controles y medidas siempre respondan a la realidad del tratamiento. Asimismo, es muy importante mencionar que el IFAI emitió una Guía para la elaboración de un documento de seguridad con la finalidad de que las todas las Dependencias y Entidades cuenten con un documento que establezca los roles de cada servidor público en esta materia, así como los controles a implementar para cada sistema de datos personales. Por último, conviene resaltar que el IFAI ha llevado a cabo diversas verificaciones en materia del cumplimiento de los principios y derechos en materia de protección de datos personales, resaltando que siempre se incluye un apartado con recomendaciones concretas en materia de seguridad.

Es este punto se subraya la recomendación hecha a la SEGOB para la emisión de una Cédula de Identidad personal y ciudadana, así como el mantenimiento y operación del Sistema Nacional de Identidad. Dicha dependencia se encuentra atendiendo las recomendaciones emitidas por el Instituto, ya que se trata de un proceso holístico y vivo, en donde es necesario hacer un análisis de riesgo y de gestión de la seguridad,

implementar los controles y verificar que se apliquen adecuadamente *(Plan, do, check aprroach).*

Normas generales en materia de seguridad de la información para la Administración Pública en el Distrito Federal

Es importante mencionar que dentro del marco jurídico aplicable al Distrito Federal existen disposiciones específicas en materia de seguridad denominadas "Normas generales que deberán observarse en materia de seguridad de la información de la Administración Pública Federal", publicadas en la Gaceta Oficial del Distrito Federal el 9 de julio de 2007.[12] Estas normas de observancia general tienen por objeto proporcionar el marco de referencia para que cualquier instancia de la Administración Pública del Distrito Federal pueda establecer, aprobar, evaluar un sistema de gestión de la seguridad de la información, con base en la mejores prácticas. Concretamente, estas normas generales establecen una serie de principios en materia de seguridad, a saber: Las dependencias, delegaciones, órganos desconcentrados y entidades deberán:

- Ser conscientes de la necesidad de contar con tecnologías de la información seguras y responsables de los recursos de TI (principio de concientización y responsabilidad).

- Actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad de los recursos de TI (principio de respuesta).

- Respetar los intereses legítimos de terceros (principio de actuación ética).

- Hacer compatibles la seguridad de las tecnologías de la información con los valores esenciales de un gobierno democrático que pretende transparentar su gestión (principio de transparencia).

[12] El texto completo de la normas generales está disponible en el siguiente vínculo de Internet: http://www.consejeria.df.gob.mx//uploads/gacetas/julio07_9_121.pdf

- Llevar a cabo evaluaciones de riesgo (principio de evaluaciones del riesgo).

- Incorporar la seguridad como un elemento esencial de los recursos de TI (principio de diseño y realización de la seguridad).

- Adoptar una visión integral de la administración de la seguridad de los recursos de TI (principio de la gestión de la seguridad).

- Revisar y reevaluar la seguridad de sus recursos de TI y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad (principio de seguimiento).

Asimismo, con base en estos principios rectores las normas generales desarrollan concretamente los controles de seguridad que deberán ser aplicados a todos los ámbitos de la gestión gubernamental, basados en las siguientes acciones cíclicas con un enfoque de mejora continua que se representan en la siguiente gráfica:

Sin duda, esta aportación normativa que hace el Distrito Federal coadyuva a promover una cultura de seguridad al interior de las organizaciones que integran la Administración Pública del Distrito Federal, salvaguardando y manteniendo la confidencialidad, integridad disponibilidad y autenticidad de la información de tal manera que sirva para la consecución de los objetivos de dichas instituciones gubernamentales, y por consiguiente, eleve la calidad y eficiencia de los servicios públicos ofrecidos a la ciudadanía.

Asimismo, derivado de la exhaustividad e importancia que estas normas generales le dan al tema de la seguridad de la información, pueden servir como modelos normativos para ser adoptados en los Estados de la República e incluso a nivel federal.

Un proyecto truncado

Un esfuerzo loable en este tema que se llevó a cabo a finales del 2008 y durante el 2009, fue la elaboración del anteproyecto normativo denominado "Lineamientos en materia de seguridad de la información en posesión de las dependencias y entidades de la Administración Pública Federal", esfuerzo liderado por la Secretaria de la Función Pública. Este anteproyecto tenía por objeto el establecimiento de un sistema de administración de la seguridad basado en la familia de estándares ISO/IEC 27000.

Cabe destacar que un aspecto importante de esta propuesta, fue la creación de órganos especializados al interior de las dependencias y entidades federales, con la atribución específica de conducir la política de seguridad y desarrollar programas para la adopción de Tecnologías de la Información, con el fin de facilitar y mejorar sustancialmente los trámites y servicios públicos.

Lamentablemente, a pesar de los esfuerzos y la cooperación entre las dependencias y entidades federales que participaron encaminadas a concretar un anteproyecto de lineamientos consensado, el proyecto normativo se quedó en el tintero y se optó por publicar un manual menos exhaustivo.

La privacidad por diseño como una alternativa valiosa en materia de seguridad

Una nueva tendencia que se ha identificado para materializar el binomio perfecto entre privacidad y seguridad, es la *privacidad por diseño*, práctica que ha permitido conciliar por una parte, los requerimientos de seguridad exigidos en las legislaciones nacionales o estándares internacionales, y por el otro, garantizar una protección efectiva de la información tratada en la consecución de políticas públicas o modelos de negocios.

La privacidad por diseño (*privacy by design*) parte de la premisa de que la privacidad no puede ser concebida como un cumplimiento legal, sino más bien, como una buena práctica, que por defecto debe estar presente desde la concepción y diseño de cualquier política pública.

De acuerdo con la Comisión de Información y Privacidad de Ontario (Canadá) la privacidad por diseño se basa en 7 principios fundamentales:[13]

1. *Preventivo, no correctivo:* la privacidad por diseño previene intrusiones de privacidad; no espera a que los riesgos se materialicen y mucho menos ofrece remedios o medidas para resolver infracciones una vez que ya ocurrieron. La privacidad por diseño llega antes del suceso, no después.

2. *Configuración predeterminada:* ¡Lo predeterminado es lo que manda!, la protección de los datos personales está implícita desde el diseño del sistema como una configuración por defecto o predeterminada.

3. *Incrustada en el diseño:* la privacidad se convierte en un componente esencial del modelado y arquitectura de los sistemas de información.

4. *Todos ganan:* la privacidad por diseño busca satisfacer y conciliar todos los intereses y objetivos legítimos en cualquier política

[13] Para mayor información al respecto, se recomienda consultar los siguientes vínculos en Internet:http://www.privacybydesign.ca

pública o modelos de negocio, bajo el lema "ganar-ganar", demostrando que sí es posible conciliar privacidad y seguridad.

5. *Seguridad extremo-a-extremo:* la privacidad por diseño se extiende a todo el ciclo de vida completo de los datos personales, garantizando una administración segura de éstos de un extremo a otro.

6. *Visibilidad y transparencia:* la privacidad por diseño permite la verificación a todos los actores involucrados.

7. *Enfoque centrado en la persona:* por encima de todo, la privacidad por diseño requiere que los arquitectos y operadores de los sistemas de información mantengan partan de la premisa de privilegiar los intereses de las personas, colocando a éstas como el centro de las prioridades.

Lotería y Juegos de Ontario

Un caso de éxito que vale la pena resaltar sobre los beneficios que proporciona esta nueva tendencia de privacidad, es el programa de exclusión voluntario de personas con problemas de adicción al juego implementado por la empresa estatal de Lotería y Juegos de Ontario (*The Ontario Lottery and Gaming Corporation*).[14]

Básicamente, este programa consiste en la inscripción voluntaria de personas con problemas de adicción al juego ante la empresa estatal canadiense, con la finalidad de que si en algún momento su fuerza de voluntad es flaqueada por la ansiedad del juego y se dirigen a un casino, el programa ofrece y garantiza la detención inmediata de los registrados al momento de pretender ingresar al casino.

Esta detención se realiza por medio del reconocimiento facial de las personas registradas una vez que las cámaras instaladas en la entrada de los casinos captan su rostro, imagen que es cotejada con el sistema de información creado para tal efecto. El sistema de información y las

[14] Para mayor información al respecto, se sugiere consultar los siguientes vínculos de Internet:http://www.olg.ca y http://privacybydesign.ca .

tecnologías habilitadas para tal fin, ha logrado incorporar desde su arquitectura y desarrollo la privacidad por defecto o predeterminada, lo cual ha permitido cumplir con los objetivos centrales del programa de exclusión impidiendo la entrada a personas que se han registrado en el programa, y a su vez, evitar afectaciones o intrusiones a la privacidad de éstas que puedan derivar en accesos no autorizados o fugas de información lesivas para la dignidad y derechos de éstas. Por supuesto, la base de datos con imágenes faciales cuenta con un alto nivel de seguridad para evitar que sea utilizada para otras finalidades.

Reflexiones a manera de conclusión

Es imprescindible procurar la seguridad de la información en posesión de las instituciones gubernamentales, particularmente esta imperiosa necesidad se atenúa por el uso extensivo de las tecnologías de la Información y las comunicaciones, ya que actualmente ésta se ha convertido en un activo fundamental para el quehacer gubernamental.

Es un hecho que la seguridad de la información no es un tema específicamente tecnológico, recae en personas y por tanto se constituye en un problema organizacional de amplio espectro. La elaboración de documentos de seguridad, las verificaciones de los planes y controles, así como el involucramiento al más alto nivel de las autoridades (alta dirección), son indispensables para lograr estrategias exitosas. La seguridad no puede ser absoluta, pero si puede gestionarse el riesgo y mitigar sus impactos negativos al contar con estrategias concretas de reacción inmediata.

Como ya se dijo, es evidente que no existe una solución única para la seguridad de la información ni políticas, o estándares o prácticas que garanticen el 100% de la seguridad, sino más bien es necesario identificar las necesidades comunes aplicables a las administraciones públicas, a fin de establecer marcos de referencia transversales que permitan una mejor gestión de la tecnología en beneficio de los mexicanos. Pueden explorarse códigos y mejores prácticas para sectores como el de salud o financieros, con el consecuente ahorro de costos y el beneficio del conocimiento compartido. Es necesario que las instituciones gubernamentales le apuesten a la creación y promoción de una cultura de la seguridad de la información, con la finalidad de

prevenir ataques malintencionados que pueden afectar la reputación y el posicionamiento del gobierno frente a los ciudadanos. Por último, dos asignaturas pendientes, la primera es involucrar a las autoridades en el ámbito penal, a fin de que cuenten con los mecanismos tecnológicos para poder reaccionar y encontrar las evidencias concretas que les permitan ejercer la acción penal en contra de aquellos que cometan delitos relacionados con vulneraciones de seguridad de la información y estos no queden impunes.

La segunda, es la adecuación de los marcos normativos en materia de protección de datos en el ámbito público ya que no se cuenta con leyes especiales en la materia en la Federación, y solo algunas Entidades Federativas como el Distrito Federal o Guanajuato por citar 2 ejemplos, cuentan con leyes comprehensivas. Las políticas públicas por venir, deberán acentuar el tema de la seguridad de la información de las personas, para garantizarles bienestar y tranquilidad.

Referencias

González, María de la Luz (2010) *Tepito vende bases de datos oficiales*, 19 de abril de 2010. Disponible en el siguiente vínculo de Internet: http://www.eluniversal.com.mx/notas/673768.html.

Holden, Micahel y Pipen, Elizabeth U.K. *Cyber attacks on government happen 600 times per day*. Disponible en el siguiente vínculo de Internet al 22 de diciembre de 2011 http://www.huffingtonpost.com/2011/10/31/uk-cyber-attacks_n_1067084.html.

Piñar Mañas, José Luis (2010), *¿Existe la privacidad?*, Compendio de lecturas y legislación. Protección de Datos Personales, México, Tiro Corto Editores, 23 pp.

Protección de Datos Personales en los medios de comunicación

Blanca Lilia Ibarra Cadena

Blanca Lilia Ibarra cadena

Fue electa Comisionada Propietaria de la Comisión para el Acceso a la Información Pública por el H. Congreso del Estado de Puebla, el 11 de diciembre de 2008 y el 10 de enero de 2011 fue nombrada por unanimidad Presidenta de la CAIP. Directora de Comunicación a Medios de los Estados de la Presidencia de la República y Directora General de Comunicación Social del Congreso del Estado.

Es fundadora de la Asociación de Mujeres Periodistas y Escritoras de Puebla y ha sido catedrática en el Instituto Tecnológico de Estudios Superiores de Monterrey, campus Puebla. Ha recibido reconocimientos a nivel nacional por su trayectoria periodística por el Club de Periodistas de México, el Sindicato Nacional de Redactores de la Prensa y recientemente por el Club Primera Plana.

Por 15 años realizó actividades profesionales como conductora y productora de diversos programas de opinión y noticias en Televisa Puebla. También ha conducido programas en SICOM Televisión, en estaciones de Grupo Acir y Radio Tribuna. Colaboró en el Periódico El Sol de Puebla y es autora del libro "Expresiones, de lo público a lo privado".

Licenciada en Ciencias de la Comunicación con maestría en Administración de la Gestión Pública por el Instituto de Administración Pública de Puebla y con estudios de maestría en "Gobierno y Administración" por la Benemérita Universidad Autónoma de Puebla. Ha realizado diplomados en Transparencia en la Gestión Pública, Mercadotecnia Política y Procesos Electorales, Comunicación Social y Gobierno y en Política Internacional.

Introducción

Indiscutiblemente los medios de comunicación han sido parte fundamental en los cambios sociales, políticos y culturales en México. La democracia se ha visto fortalecida con la apertura de la información gubernamental a través de las leyes de transparencia que existen en todo el país. No obstante, en este ejercicio social de comunicación aún quedan algunos temas pendientes para la discusión; tal es el caso del uso y manejo de los datos personales en la difusión de las noticias y la invasión en la esfera privada de las personas por parte de los medios de comunicación.

Si bien es cierto que existen algunos principios deontológicos que rigen, de forma volitiva, la conciencia y el actuar profesional de los informadores para respetar la intimidad, el honor y la propia imagen, también lo es que en múltiples ocasiones estos fundamentos se contraponen con otros, como el derecho a la información y la libertad de expresión. Es por ello que los procesos de autorregulación y normatividad legislativa tienden a crear reglas que atiendan las necesidades actuales.

En este estudio se observa que existen escasos referentes institucionales en el sector público, para la protección de los datos personales en comunicados oficiales, por lo que únicamente se abordarán algunas directrices que han considerado los órganos encargados de impartir justicia en México, cómo depositarios de información confidencial. Asimismo se hará un breve recorrido de casos por el que los medios de comunicación y la sociedad civil organizada, han realizado para aliarse y determinar cuál debe ser la mejor forma para comunicar la ola de violencia presentada en el país, y adoptar acuerdos específicos para la protección de los datos personales.

Medios de Comunicación-Estado: una relación en constante transformación

La vida democrática mexicana ha transitado, aunque muy lentamente, por caminos nunca antes explorados. Aún con esa lentitud, hemos sido sorprendidos con el surgimiento de temas de carácter mundial,

que hoy deben ser motivo de análisis en nuestro país. Mucho se ha discutido el caso específico de los medios de comunicación y el papel que desempeñan en la democracia. Es indudable que han sido protagonistas del cambio, la crítica y la pluralidad. Sin embargo, el actual escenario los ha colocado frente a nuevos retos y desafíos que requieren necesariamente su atención. Es momento ya, por ejemplo, de discutir el papel que deben asumir ante uno de los grandes problemas que aquejan a la población mundial, y que es tema de preocupación tanto de gobiernos de las naciones, como de organismos internacionales y de la población en general: la vulneración de los datos personales y la consecuente invasión a la esfera privada de las personas.

El establecimiento de códigos éticos en los medios de comunicación es otro tema poco explorado. Existen escasos antecedentes sobre la necesidad de regular aspectos relacionados con la privacidad, el honor, las relaciones con las fuentes y la incompatibilidad de algunas actividades con la tarea de informar. No hay claridad respecto a los mecanismos que se deben aplicar para que se cumplan dichos códigos, en caso de que éstos existan.

La falta de una regulación y de una definición expresa sobre el papel de las redes sociales y las nuevas tecnologías, para ser concebidas o no como medios de comunicación, es también otra de las asignaturas pendientes por resolver.

La evidente escasez de informes, análisis, documentos y trabajos de investigación sobre estos temas ratifica su ausencia en la agenda de prioridades de analistas, académicos y los propios medios de comunicación. En el terreno de la práctica, no hay referencias que ayuden a entender su comportamiento, tampoco existen experiencias concretas en agencias periodísticas o en oficinas de gobierno que permitan realizar un análisis comparado.

En síntesis, en nuestro país no hay antecedentes que sirvan como punto de partida para entender, o explicar, el papel que desempeñan los medios de comunicación respecto a la protección de datos personales y el derecho a la privacidad de los ciudadanos. Esa es la realidad. También nuestra historia. Ante este desértico panorama, es imperioso construir una agenda de trabajo para discutir la naturaleza, utilidad, importancia, función y carácter de la protección de datos

personales. En particular es necesario explorar su relación con los medios de comunicación, como se advertirá a lo largo de estas líneas; definir líneas de acción que se deberán seguir en las instituciones del Estado y en las oficinas de gobierno, así como en los propios medios. El reto, desde luego, es mayor, sobre todo porque es algo que debemos construir.

En la medida en que nos adentremos al tema, el debate conducirá a otros lugares complicados, como lo son la delimitación de lo público y privado, el derecho a la libertad de prensa y de expresión, el derecho al acceso a la información y la transparencia, la ética periodística, entre otros. Aspectos todos ellos que están inmersos en la protección de datos personales. La discusión, sin embargo, es necesaria; nuestro país, al igual que otras naciones, vive este problema como un asunto de interés público.

En el fondo de los múltiples debates, sin duda está, el de la definición de la nueva relación medios de comunicación-Estado-sociedad. Orientando al análisis de sus vínculos, el material producido al respecto es abundante. En los últimos años, por ejemplo, han sido publicados infinidad de textos, ensayos y artículos que tienen el propósito de documentar la importancia que los medios de comunicación tuvieron en el proceso de transición en la democracia mexicana, por mencionar algunos, "La nueva comunicación", de Manuel Castells, Ignacio Ramonet, Armand Matterlart y otros (2006), o "Estrategias de Comunicación para gobiernos", de Roberta Izurieta, Rubén M. Perina y Christopher Arterton (2001).

Durante este largo y complejo proceso, el surgimiento de espacios noticiosos en la radio y los medios impresos fue perfilando una figura más plural del periodismo, a partir de los diferentes enfoques editoriales. Su influencia en la toma de decisiones por parte de los ciudadanos creció considerablemente, sobre todo la de carácter electoral. La crítica se fortaleció.

La relación que existió entre los medios de comunicación y el Estado surgido de la Revolución de 1910 creó, como en otros sectores empresariales, las condiciones para establecer una relación de intercambio con los medios corporativos. En ella, el Estado otorgó beneficios técnicos y económicos que favorecieron el desarrollo de

negocios rentables, a cambio del apoyo irrestricto al régimen político (Guerrero, 2010).

Sin embargo, sería un error afirmar que, en aquellos años, la libertad de expresión y de prensa fuera inexistente, o que la característica dominante haya sido la censura total. Evidentemente, la relación entre medios de comunicación y el Estado fue difícil, con momentos significativos de fuerza entre unos y otros. El régimen encontró una salida adecuada que permitiera determinar los límites de la opinión pública, sin necesidad de prohibir la libertad de expresión. El instrumento eficaz fue legislar la materia; es decir, recurrir a la ley para legitimar las acciones del Estado. Uno de los grandes especialistas en el tema, Miguel Ángel Granados Chapa, lo escribió de la siguiente manera:

> Más que un control gubernamental sobre la prensa (y los medios, en general), la verdad es que se trata de un autocontrol, una especie de censura ambiental. Los medios saben hasta dónde llegar, o por lo menos, saben hasta dónde quieren llegar. Los eventuales mecanismos de control no se utilizan porque, en realidad, se vuelven innecesarios. (Granados Chapa, 1981:9).

Al paso de los años, como resultado del proceso de liberalización política, la presencia de la prensa crítica modificó la relación de los medios con el Estado.

Medios de comunicación y democracia

Se ha dicho con insistencia que la democracia sin los medios de comunicación difícilmente podría ser un proyecto de largo aliento para el país. El razonamiento parece correcto si nos apoyamos en la idea de Norberto Bobbio (1986), de asumir a la democracia como el gobierno del poder público en público.

Esta forma de gobierno considera la existencia de ciudadanos libres que vigilan el desempeño de las instituciones públicas y de quienes las conducen. También permite que en una sociedad abierta, para definirla en los términos de Karl Popper (1997), los gobiernos tienen que actuar bajo vigilancia de los ciudadanos y, en consecuencia, con transparencia.

En efecto, una democracia se caracteriza por tener un gobierno abierto a los ciudadanos (*open government*), lo cual implica, entre otros aspectos, que la información gubernamental esté disponible para cualquier ciudadano que la solicite, salvo casos de excepción determinados por la propia ley, y que los funcionarios de gobierno rindan cuentas de sus acciones. Bajo esta perspectiva, en el nuevo contexto democrático la transparencia adquiere especial importancia en un gobierno que se abre a las exigencias ciudadanas de obtener información de utilidad.

Y aunque la transparencia no es exclusiva del gobierno, es en este ámbito donde el concepto ha sido colocado de manera sistemática. Bajo este razonamiento, un gobierno elegido democráticamente, ha de someterse por su propia naturaleza política al escrutinio público, ya que una de las reglas del régimen democrático es que el gobierno debe alumbrar los espacios públicos del poder, que en el pasado habían sido cobijados por la oscuridad de la impunidad y la discrecionalidad.

De esta forma, informar sobre los asuntos públicos, se convierte en un derecho ciudadano y una obligación del gobierno. Como bien lo refiere Norberto Bobbio:

> La obligación de publicar los actos de gobierno es importante no sólo, como suele decir, para permitir al ciudadano sobre los actos de quien detenta el poder y por tanto de controlarlos, sino también porque la publicidad es en sí misma una forma de control, es un expediente que permite distinguir lo que es ilícito y de lo que no lo es. (Bobbio; 1986: 71).

En una democracia los derechos individuales pueden ser ejercidos y por tanto, reconocidos; pero también la democracia se amplía y fortalece a través de la ampliación de los derechos ciudadanos. Por el contrario, en una sociedad con un Estado autoritario, en el que se niega la participación de la sociedad, el gobierno se niega a rendir cuentas de su proceder. Con la ampliación de los derechos ciudadanos, la democracia se convierte en un modo de comunicación de las preferencias de los ciudadanos frente al gobierno.

Principios deontológicos de los medios de comunicación

De manera general, la deontología profesional periodística, entendida como el conjunto de normas específicas que regulan la conciencia profesional de un informador, se constriñe a dos principios fundamentales: la responsabilidad social y la veracidad informativa.

Contrario al planteamiento anterior, es común que la deontología atienda cuestiones meramente volitivas, bajo la forma de normas voluntarias de conducta, a las cuales una persona puede o no sujetarse en el ejercicio de su profesión.

Uno de los principales problemas del ejercicio periodístico reside en sus aspectos éticos, por lo que diversos profesionistas en la materia han sugerido la implantación de códigos con el objetivo de regular todo lo relativo a la intimidad, el honor, y cuestiones de carácter personal.

Hugo Aznar advierte que gracias a la función y utilidad de los códigos deontológicos, la sociedad dispone de criterios de exigencia de verdad y credibilidad a periodistas y medios de comunicación.

Sin embargo, existen casos controvertidos en la observancia de los principios deontológicos, principalmente cuando concurren derechos que aluden a la libertad de expresión e información, y generan tensiones con los derechos al honor, a la intimidad y a la propia imagen, aspectos estrechamente ligados a la protección de los datos personales, derechos que son reconocidos como fundamentales, que establece que los datos personales son inalienables, irrenunciables e imprescriptibles. Ante tal situación, los medios de comunicación deben tener como uno de sus principales principios, la protección de los datos personales, esto es, la información estrictamente de carácter personal o familiar, en el ámbito privado o íntimo de las personas.

Dentro de las posturas que señalan los códigos deontológicos relativos a la protección de la intimidad personal, se recomienda evitar las intromisiones ilegítimas a la esfera íntima de las personas, así como salvaguardar el derecho a la propia imagen, es decir, la reproducción total o parcial de una persona en particular.

No obstante, el creciente uso de nuevas tecnologías de la información, como la internet, ha alterado considerablemente los aspectos deontológicos comentados, ya que es común ver en dicho medio información poco confiable en otros casos anónima, alterada y tendenciosa que genera el cuestionamiento de la veracidad de lo aportado por el informante, debido a que no existen normas de control y es muy reciente la incorporación de mecanismos de seguimiento, seguridad y vigilancia de los contenidos.

De manera paulatina, los códigos deontológicos se han adaptado a la problemática, a las necesidades actuales y a los espacios informáticos emergentes. Por ello, diversos medios de comunicación nacionales e internacionales, de manera individual o bien a través de sus asociaciones o redes de periodistas, han plasmado de manera general las directrices a las cuales deben apegarse sus miembros o, en lo general, los periodistas. Dichos códigos éticos abarcan principios como la confianza pública, la verdad, la justicia, la integridad, el respeto, entre otros; pero sólo contienen un breve apartado en el que se recomienda no vulnerar la integridad, seguridad e imagen de las personas, esto es, guardar cautela en la difusión de los datos personales y la esfera de la vida privada. Asimismo, estos códigos deontológicos van acompañados por normatividades específicas que aseguran un debido tratamiento a los derechos que todo periodista debe observar en el ejercicio de su profesión. En el caso del Distrito Federal, la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen constituye un límite al derecho a las libertades de expresión e información, al entrar en pugna con otros bienes jurídicos protegidos como el derecho a la vida, al honor y a la propia imagen. Aunado a lo anterior, ante la creciente necesidad de salvaguardar el derecho a la protección de los datos personales, en nuestro país han comenzado a surgir diversas leyes en la materia,[1] incluida la reciente creación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[1] En el caso de: Colima, Guanajuato, Oaxaca y Distrito Federal.

Medios de comunicación, transparencia y acceso a la información

En los últimos años, han surgido interesantes aportaciones sobre la relación medios de comunicación-opinión pública y la transparencia. En el proceso de transformación política de nuestro país, se ha incorporado en la agenda un tema que parecía lejano al desarrollo democrático nacional: el acceso a la información y la transparencia. Aprendimos a comparar la democracia con una casa de cristal donde el poder es ejercido a la vista de la gente. Es visible y, por tanto, controlable:

> Las instituciones responsables de la transparencia son los medios. En ellos está una función sustancial de la práctica democrática. (Silva-Herzog, 1996).

Sin embargo, aunque los medios de comunicación son considerados un espacio para la discusión pública, un medio de control del poder y un vehículo para el ejercicio del poder político, el ágora de nuestros tiempos (Silva-Herzog, 1996), lo cierto es que en el nuevo contexto democrático, su papel no es claro ni preciso en torno a la protección de datos personales; aún más, como se refirió en párrafos anteriores, ni siquiera es objeto de discusión. Debemos aceptar que esta correcta aseveración está sujeta a una realidad que no vivíamos en el pasado reciente, y que hoy se presenta contradictoria, difusa, incluso inconcebible para los poco enterados. Hoy, como en el pasado, los medios de comunicación son un espacio para la discusión pública.

A los ciudadanos les proporcionan herramientas para formarse una opinión de los asuntos públicos y los aspectos relacionados con el poder político. Actualmente los medios de comunicación ejercen tres funciones básicas:

- Proporcionar información a la sociedad para que pueda fundamentar sus decisiones.
- Constituirse como un espacio abierto donde se exprese con plena libertad la diversidad de ideas y posturas sobre los asuntos públicos.

- Vigilar, publicar y denunciar abusos cometidos por la autoridad.

Con base a estas funciones se puede resumir que el periodismo tiene la tarea de proveer información, expresar diferentes posturas sobre un mismo problema público y vigilar la actuación de quienes ejercen el poder. Para el periodista Raymundo Riva Palacio (2003: 13):

> La única función válida del periodismo es informar, descifrar los códigos de comunicación que no son accesibles a la mayor parte de la sociedad, y darle las herramientas y los conocimientos para poder comprender los hechos y las acciones.

Para cumplir con esta misión, los medios de comunicación gozan de una libertad que no tienen, en general, otros actores sociales. No están por encima de la ley, pero la ley no puede coartar el ejercicio de su función, desnaturalizándola, desviándola o reduciéndola, como lo afirma el jurista Sergio García Ramírez: (2011)

> En su desempeño, los medios deben tomar en cuenta los bienes y derechos que constituyen el límite racional, jurídico y moral para el ejercicio de sus propios derechos. Considerando el enorme impacto que tienen sus informaciones y opiniones, es necesario que ponderen los términos del mensaje, sin que ello constituya, en modo alguno, renuncia a su libertad y a su función social. Por supuesto, están sujetos (como cualquier persona) a la responsabilidad que corresponda por el comportamiento que observen.

En nuestro país las leyes de transparencia y acceso a la información surgen como respuesta a una legitima exigencia ciudadana para que los gobiernos transparenten su actuar y hagan pública la información que está en su poder. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, fue, en gran medida, resultado del papel que jugaron diversos medios de comunicación y figuras individuales del periodismo mexicano.

Gracias al activismo que protagonizó el periodismo, el país hoy cuenta con una Ley en la materia, la cual fue resultado de una discusión entre

periodistas, intelectuales, partidos políticos y asociaciones civiles, y aprobada por consenso entre las distintas fracciones legislativas. En este proceso, los medios de comunicación tuvieron un papel decisivo porque dieron un cuidadoso y permanente seguimiento al tema de la transparencia desde sus orígenes, hasta el diseño de su arquitectura constitucional.

Cuando un periódico en cualquiera de sus formatos, impreso, radiofónico o digital, da a conocer a la opinión pública una noticia sustentada en información solicitada a las instancias gubernamentales, como consecuencia del acceso a la información, la población se ve beneficiada, ya que de este modo, es una de las formas en que la sociedad se entera del buen funcionamiento de la administración pública y sus autoridades. Bajo esta práctica, el periodismo se ha convertido, hoy en día en educador y promotor del derecho de acceso a la información. Ahora bien, el nuevo contexto democrático modifica el papel del periodista; la validez de la información obtenida hoy en día, se sustenta en los documentos solicitados y, por lo tanto, entregados por la propia autoridad como sujeto obligado. En ese sentido, los periodistas demuestran, con información que proviene de la misma autoridad, lo que sucede dentro del gobierno. Así, las leyes de acceso a la información se convierten, para el periodista, en una herramienta útil y estratégica para adquirir información gubernamental.

En la actualidad no podemos entender la acción pública al margen de la comunicación ni la comunicación distanciada de la gestión pública. Desde esta perspectiva, en una sociedad democrática la comunicación gubernamental se convierte en una actividad primordial por dos motivos:

1. El ciudadano está más atento a las grandes decisiones políticas.

2. Los medios de comunicación contribuyen a delimitar el campo del debate público.

Bajo este contexto, esta demanda creciente del derecho a la información es resultado de una mayor consolidación democrática del sistema político. Condición que hace que la comunicación gubernamental se convierta en un instrumento necesario para fortalecer la gobernabilidad y la legitimidad de los gobiernos.

El problema, sin embargo, sigue siendo, qué informar, para qué informar y cómo informar. No se trata pues, de mantener una visión simple y reduccionista de la comunicación a través de los medios de comunicación. Tampoco se puede pensar que por el hecho de vivir en una era de la video-política, la eficiencia de la comunicación política se genera por sí sola.

Comunicación y política son dos conceptos que se vinculan recíprocamente a través de la relación entre gobernantes y gobernados. Por tal motivo, la comunicación política debe asumirse como uno de los instrumentos estratégicos que más contribuyen a mantener la gobernabilidad en contextos democráticos.

Protección de los datos personales en los medios de comunicación

Hasta aquí se ha tratado de hacer un breve recuento sobre la transformación de la relación de los medios de comunicación con el Estado mexicano en diferentes contextos políticos, a través de la transición de un régimen autoritario-corporativista a un país que hoy tiene a la democracia como su forma de gobierno.

Pero nos enfrentamos a un dilema: en medio del nuevo contexto democrático y de la ampliación de derechos ciudadanos como el de acceso a la información, los medios de comunicación en nuestro país, no han definido hasta ahora los mecanismos de relación con el Estado mexicano en temas específicos como la protección de datos personales ni se han ocupado de revisar cuál es o debe ser su postura para que no se viole el derecho a la privacidad. Tampoco hay rastros de la existencia de códigos de ética periodística vinculados de manera detallada a este derecho ciudadano; quizá apenas se dediquen algunos escuetos párrafos para hacer referencia a la privacidad. Atentos a lo anterior, se debe reconocer que hay dos derechos fundamentales que tienen su propia razón de ser, que es necesario definir con precisión sus fronteras ya que podrían concebirse con naturaleza contradictoria u opuesta. Uno de ellos es el derecho a la privacidad. El otro, la libertad de expresión. En opinión de Sergio García Ramírez, por lo que toca a datos personales, es indispensable tomar en cuenta que la sociedad tiene el derecho a saber, y los medios tienen el derecho y la obligación

de informar todo aquello que revista importancia para la sociedad y sus integrantes; en virtud de que contribuyen a formar opinión sobre asuntos de interés público y guiar la conducta de los miembros de la sociedad sobre bases ciertas y firmes. Empero, estos derechos y obligaciones se concretan al deber de informar sobre cuestiones de importancia para la sociedad, en el marco de la democracia. Esto no incluye cuestiones de carácter estrictamente personal que sólo atañen al interesado, cuya difusión innecesaria no genera bien alguno para la vida colectiva, produciendo en cambio, daño injusto a la persona sometida a un escrutinio innecesario y perjudicial. Por eso, García Ramírez concluye "nuevamente hay que tomar en cuenta los límites para el ejercicio de la libertad (que aparecen en los tratados de derechos humanos) y responder, en su caso, por los daños que se causen".

Importancia de las estrategias de comunicación social en el sector público en materia de protección de datos personales

Ante la ausencia de políticas específicas en el sector público que permitan establecer estrategias para proteger el derecho a la privacidad, resulta necesaria una adecuada interacción de las áreas de comunicación social del gobierno con los medios de comunicación.

Para acotar esta base, nos limitaremos en este estudio a uno de los principales depositarios de información personal: los órganos encargados de impartir justicia en México. Las Procuradurías Generales de Justicia de los diversos estados de la República, en el ejercicio de sus facultades, recaban datos confidenciales de los indiciados, entre ellos su nombre, alias o apodos, domicilio, señas particulares, su imagen mediante fotografías, entre otros.

Definitivamente, cuentan con una gran cantidad de información que identifica puntualmente a una persona que ha cometido algún delito o se encuentra en un proceso para determinar su debida responsabilidad. No es de extrañar que diariamente, en periódicos, noticieros y otros medios de comunicación, nombres e imágenes de personas que han cometido delitos de diferente naturaleza, o son acusados o señalados como presuntos culpables. Asimismo, las autoridades competentes hacen pública la imagen de los detenidos.

La Procuraduría General de Justicia del estado de Puebla ha reconocido, en su respuesta a una solicitud de información que hacer públicas imágenes, fotografías, videos o cualquier tipo de reproducción de la imagen de los presuntos responsables, resulta un mecanismo de vinculación con la sociedad para fortalecer la cultura de la denuncia, ya que en diversas ocasiones, esto ha permitido que las víctimas reconozcan plenamente a los indiciados y lo manifiesten ante la autoridad investigadora.[2]

Existen casos en los que es de suma relevancia sin prejuzgar la responsabilidad del detenido hacer del conocimiento público dicha detención, para que la persona o las personas sean identificadas por la población en la eventualidad de que haya cometido otros delitos. De este modo se busca robustecer las indagatorias correspondientes cuando la conducta del detenido sea de alto impacto social, para darlo a conocer a la sociedad. El tratamiento de este tipo de acciones es diferente en el Distrito Federal. A fin de no vulnerar derechos fundamentales, la Procuraduría General de Justicia del DF ha emitido lineamientos específicos para la presentación de presuntos responsables ante los medios de comunicación los que destacan que dicha presentación deberá limitarse a informar únicamente sus datos generales, el delito y circunstancias por las cuales se llevó a cabo la detención y las consideraciones o trascendencia social para su presentación ante los medios, así como atender cuestionamientos realizados por los periodistas, que se consideren procedentes.[3]

Asimismo, en caso que sea necesaria la presentación en forma conjunta con los objetos o instrumentos relacionados con los delitos objeto de investigación, se evitará que los presuntos responsables porten o sostengan dichos objetos. Este tipo de disposiciones no es común en otros estados de la República, por lo que es común ver a presuntos delincuentes sosteniendo armas, drogas, y otros objetos. Derivado de que a nivel nacional no existe un documento rector del manejo de los acontecimientos que suceden en el país en materia de seguridad pública, en el año 2011, se firmó el "Acuerdo para la Cobertura Informativa de la Violencia", suscrito por más de 700 medios

[2] INFOMEX PUEBLA, solicitud de información con número de folio 00387211.

[3] Acuerdo A/004/2005, Gaceta Oficial del Distrito Federal, 12 de septiembre de 2005.

de comunicación de todo el país, que pretende, entre otros objetivos, proponer criterios editoriales comunes para la cobertura informativa de la violencia generada por la delincuencia organizada, asunto relevante por lo que compete en torno al manejo de la información que los medios de comunicación, bajo el supuesto de que los involucrados son inocentes en tanto no cuenten con una sentencia condenatoria o estén confesos. Por otra parte, los medios deben respetar los derechos de las víctimas y menores de edad involucrados; sobre todo, no aportar información que ponga en riesgo la identidad de las víctimas.

Regulación de la protección de los datos personales en los medios de comunicación

Otra asignatura pendiente que debe atenderse a la mayor brevedad, es la relacionada con la necesidad de normar protección de los datos personales en los medios de comunicación. En principio el tema es polémico, controvertido y lleno de confusión. El problema de la ética en la tarea informativa, por poner un ejemplo central del debate, es que aún no está resuelto. Cada día aparecen nuevos asuntos que carecen de procedimientos o normas que guíen la labor periodística, mientras que los mismos diarios informativos tienen una diversidad de posturas algunas de ellas contradictorias entre lo que unos consideran qué debe contener un código de ética, en tanto que otros difieren.

¿Cuáles son los límites de lo privado para los medios de comunicación, y cuándo consideran que los datos son de "orden público" para que sean publicables? Este es un asunto lleno de contradicciones que los propios medios no han podido aclarar.

En el centro del debate está la necesidad de establecer valores éticos por encima de los económicos por parte de los medios, que señalen los límites de la difusión de los datos personales. Como señala Mauricio Merino:

> La ética pública propone límites y barreras morales, ofrece definiciones para reconocer y situar lo que ha dejado de ser público; propone valores para hacer posible la convivencia de los distintos y hasta de los opuestos, sin vulnerar su personalidad propia. (2010:22).

La UNESCO, por su parte, establece que:

> Una parte fundamental de los valores profesionales del periodista es el respeto al derecho del individuo a la intimidad y a la dignidad humana, en conformidad a las disposiciones del derecho internacional y nacional, referente a la protección de los derechos y la reputación de las personas, prohibiendo la difamación, la calumnia, la tergiversación y la injuria.

Ahora bien, la complejidad del problema a resolver, conduce necesariamente a otro debate que ha llamado la atención de diversos investigadores sociales: la relación entre lo público y privado, que ayude a distinguir los límites éticos de los medios de comunicación. Nora Rabotinikof (2010: 45-46) establece tres criterios para diferenciar un espacio del otro:

1. Lo público como lo que es de interés o de utilidad común a todos, lo que atañe al colectivo, lo que concierne a la comunidad y, por ende, a la autoridad de allí emanada, en contraposición a lo privado, entendido como aquello que se refiere a la utilidad y el interés individual (...).

2. Lo que es y se desarrolla a la luz del día, lo manifiesto y ostensible en contraposición a aquello que es secreto, preservado, oculto (...).

3. Lo que es de uso común, accesible para todos, abierto, en contraposición a lo cerrado, que se sustrae a la disposición de los otros.

Por otra parte, la privacidad se define como..."aquella parte de la vida humana que se desarrolla a la vista de pocos o que constituye la vida personal y particular" (Novoa, 2001:31). Como se puede apreciar, el problema de constituir códigos de ética en torno al derecho a la privacidad en los medios, no es sencillo. Sin embargo, son dos los principales elementos que determinarán en el futuro inmediato la regulación de los datos personales en los medios de comunicación: por un lado, la legislación en la materia; la cual debe concretarse junto con los códigos y reglamentos que de ella se deriven. Es a través de

la ley que quedarán determinados esos límites. No obstante; el tema no queda ahí, se tendrá que ampliar la jurisprudencia, ya que se pronostica que en el mediano y largo plazo, se susciten controversias al respecto. Por otro lado, será necesariamente, la creación de códigos de ética de los medios que les permita seguir haciendo uso del derecho a la libertad de prensa y de expresión, y al mismo tiempo respetar el derecho a la privacidad de los ciudadanos.

La tarea, desde luego, no es sencilla. Las experiencias en países de Europa nos muestran que, a pesar de los años que llevan debatiendo sobre este tema, no se han podido generar consensos. La diversidad de posiciones y la pluralidad que existe en el mundo periodístico, también limita la posibilidad de que se tenga claridad sobre estas fronteras entre lo público y lo privado.

Retos y perspectivas

El camino para México no sólo es largo, sino además difícil. Ya se dio el primer paso y quizá el más importante. Contar con marcos normativos que regulen la protección de los datos personales tanto en posesión del gobierno como de particulares y con instancias que vigilen el uso y manejo de los mismos es fundamental. El esfuerzo realizado por los órganos garantes es digno de reconocer. Existe, sin embargo, un enorme desconocimiento general sobre los derechos de la privacidad por parte de la población, por ser un tema nuevo. El siguiente paso es impulsar campañas para difundir y fomentar la protección de los datos personales a nivel nacional, en escuelas, universidades y oficinas de gobierno. Paralelamente es necesario crear sinergias con los diferentes niveles de gobierno y los organismos garantes de las entidades federativas, para formar y capacitar a los funcionarios públicos que tienen asignada su labor a las actividades de transparencia y acceso a la información. Y finalmente los medios de comunicación tienen el reto de asumir un papel protagónico, al igual que lo han hecho en otros procesos de gran trascendencia para el país, para generar una cultura de respeto al derecho a la privacidad.

Asimismo, resulta trascendental que las autoridades competentes y los institutos de transparencia y protección de datos impulsen, en conjunto con los medios de comunicación y las áreas de comunicación

social de los gobiernos, un modelo único relativo al tratamiento de los datos personales, que sirva de base en las redacciones y áreas de producción de noticias, que permita establecer reglas mínimas en el uso y tratamiento de este tipo de información sensible.

Sin duda, el camino es largo, la sociedad espera mantener lejos de las miradas ajenas su espacio personal.

Referencias

Autores varios (1998) *Homenaje a Rafael Segovia*, El Colegio de México/FCE,

Bobbio, Norberto (1986) *El futuro de la democracia*, FCE.

Castells, Manuel y otros (2006) *La Nueva Comunicación*, Le Monde Diplomatique.

Izurieta, Roberto y otros (2001) *Estrategias de comunicación para gobiernos*, editorial F.B.T.

Loaeza, Soledad y Prud´homme, coor. (2010) *Instituciones y procesos políticos*. El Colegio de México.

Martínez, Omar, comp. (2003) *Esencia del periodismo*. Fundación Manuel Buendía,.

Merino, Mauricio (2010) *Ética Pública*, editorial siglo XXI,

Novoa Monreal, Eduardo (2001) *El derecho a la vida privada y libertad de la información: un conflicto de derechos*. 6ª ed. México, Ed. Siglo XXI.

Riva Palacio, Raymundo (1998) *Más allá de los límites*, Universidad Iberoamericana.

Silva-Herzog Márquez, Jesús J (1996). *Esferas de la democracia*. Cuadernos de Divulgación de la Cultura Democrática. Instituto Federal Electoral.

Toledo, Francisco y Florescano, Enrique, coor. (2006) *Los desafíos del presente mexicano*. Taurus.

Políticas públicas para proteger los datos personales de los menores en internet y redes sociales

Miroslava Carrillo Martínez

Miroslava Carrillo Martínez

Comisionada del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

Ha sido docente de asignatura en la Facultad de Derecho de la Universidad Autónoma del Estado de México, en las materias de Derecho Constitucional I, Derecho Políticos y en la Facultad de Ciencias Políticas y Sociales de Derecho de la Información, así como Secretaria Técnica de la Junta de Coordinación Política de la LV y LVI Legislatura.

Es Licenciada en Derecho por la Universidad Autónoma del Estado de México; tiene estudios de Maestría en Derecho y una especialización.

Introducción

Con la visión de plantear problemas y sus alternativas de solución, este artículo traza como objetivo central, la exposición de algunas reflexiones alrededor de los riesgos inminentes que enfrentan los menores de edad y sus datos personales, en el uso de las distintas herramientas que ofrecen las nuevas tecnologías de la información y comunicación (TIC), en el desarrollo de las denominadas *sociedades de la información*. A partir de ello, es importante desmenuzar la serie de implicaciones y problemáticas, con énfasis en la protección de los datos personales, para plantear algunas propuestas para prevenir, educar y sentar las bases de una cultura de la protección de los datos personales de los menores de edad.

Este artículo comienza por definir los derechos humanos de cuarta generación; expone el marco conceptual del Estado constitucional democrático, de acuerdo con diversos doctrinarios en la materia; para, posteriormente, establecer el marco jurídico específico y vigente de la protección de los datos personales, desde una visión internacional hasta el ámbito del Estado de México. Por otro lado, analiza el derecho informático comparado y su vinculación con la sociedad tecnológica, para, finalmente, precisar la necesidad de implementar políticas públicas encaminadas a la prevención y orientación a los menores, padres de familia y docentes.

Derechos humanos de cuarta generación

Las violaciones a los derechos humanos en los diversos ámbitos de la vida tienen distintos orígenes. Para analizar, de manera integral, el fenómeno de la violación de los datos personales, es necesario realizar un estudio desde las diferentes implicaciones que conlleva este fenómeno. Una de ellas radica en el uso de las TIC, cuyo empleo ha crecido vertiginosamente, lo que ha derivado en el mal uso de los datos –por ejemplo, el nombre y los apellidos, la fotografía, el domicilio, la dirección de correo electrónico, los números de teléfono celular y fijo y los números de cuentas bancarias– que son propiedad "personal" de quienes los acumulan, principalmente con fines comerciales. Hay organismos que, debido a sus actividades institucionales públicas,

concentran grandes cantidades de datos personales –como alguna oficina gubernamental recaudadora de impuestos– y también existen instituciones privadas –como los bancos– que, por su naturaleza, deben manejar datos personales. Esto también ocurre con los datos personales de los menores de edad; sin embargo, en sí misma, la concentración de datos no supone un problema. En cambio, los riesgos se presentan cuando existe la intervención de quienes, en un ámbito distinto –como el Internet y las redes sociales–, llevan a cabo una serie de actos indebidos, como la acumulación y el uso indebido de los datos personales con propósitos delictivos. El fenómeno se torna más complejo cuando se trata del trasiego de los datos de los menores de edad; sobre todo, por el desconocimiento de este grupo sobre el empleo de las tecnologías mencionadas y por la información que proporcionan de manera inconsciente.

Por otra parte, la cultura de los derechos humanos, (Ornelas, 2010:155)[1] ha generado las aportaciones científicas correspondientes, dirigidas a garantizar su pleno respeto. Para ello, algunos estudiosos citados por Aristeo García González[2] han clasificado a los derechos humanos en generaciones, las cuales reflejan el crecimiento de sociedades como la nuestra, con el fin de fortalecer, con base en el conocimiento, el respeto de los derechos de las demás personas, independientemente de la relación humana en que se verifique la interacción. Haciendo un recorrido por la evolución de los derechos humanos, los de primera generación corresponden al reconocimiento de los derechos civiles y políticos, en la época de la Revolución Francesa, desencadenada por el propio pueblo galo. En dicho periodo, se defendían los principios de libertad, igualdad y fraternidad, con el objetivo de equilibrar las relaciones entre la sociedad y el Estado.

Así, sus características se definen como imprescriptibles, inajenables, intrasmisibles, irrenunciables y gozan de protección jurídica.

[1] Ornelas, Lina. E*l derecho de las niñas, niños y adolescentes a la protección de derechos y su exigencia frente a las redes sociales. Protección de datos personales*. Compendio de lecturas y legislación. IFAI, ITAM, 2010.

[2] García González Aristeo. "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *en Boletín mexicano de derecho comparado*, núm. 120, consultado el 26 de octubre de 2011 en www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm.

Después de un lapso evolutivo social, marcado por la Revolución Industrial –en la que, nuevamente, tienen presencia los desequilibrios sociales provocados por este hecho histórico, protagonizados por los obreros, campesinos e intelectuales–, los doctrinarios reconocen los derechos humanos de segunda generación, basados en los principios de justicia social y bienestar común, destinados a la obtención de satisfacciones mínimas en la prestación de servicios. Es decir, en esta etapa de la historia, se luchó por el reconocimiento de los derechos económicos, sociales y culturales.

Posteriormente, a mediados del siglo pasado, el surgimiento de dos bloques de países durante la Guerra Fría provocó desigualdad, pobreza y marginación, que aún persisten en muchas naciones –entre ellas, la nuestra–. Este es el origen de los derechos humanos de tercera generación,[3] que incluyen temas como la solidaridad internacional, la protección del medio ambiente, el reclamo de la autodeterminación y el desarrollo digno de los pueblos indígenas y de los países tercermundistas.[4]

Con una nueva etapa en la evolución histórica de la humanidad, se han integrado los derechos humanos de cuarta generación, cuya defensa ha recaído en las diversas clases sociales de la mayoría de los países del mundo. Éstos se refieren a los derechos con oportunidades de autogestión social, participación ciudadana en pro de una mayor transparencia social.

Finalmente, los estudiosos de los derechos humanos han considerado una cuarta generación, la cual se distingue por la proliferación de nuevas formas de relaciones humanas, a través de las TIC. Éstas deben integrar una sólida cultura axiológica –nombrada también *ciberderechos*–, para salvaguardar la información que constituye a las nuevas sociedades del conocimiento.

[3] En la página electrónica www.derechoshumanos.org.mx, consultada el 16 de noviembre de 2011, se encuentra una gama de aportaciones a los derechos humanos, la cual se ha fortalecido continuamente por las investigaciones jurídicas de diversas instituciones.

[4] Las constituciones son los instrumentos legales sustantivos en los cuales se establecen los derechos y las garantías de los ciudadanos que conforman un país. Este tipo de documento nace en varios países europeos, que adoptaron la forma de gobierno que se originó en Francia en 1789.

La interacción de los menores de edad con las tecnologías mencionadas implica una serie de riesgos que, muchas más veces, ellos mismos ignoran. Esta es la base para que, de manera fácil y rápida, envíen sus datos personales a gente que no conocen, con lo que se exponen a ser vulnerados o dañados, en aspectos físicos, morales y económicos, pues existen tantas conductas delictivas como imaginación dañina en quienes, desde la delincuencia, se dedican al acoso, al robo de infantes, a la prostitución infantil, a la trata de blancas, al tráfico de órganos y a los ataques a la moral, entre otras conductas delictivas que han encontrado, en las TIC, los recursos sustantivos para su ejecución.[5]

Esto implica, entonces, una responsabilidad social, gubernamental, institucional, legal y jurídica; sobre todo, porque las nuevas generaciones acceden a Internet de forma ilimitada y, lo que es peor, sin la supervisión de quienes ejercen su patria potestad o su tutela. Esto constituye el origen de los derechos humanos de la cuarta generación, los cuales deben ser protegidos desde la ley y la sociedad, con el fortalecimiento de la cultura de la legalidad y el respeto. Además, deben prevenir y sancionar las conductas delictivas, con la finalidad de propiciar el desarrollo sano, justo y armonioso de la colectividad.

Desde esta perspectiva, los derechos humanos comenzaron a reconocerse en los grupos normativos fundamentales[6] de los países europeos, dada la importancia que revisten para los seres humanos, como objeto de la existencia del Estado constitucional y democrático.[7]

---

[5] En este sentido, no ha sido suficiente la existencia de las policías cibernéticas, que investigan la comisión de estos delitos, aunque siempre tendrá doble valor la implementación de acciones preventivas que correctivas. Esta división de la policía Federal Preventiva recibe denuncias a través de la aplicación de Denuncia Ciudadana, en www.icesi.org.mx/consejos/seguridad_queDondeDenunciar.asp, consultada el 17 de noviembre de 2011.

[6] En el artículo *El derecho a la intimidad, al honor y a la propia imagen*, Cuauhtémoc Manuel de Dienheim Barriguete señala: dentro de la esfera de la vida privada, podemos considerar las relaciones personales y familiares, afectivas y de filiación; las creencias y preferencias religiosas; las convicciones personales e inclinaciones políticas; las condiciones de salud, identidad y personalidad psicológica; las inclinaciones sexuales; las comunicaciones personales privadas por cualquier medio. Incluso, algunos incluyen la situación financiera personal y familiar. La necesidad de intimidad es inherente a la persona humana y al respeto a su vida privada. Mantener alejadas las injerencias no deseables y las indiscreciones abusivas permitirá que la personalidad del hombre se desarrolle libremente. De esta forma de protección a la vida privada, se constituye un criterio de carácter democrático de toda sociedad.

[7] "la dignidad de la persona adquiere toda su potencialidad no abstencionista, sino promotora

Además, su cultura genera relaciones humanas equilibradas, las cuales impulsan a la sociedad hacia un círculo virtuoso, cuya base también se encuentra en la práctica de valores morales en todos los ámbitos de la vida; es decir, en el ámbito personal –también llamado derecho a la intimidad[8] y a la dignidad–[9] y en su interacción con los demás.

Esto, sin duda, proporcionaría a cualquier colectividad las herramientas mínimas indispensables para apoyar su crecimiento y desarrollo. Por lo tanto, el respeto de los derechos humanos propicia el desarrollo social.

Por otra parte, en las últimas décadas, se han fortalecido las relaciones humanas a través de las nuevas TIC, que se basan en la existencia de un mundo virtual, que involucra el ejercicio de valores propios de la dignidad humana, cuyo respeto, por parte de las instituciones públicas y privadas, supone la necesidad urgente de educar sobre el uso de las redes sociales. En la *cibersociedad*, es conocida la comisión de delitos informáticos, que implica un gran reto para el Estado constitucional y democrático, ya que para prevenir y

de la persona humana; en la cual se busca ya no limitar y controlar al Estado y a la sociedad; sino, por el contrario, fomentar o crear las condiciones jurídicas, políticas, sociales, económicas y culturales que permitan el desarrollo de la persona humana en dignidad. La dignidad está vinculada directamente a los derechos fundamentales; buscando integrarla y ponderarla con los diversos bienes jurídicos tutelados por la Constitución. Es precisamente en esta relación entre la dignidad y los derechos fundamentales donde se presentan una serie de viejos dilemas con relación al derecho a la vida, y de novísimos desafíos provenientes del derecho genético, frente a los cuales el derecho constitucional no puede estar atrás de los acontecimientos científicos, tecnológicos y sociales, pero tampoco puede adelantarse imprudentemente a éstos".

[8] Los preceptos de la razón sólo pueden guiar las intenciones individuales a la luz de conceptos de justicia, equidad, compasión y tolerancia, entre otros. Como normas morales, nos obligan in foro interno, pero cosa muy distinta es que tengan lugar y se hagan valer *in foro externo*. Tal como Hobbes hace ver, esos preceptos, por sí mismos, no tienen poder para operar socialmente si no hay instituciones que los hagan respetar. Las sociedades humanas, que se debaten entre la barbarie y la civilización, tienen ante sí la tarea de apelar al poder de la razón, a este llamado derecho natural, para instaurar, de común acuerdo, la legitimidad de un poder político capaz de asegurar la paz y garantizar la justicia para todos. Este concepto de poder político, como representación de las necesidades e intereses de todos, dará lugar a lo que, más tarde, el demócrata y republicano Weber llamará un Estado constitucional de derecho.

[9] En suma, a través del Estado Constitucional, se pretende, simplemente, poner de manifiesto qué rasgos han venido definiendo al Estado Constitucional hasta su actual concepción, que hemos tratado de abordar a través del estudio del proceso de configuración del Estado constitucional, de la Teoría de la Constitución, del Estado constitucional como garante de derechos y libertades, del Estado constitucional y la Teoría de las formas políticas y del Estado constitucional como democracia representativa y de relaciones entre el gobierno y el Parlamento, en los sistemas parlamentarios.

sancionar este tipo de conductas, debe implementar políticas públicas generales y específicas, encaminadas a atender las necesidades de justicia y de equilibrio de la sociedad. El *ciberespacio,* como nuevo universo para comunicarse, desarrollarse, trabajar, crear, pensar y, en definitiva, vivir, no puede quedar ajeno a las políticas públicas. La humanidad se encuentra en un nuevo periodo, inédito en su historia: la era de la información. Actualmente, la tecnología se inserta en todos los contextos y no deja dimensión humana indiferente; por lo tanto, las posibilidades de comisión de delitos informáticos son elevadas. Basta oprimir una tecla para transgredir los derechos de los demás.

Por estas razones, es imperativo que el Estado se coloque a la vanguardia de los avances tecnológicos, para prevenir y sancionar las conductas que vulneran los derechos humanos y, específicamente, el derecho a la protección de los datos personales. Resulta importante enfatizar la estructura y emisión de normas que protejan a los menores, con políticas públicas eficaces, entre las que se incluyan campañas de uso responsable de datos personales, fortalecer los marcos jurídicos necesarios y las instituciones garantes integrales, desde el punto de vista de recursos humanos, materiales y económicos. Abatir el fenómeno delictivo de la pornografía infantil, el *sexting*, el acoso cibernético y el tráfico de datos supone implementar medidas de seguridad con esquemas multidisciplinarios educativos y preventivos.

Marco conceptual del Estado constitucional y democrático

El Estado constitucional[10] es un concepto doctrinario construido en el área del conocimiento del derecho constitucional e integrado, entre otras perspectivas, por el Estado que, con base en su constitución política, reconoce y organiza la vida política, social y económica de un país. Desde estas consideraciones, implica poner en práctica un conjunto de políticas públicas que contemplen la atención a los fenómenos surgidos por la interacción social, como la protección

[10] De acuerdo con Antonia Navas Castillo y Florentina Navas Castillo en *Esquemas de derecho constitucional y programa*, el papel del Estado es el resultado del involucramiento de las instituciones que van surgiendo en el curso de los procesos de resolución de las cuestiones socialmente problematizadas, exista o no consenso en que sea el Estado nacional quien deba resolverlas, 2007.

de datos personales, que protejan los derechos de las personas, en relación con el empleo de las TIC, el propio Estado y la iniciativa privada.

Entonces, el fenómeno se presenta cuando existen desequilibrios en el manejo de los datos o, peor aún, cuando con la manipulación de la información se efectúa con propósitos delictivos.

En estas situaciones, el Estado constitucional debe diagnosticar, para prevenir las conductas lesivas, y para sancionar los actos que violenten la dignidad o la intimidad del ser humano.[11] El espíritu de las acciones que marcan la evolución del Estado constitucional y democrático radica, en síntesis, en limitar su poder en relación con los seres humanos a los que sirve. De esta manera, se predetermina un equilibrio entre las instituciones públicas y la sociedad, como un punto de convergencia con el sentido de la justicia, para el cual se establecen las normas jurídicas que apoyan al Estado y su forma de gobierno.

Otra característica que representa al Estado constitucional, según Ferrajoli, es que se identifica como un Estado garante,[12] cuya facultad se ejerce con el establecimiento de las normas, a través de los cuerpos especializados para emitirlas. Esta dinámica da origen a las instituciones –también llamadas garantes–, cuya misión consiste en salvaguardar una o varias garantías constitucionales, como parte de su función social sustantiva, que cobra efectividad a partir de la petición de defensa motivada por la violación de una garantía constitucional o un derecho humano, entre los que se engloba la protección de datos personales.

De igual modo, el Estado democrático[13] puede concebirse filosóficamente, a través de conceptos esenciales y formales. Estos

[11] Esto significa que el pleno respeto a la dignidad de los seres humanos implica, también, proporcionar todos los medios para que éstos se desarrollen plenamente como tal, en lo individual y en su vida colectiva.

[12] Lo cual está representado no sólo por las leyes especializadas, sino por las instituciones que también reciben el nombre de garantes, cuya misión es salvaguardar o proteger los derechos humanos y las garantías individuales en contra de los posibles actos del Estado mismo.

[13] Este Estado se describe como aquél que privilegia la participación de los ciudadanos en todas las acciones de gobierno; a diferencia del Estado constitucional, que enfoca más su atención a la estructura de la propia Constitución.

elementos, propuestos por Bobbio (1986:84), aluden a la democracia, la cual se define por el conjunto de reglas que permiten, al mayor número de personas de un país, participar en la toma de decisiones colectivas vinculantes. Estas líneas normativas señalan quién y cómo determina el destino de la sociedad, así como los mecanismos para legitimar estas decisiones. Así, Bobbio[14] destaca la *regla del sufragio universal*, la *regla de la igualdad,* la *regla de la libertad,* la *regla del pluralismo,* la *regla del consenso* y la *regla del disenso.* De acuerdo con estos postulados, si estas reglas no se verifican, no hay ámbitos democráticos, lo que implica que tampoco hay equilibrios entre los distintos aspectos de un Estado democrático.

Estado del arte en la protección de datos de menores

Marco jurídico específico y vigente de la protección de datos

De acuerdo con el panorama trazado hasta el momento, el derecho de acceso a la información, en general, ha tenido una notable evolución en nuestro país, a partir de la reforma del artículo 6 de la Constitución Federal, en 1977. Sin embargo, la ley normativa secundaria fue expedida mucho tiempo después, en la que se contempla el derecho a la protección de datos personales.

A pesar de lo anterior, y a decir de algunos estudiosos del derecho, el concepto más utilizado por la dogmática jurídica, en el tratamiento del derecho a la privacidad y la intimidad,[15] alude más a la idea de la libertad negativa; concepto tomado por la influencia del pensamiento liberal. Sin embargo, no presenta criterios claros ni medidas consistentes sobre los límites de la libertad de cada uno y, consecuentemente, sobre

[14] La transcripción de estas reglas pertenece a Norberto Bobbio (1986:84), "¿Qué alternativas a la democracia representativa?", en *¿Qué socialismo?*, Barcelona, Plaza y Janés, trad. J. Moreno Plaza.

[15] De acuerdo con Ernesto Villanueva (2003: 233) Quito, CIESPAL, el derecho a la intimidad es "el derecho fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que, legítimamente, deciden mantener fuera del conocimiento público".

las fronteras mínimas de la privacidad que deben garantizarse a cada individuo. De ahí surge la propuesta de utilizar criterios pragmáticos –y no ideales– para la medición de la privacidad, a partir de las reglas del juicio social acerca de la definición del límite provisorio, adecuado y reflexivo, de la medida de lo público y lo privado. Así, entonces, es posible establecer un sistema de regulación de la información en el mercado y sus efectos, que consideren el derecho a la privacidad (Porto, 2002).

De este modo, la privacidad sufre hoy embates provenientes de diferentes ámbitos; en especial, alrededor de la protección de los datos personales, que incluyen, también, los datos sensibles.[16] Por esta razón, impera la necesidad de salvaguardar estos derechos, constituidos como la protección a la vida privada, en contraposición con la vida pública, lo que requiere establecer límites y discernir entre los conflictos individuales y el derecho a la privacidad, en relación con los datos sensibles.

En este contexto, la necesidad de implementar políticas públicas en torno a la protección de los datos personales en general, resulta impostergable, puesto que, en un mundo globalizado, el derecho no puede quedar rezagado ante los adelantos tecnológicos que conforman el Internet y las redes sociales y que, incluso, han conducido, como señala Benkler (2003 y 2006), a la consideración de ecosistemas digitales,[17] formados por especies como aplicaciones informáticas, sistemas operativos, protocolos de comunicación, servicios en línea y modelos de negocios, que se vinculan a través de relaciones simbióticas, de mutuo refuerzo o mutua dependencia.

[16] Los datos sensibles responden a una denominación empleada preferentemente en el ámbito del derecho jurídico, que tiene que ver con la información que afecta lo más propio de una persona; es decir, su intimidad. Así, son todos aquéllos que identifican o permiten la identificación de una persona y pueden servir para la confección de su perfil ideológico, racial, sexual, económico, de salud o de cualquier otra índole que, revelado en ciertas circunstancias, puede constituir una amenaza. Estos datos sólo pueden ser revelados por la persona y no se descubren con sólo mirarla o hablar con ella o de ella; pueden ser adivinados o intuidos por un espíritu muy sagaz; pueden sospecharse por determinados indicios o señales, pero la única certeza sobre ellos proviene de su revelación por parte de la persona. Entre éstos, se encuentran las referencias a la información genética de cada individuo, que comprende la parte más íntima de cada ser humano.

[17] Un ecosistema digital se define como una estructura digital autorganizada, orientada a la creación de un entorno digital distribuido en red y caracterizada por numerosos elementos: conocimiento compartido; tecnologías, estándares y protocolos abiertos; cooperación solidaria y nuevos modelos de negocios.

Ante esta realidad, es posible distinguir entre relaciones positivas, encaminadas a la colaboración y al beneficio mutuo, y relaciones negativas, similares a la depredación y al parasitismo. Estos vínculos desempeñan un papel fundamental en la creación de nuevas especies digitales y en la extinción de aquéllas que se quedan obsoletas, pues no siguen las reglas de selección natural dictadas por el mercado. En este entorno, continúan surgiendo especies digitales que desplazan el centro del poder y lo conducen a la periferia del sistema, de vuelta al individuo, que implican una interacción entre derechos intermedios y *metaderechos*; el poder comunicacional como *biopoder* y el conocimiento libre, entre otros aspectos de gran importancia, como el comercio digital.

En consecuencia, las nuevas tecnologías en la vida cotidiana generan la necesidad de garantizar, cada vez más, la intimidad y la privacidad, ante una innumerable cantidad de violaciones a dichos derechos, que se producen por la falta de una protección precisa. En este sentido, algunos países, como Argentina,[18] han destacado como un modelo en materia de normatividad para la protección de datos personales, primordialmente por la expedición del *H*ábeas Data,[19] que ha sido elevada a rango constitucional, como vía de amparo destinada a asegurar la vigencia efectiva del derecho a la privacidad, frente al abuso del tratamiento automatizado de la información nominativa. No obstante, los derechos tutelados –como la privacidad, la intimidad y el honor– y los tipos existentes de *Habeas Data* –como informativo

[18] Bernigaud, Jorge Rafael. Hábeas Data. Derecho Constitucional II. 2003 .Consultada el 11 de octubre de 2011 en www.terrileyasociados.com/estudio/derecho/HABEAS%20DATA.doc.

[19] El nombre de Hábeas Data proviene del antiguo instituto Hábeas Corpus. Hábeas, del latín, significa "conserva o guarda" y Data, del inglés, "información o datos". Literalmente, expresa "conserva o guarda tus datos". Esta denominación, mitad latina, mitad inglesa, apareció por primera vez en 1988, en la Constitución de Brasil. Según una definición más técnica (Ekmekdjian-Pizzolo,1996), es la garantía que permite a toda persona, determinada o determinable, a solicitar judicialmente la exhibición de los registros, bancos de datos y archivos que incluyan sus datos personales o de su grupo familiar, para conocer su exactitud, requerir su rectificación y demandar la supresión de datos inexactos, obsoletos o que impliquen discriminación. El Hábeas Data es una herramienta a partir de la cual es posible remover un obstáculo que impide el goce de un derecho reconocido o reponer ese derecho, en caso de que haya sido violado. La garantía, por excelencia, es el amparo, pero, en la legislación argentina, coexisten otras garantías, como el Hábeas Corpus y el derecho de réplica. El Hábeas Data no tiene una larga trayectoria en la legislación mundial, pues ha empezado a incorporarse en las legislaciones desde hace solamente tres décadas. Parte de la doctrina lo incluye como una subespecie del amparo (Sagües), como lo han ratificado algunos ministros de la Corte; sin embargo, otra parte de la doctrina y la jurisprudencia (Petracci), lo considera como un instituto independiente del amparo, con una amplia clasificación.

o cancelatorio– han provocado una confusión conceptual respecto a la naturaleza de la institución, bien como un derecho autónomo, de autodeterminación informativa, garantía o proceso; bien como amparo especializado para los datos personales sensibles.

Sin embargo, es necesario reflexionar aún más sobre el derecho a la protección de los datos personales, a partir de los problemas que plantea el mundo globalizado. Por tal motivo, el uso y control sobre los datos de cada persona debe ser reconocido ya no sólo como una mera prerrogativa, sino, además, como un derecho fundamental, protegido y garantizado por mecanismos idóneos.

El tratadista Ferrajoli (2008) distingue las garantías primarias de las secundarias, así como la teoría de derechos fundamentales, que consisten en las expectativas positivas o negativas, a las cuales corresponden obligaciones (de prestación) o prohibiciones (de lesión). En razón a estas consideraciones, las garantías primarias se identifican con las obligaciones y prohibiciones, mientras que las garantías secundarias radican en las obligaciones de reparar o sancionar las lesiones contra los derechos o las garantías primarias.

Efectuadas estas observaciones, es necesario acotar que, en nuestro país, la garantía primaria en materia de protección de los datos personales se encuentra plasmada en los artículos 6 y 16 de la Constitución Federal, en tanto que la normatividad secundaria se encuentra protegida por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que se expidió en 2002 y se reformó el 20 de julio de 2007, precisamente con la adición de un segundo párrafo y siete fracciones al artículo 6.[20]

Análogamente, el capítulo cuarto y los artículos 20 al 26 de la LFTAIPG regulan la protección de los datos personales de los individuos, exclusivamente en posesión del sector público. Sólo hasta 2010, con la expedición de la Ley Federal de Protección de Datos en Posesión de los Particulares, quedó igualmente regulada.

[20] Reforma publicada en el Diario Oficial de la Federación, el 20 de julio de 2007.

Derecho informático comparado

Un análisis de los avances internacionales del derecho a la protección de los datos personales revela que, en esta materia, nuestro país se encuentra con un largo camino por recorrer. Pese a las innovaciones introducidas en este ámbito. Además de las aportaciones efectuadas en Argentina, otros países europeos, como España, se han preocupado por la regulación de los datos personales. En ese país, se ha creado la Agencia Española de Protección de Datos[21] y, además, se han expedido leyes orgánicas, leyes reglamentarias y, en especial, se han fundado instituciones que protegen e, incluso, sancionan el uso indebido de los datos personales en manos de los sectores público y privado. Estos instrumentos, que abordan la parte sustantiva y adjetiva de este derecho, muestran el rezago de algunas entidades de nuestro país en la observancia de esta garantía.

En los países latinoamericanos, sólo Argentina, Bolivia, Brasil, Colombia, Ecuador, Guatemala, México, Panamá, Paraguay, Perú y Venezuela cuentan con una garantía primaria establecida en la Constitución, en materia de datos personales. En Argentina, se encuentra contemplada en el artículo 43 del tercer párrafo constitucional; en Bolivia, en el artículo 23 constitucional, mediante la acción de *Hábeas Data*; en Brasil, en el artículo 5 constitucional; en Colombia, en el artículo 15 constitucional; en Ecuador, en el artículo 30 constitucional; en Guatemala, en el artículo 31 constitucional; en Panamá, en el artículo 44 constitucional; en Paraguay, en el artículo 135 constitucional; en Perú, en el artículo 200, inciso 3, constitucional, y; finalmente, en México, en los artículos 6 y 16 constitucionales.

Por otra parte, el derecho informático, vinculado con las TIC y aún en desarrollo, es contemplado someramente en algunos estatutos internacionales, como el Tratado de Libre Comercio, que ha generado diversos problemas –e, incluso, delitos– que hacen vulnerables a determinados grupos. De este modo, no basta con reconocer y garantizar el derecho a la protección de los datos personales, sino que se debe crear toda una cultura de la importancia de este derecho.

[21] Parte del artículo 18, inciso 4º, de la Constitución Española y su implementación en 1978.

La condición humana en la sociedad tecnológica (grupos vulnerables)

Como se desprende de la actualidad, las nuevas TIC[22] hacen más vulnerables a los individuos. Por un lado, permiten su intervención masiva en una mayor cantidad de asuntos de interés, pero, por otro, los exponen a la manipulación de un grupo minoritario de personas, según advirtieron los participantes del Foro "Democracia electrónica y gobiernos abiertos", realizado el 18 de octubre de 2011 en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.

Estas consideraciones evidencian la necesidad de una legislación integral que regule el derecho de acceso a la información, en general, y el derecho a la protección de los datos personales, pues, aunque los individuos son vulnerables, existen determinados grupos más expuestos –como los usuarios móviles– a las estafas por Internet, a la acción de los *hackers* y a los efectos del *phishing* dirigido, un conjunto de técnicas empleadas para robar la identidad electrónica de un individuo; es decir, "una forma más furtiva y siniestra de spam o correo electrónico no deseado [...]; correos electrónicos que aparentan ser reales porque el estafador conoce los datos".[23]

Por lo que se refiere al derecho de la protección de datos personales, los menores de edad constituyen el grupo más vulnerable, ante su falta de experiencia en el manejo de recursos informáticos. Así, se vuelven presas fáciles para la comisión de delitos, motivo por el cual el Estado debe garantizar su protección.

Esto ya representa un derecho constitucional reconocido y de interés público, frente a la evolución de las legislaciones internacionales. Desde 1959, la Organización de las Naciones Unidas emitió diez principios englobados en la Declaración de los Derechos del Niño. El segundo de ellos afirma que "el niño gozará de una protección especial para que

[22] Francisco Cortázar Rodríguez (1997), "Trabajo, empleo y tecnologías de la información", en Revista Espiral, vol. III, número 9, pág. 121-138.

[23] Información extraída de mexico.cnn.com/tecnologia/2011/04/07/los-usuarios-moviles-son-mas-vulnerables-a-las-estafas-por-internet, consultada el 17 de noviembre de 2011.

pueda desarrollarse física, mental, moral, espiritual y socialmente". En el contexto actual, el derecho a la protección de los datos personales también debe incluir los diversos ámbitos que definen las TIC. Sin embargo, los procedimientos establecidos por el Código PEGI no garantizan este derecho básico de la infancia.[24]

El código PEGI *(Pan European Game Information)* es un código de autorregulación europeo. Cuyo objetivo es que los consumidores, principalmente padres y docentes, cuenten con información suficiente sobre los contenidos y las edades recomendadas de cada videojuego que existe en el mercado.

De esta manera, el análisis de la vulnerabilidad se identifica con el elemento central: la conexión entre la "libertad desde" (eventos críticos) como elemento necesario para lograr la "libertad para" (el logro de capacidades). Por su condición humana, los menores de edad son más vulnerables que los adultos, lo que implica la necesidad de resguardar la confidencialidad y el tratamiento de la información que se refiere directa o indirecta a ellos. Empero, no siempre existen criterios claros sobre cómo tratar la información referida a los menores o a sus familias: qué datos recabar, cómo reflejarlos documentalmente, quién puede acceder a ellos, qué hacer con ellos cuando la intervención puede darse por terminada, entre otros aspectos.

Evidentemente, se trata de preservar la intimidad y de respetar el criterio de confidencialidad, lo que no siempre resulta fácil, pues pueden originarse, de hecho, criterios o intereses enfrentados. A fin de preservar el interés superior de los niños, niñas y adolescentes, se han creado diversos proyectos. El Instituto de Investigación para la Justicia ha emitido el Memorándum sobre la protección de los datos personales y la vida privada en las redes sociales de Internet, que representa un instrumento para el avance en la protección de la infancia y la adolescencia.

El Memorádum data de julio de 2009 y está especialmente dirigido a los países de Latinoamérica y el Caribe, puede afirmarse que buena

[24] Petra María Pérez Alonso-Geta (2008), "Protección de la infancia y las nuevas tecnologías de la comunicación: el código PEGI de regulación de los videojuegos y el juego on - line", en Teoría de la educación. Educación y cultura en la sociedad de la información, Universidad de Salamanca, vol. 9, núm. 3, pp. 29-47.

parte de sus indicaciones y la totalidad de los principios que lo inspiran son aplicables a España y a Europa.[25]

Relación entre derechos humanos, democracia y tecnología

Actualmente, en México, las instituciones garantes de la protección de los datos personales reflejan las políticas gubernamentales, las cuales, en los Estados y en los municipios, tienen una corresponsabilidad social sustantiva, en razón de que los índices delictivos, con base en el uso de las TIC, se han incrementado. Por lo tanto, el Estado debe concentrar su atención y sus acciones en la generación de nuevas normas, para prevenir y sancionar las conductas delictivas ejecutadas.

Es necesario enfatizar la defensa de la libertad individual, con respecto a las posibles invasiones a la vida privada; es decir, en razón de que estos ámbitos novedosos presentan un campo fértil para las expresiones delictivas, ya que la delincuencia organizada, la iniciativa privada y el Estado acumulan datos personales de la sociedad desde perspectivas determinadas y pueden allegarse de personas de "confianza" que manipulan bases de datos con diversos fines. Esto plantea la necesidad de que el propio Estado se coloque a la vanguardia de las probables conductas delictivas en contra de los individuos o de la sociedad.

Si bien es cierto que ya existen avances en las disposiciones legales para este propósito, también destaca que el fenómeno criminal sigue avanzando en este rubro, lo que convierte a las personas, en general, y a los menores de edad, en específico, en objetivos para la ejecución de una diversidad de delitos.

La denominación de las TIC obedece a una evolución sustantiva y científica. Desde el punto de vista económico, proponen a la sociedad beneficios basados en las bondades de la innovación. Es verdad que, en estos ámbitos, quienes generan estas herramientas también han puesto a disposición de los padres de familia un conjunto de programas informáticos que impiden el acceso a páginas electrónicas

[25] Con información de www.pantallasamigas.net, consultada el 17 de noviembre de 2011.

con contenido nocivo, por lo cual es pertinente hacer referencia a la autorregulación. Como ejemplo de programas consultables en línea, se encuentran *"Protección de la infancia en línea: directrices para los niños"*; *"Iniciativa de protección de la infancia en l*ínea*"* y *"Actividades de la UIT sobre ciberseguridad"*, que pueden consultarse en la página electrónica www.itu.int/cop. Estos candados pueden contener reglas para los padres de familia, los docentes y los administradores de los espacios comerciales que ofrecen acceso a Internet; igualmente, pueden existir no sólo en los documentos previstos, como cuerpos normativos o legales en el capítulo de los derechos de los usuarios.

Algunas páginas electrónicas coinciden en la necesidad de educación en este rubro y colocan información útil, que puede evitar que los menores de edad sean víctimas de la delincuencia cibernética.[26] Algunas de las recomendaciones para proteger a los menores en el uso de Internet son:

1. Identificar las partes que intervienen en los procesos de interacción cibernética que se desarrollan en la casa, en la escuela o en el *cibercafé*; es decir, que los padres, docentes y los dueños de los establecimientos mencionados conozcan los riesgos, las ventajas y la responsabilidad de los adultos y de los menores de edad.

2. Promover una mayor comprensión de las redes sociales entre los padres y los educadores. Es recomendable que abran sus propias cuentas en las principales redes sociales (Facebook, Twitter y YouTube) para conocer los patrones de socialización de los menores de edad y advertir cualquier anomalía en los mensajes que éstos reciben.

3. Construir mecanismos de colaboración entre los padres, los educadores y los menores de edad, para promover la importancia de proteger sus datos personales en las redes sociales y el internet, en general.

[26] Como ejemplos de páginas electrónicas que proporcionan información útil para padres y educadores en beneficio de los menores de edad, pueden consultarse www.pantallasamigas.net/proteccion-infancia-consejos-articulos/sexting-adolescentes-sexo-y-telefonos-moviles.shtm, www.itu.int/cop y www.amipci.org.mx.

4. Difundir, de los padres y los educadores a los menores de edad, los riesgos de publicar y compartir información, videos o fotografías personales a través de las redes sociales.

Estos son sólo algunos ejemplos de la necesidad de educación que permea en la sociedad mexicana, que constituye un campo fértil para reforzar, con políticas educativas preventivas y efectivas, con el fin de que la sociedad en su conjunto se encuentre a salvo de las acciones antisociales de los *ciberdelincuentes.* Por lo tanto, la responsabilidad del Estado no concluye con publicar las normas que considera relevantes para disminuir los riesgos ante la delincuencia, no sólo mediante las instituciones garantes y de educación, sino que, también, debe fortalecer el tejido social con la distribución de información, para que las políticas sean más efectivas, eficaces y eficientes.[27]

Tecnologías de la información y la comunicación (TIC)

Las TIC son producto de la investigación científica, cuyos avances han sido vertiginosos. Tan es así que la innovación en los productos presentes en el mercado se renueva en lapsos cada vez más breves, lo que refleja una tarea sistemática en la invención tecnológica. La Asociación Mexicana de Internet (AMIPCI), en su séptimo estudio sobre los hábitos de los internautas en México, considera como usuarios de Internet a las personas que van desde los 6 años en adelante, así como a quienes que se conectan a la web en los *cibercafés*. En 2010, el número de internautas alcanzó los 34.9 millones; así, en diez años se ha triplicado la posesión de computadoras en hogares mexicanos, superando a la televisión y la radio.[28]

Como se ha referido anteriormente, con el empleo de los equipos informáticos, los seres humanos han fomentado nuevas formas de interacción. Estas herramientas se han convertido en instrumentos muy útiles, pues hacen más cómoda la vida, facilitan las relaciones

[27] Según se observa en www.itu.int/osg/csd/cybersecurity/gca/cop, con base en las directrices mencionadas, se invita a todas las partes interesadas, incluidos niños y jóvenes, a promover la adopción de políticas y estrategias de protección de los menores de edad en el ciberespacio y a proporcionar acceso seguro a las extraordinarias oportunidades y recursos que están disponibles en línea.

[28] Datos extraídos de www.amipci.org.mx/, consultada el 17 de noviembre de 2011.

entre la sociedad, el Estado y la iniciativa privada, y propician, sobre todo la comunicación efectiva. De este modo, las TIC han extendido sus bondades a través de la creación de un mundo virtual.

En consecuencia, no basta que el Estado dicte y ponga en vigencia las normas que prevengan los delitos cibernéticos o las conductas antisociales, porque no es la única forma de hacerlo, sino que, también, se debe atender las necesidades de educación en este sentido. Esto es posible a través de políticas educativas vanguardistas, que integren las responsabilidades de todos los que intervienen en los procesos educativos de las nuevas generaciones de seres humanos, para que de esta manera se puedan prevenir los delitos cometidos a través de las TIC.

Democracia y políticas públicas en protección de datos

Las políticas públicas vigentes en el gobierno federal y estatal, así como en varios municipios en nuestro país, despliegan una mayor presencia en ámbitos legales reiterados por la creación de las instituciones garantes de los derechos de acceso a la información pública y a la protección de datos personales. Este panorama proyecta la relevancia y la pertinencia de la integración de políticas públicas educativas,[29] no sólo entre las nuevas generaciones, sino entre todos aquéllos que integran el mundo virtual, como padres de familia, docentes y creadores de los programas informáticos que dan sustento a la *cibersociedad*.

En consecuencia, las estrategias establecidas en las políticas públicas no deben limitarse a fortalecer el ámbito legal, sino que también pueden enriquecerse con aportaciones teóricas y académicas y con la colaboración de las organizaciones no gubernamentales, con énfasis, en la generalidad, en las necesidades sociales y, en lo específico, en los reclamos de protección de los grupos cuyos derechos y datos han sido vulnerados o se encuentran en una situación vulnerable. De esta manera, con el compromiso de todos los componentes del tejido social,

[29] Actualmente, la Secretaria de Educación Pública, en el programa de cuatro grado de primaria, para la materia de formación cívica y ética (página 114), ha incluido breves referencias sobre la protección de los datos personales, al abordar el tema "La transparencia y el acceso a la información gubernamental".

se puede vislumbrar un mundo virtual con menos desequilibrios y con menos delitos.

De acuerdo con el estudio desarrollado por la AMIPCI, el Estado de México es la entidad con mayor número de internautas, seguido por el Distrito Federal y Jalisco. Consecuentemente, requiere la implementación de políticas públicas encaminadas a la prevención y protección de los datos personales de los menores de edad que utilicen las TIC.

En el Estado de México, la regulación de los datos personales se encuentra inserta, hasta el momento, en la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

Sin embargo, es necesaria una legislación específica en esta materia. A la fecha, se encuentra en estudio, en la Legislatura estatal, una iniciativa de Ley de Protección de Datos Personales que sólo prevé la protección de los datos personales en posesión de los entes públicos.

Sin embargo, con base en la legislación vigente, el Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios (Infoem) ha diseñado un programa permanente de pláticas informativas en las distintas instituciones educativas en la entidad, dirigidas a menores de edad, sobre el uso responsable de sus datos personales en redes sociales.

De este modo, aún con las limitantes que ofrece la ley, el Infoem, por convicción, se ha erigido como el órgano garante de la protección los datos personales de los menores de edad.

Conclusiones

- Los derechos humanos son prerrogativas de todos los seres humanos, cuya misión radica en reconocer y garantizar que mujeres y hombres se desarrollen plenamente, lo cual constituye la base del equilibrio social. Por ello, el estudio teórico y doctrinario de estos derechos, tomando en cuenta los grandes movimientos sociales, ha marcado las etapas que han permitido clasificarlos en primera, segunda, tercera y cuarta generación.

- Los estudiosos de las ciencias del derecho han realizado aportaciones desde la investigación científica, en los ámbitos de las ciencias jurídicas, cuya base se asienta en la sociedad. Así, han reiterado la importancia y la necesidad de promover la armonía social, conformada por los elementos que la integran: seres humanos que desarrollan papeles determinados, cuyas funciones deben mantener ese necesario equilibro, de crecimiento y concordia. Sólo de esta manera se podrán atender las necesidades de los grupos vulnerables y vulnerados en sus derechos, mediante estrategias de prevención y de educación, para que ellos mismos constituyan factores de cambio en su propio beneficio. Esta corresponsabilidad radica, directa y exclusivamente, en el Estado.

- Los vínculos entre los derechos humanos, la democracia y la tecnología se integran a través de la eficacia, la eficiencia y la efectividad, como premisas para la formulación de políticas públicas encaminadas, en términos del contrato social, a proporcionar a la sociedad las bases mínimas de educación y orientación, a fin de que se incorporen a un frente común contra la delincuencia electrónica, que afecta tanto al Estado como a la democracia. Para ello, resulta imperativo ejercer actividades de prevención significativa, desde el papel social que cada uno desempeña, como padres de familia, docentes o alumnos; como institución garante o educativa. Está claro que el fenómeno de la ciberdelincuencia demuestra un crecimiento sistemático, producto de una actividad muy bien organizada, lo cual impulsa la urgente necesidad de implementar políticas públicas para educar, orientar, prevenir y proteger al tejido social.

Referencias

Alonso-Geta, Petra María Pérez (2008), *Protección de la infancia y nuevas tecnologías de la comunicación: el código PEGI de regulación de los videojuegos y los juegos on-line,* en *Teoría de la educación. Educación y cultura en la sociedad de la información*, Universidad de Salamanca, vol. 9, núm. 3, pp. 29-47. Consultada el 28 de noviembre de 2011 en www.redalyc.uamex.mx.

Basterra, Marcela I. (2008), *Derecho constitucional provincial. Iberoamérica y México. Protección de datos personales. Ley 25.326 y Decreto 1558/01 comentados*, Buenos Aires, EDIAR / UNAM.

Bernigaud, Jorge Rafael (2003), *Hábeas Data*, Derecho Constitucional II. Consultada el 11 de octubre de 2011 en www.terrileyasociados.com/estudio/derecho/HABEAS%20DATA.doc.

Bobbio, Norberto (1986), *¿Qué alternativas a la democracia representativa?*, en ¿Qué *socialismo?*, Barcelona, Plaza y Janés, trad. J. Moreno.

Ferrajolli, Luigi. *Democracia y Garantismo*, Trotta, 2008.

Porto Macedo, Ronaldo (2002) *Privacidad, mercado e información*, en Cuestiones constitucionales, México, Universidad Nacional Autónoma de México, número 006, enero - junio, Red de Revistas Científicas de América Latina y el Caribe, España y Portugal, Universidad Autónoma del Estado de México.

Ornelas, Lina (2010), *El derecho de las niñas, niños y adolescentes a la protección de los derechos y su exigente frente a las redes,* en *Protección de datos personales. Compendio de lecturas y legislación*, México, IFAI / ITAM.

La protección de los Datos Personales en el Sector Salud

Germán E. Fajardo Dolci

Germán E. Fajardo Dolci

En este 2011 al frente de la CONAMED, ha impulsado el logro de eventos de trascendencia que permitan difundir las funciones de la Comisión en distintos ámbitos de la sociedad. Uno de los logros más destacados es la gestión ante la Organización Mundial de la Salud, para que la CONAMED fuera designada Centro Colaborador de la OMS/OPS. Médico Cirujano egresado de la Universidad La Salle; especialista en Otorrinolaringología en el Hospital General de México; especialidad en el Programa de Alta Dirección del IPADE.

Es miembro de doce Asociaciones Médicas entre las que destacan la Academia Nacional de Medicina, la Academia Mexicana de Cirugía y la Sociedad Mexicana de Calidad de la Atención Médica.

Ha sido profesor de pregrado y posgrado de la Universidad Nacional Autónoma de México y la Universidad Anáhuac. Ha dictado conferencias y presentado trabajos en foros nacionales e internacionales, entre los que destacan: Australia, España, Venezuela, Dinamarca, Argentina y los Estados Unidos. Es coautor de 88 artículos científicos en revistas médicas, 17 capítulos de libros de medicina y 11 libros sobre diversos temas médicos. Receptor de varios premios y distinciones como el Bienal Funsalud “Alfonso Robinson Bours” 2001; premio de la Academia Nacional de Medicina a la mejor Obra Médica 2001; Premio “Dr. Manuel Castillejos”, Academia de Cirugía, 2005; Premio Nacional de Investigación 2009, Fundación GlaxoSmithKline (GSK) y FUNSALUD en “Economía de la Salud”, 2009; entre otros).

Introducción

En México la protección de Datos Personales es un área del conocimiento relativamente poco explorada, con una legislación de reciente desarrollo, sobre todo en lo que se refiere a cuestiones que se relacionan con el tratamiento de datos relativos al estado de la salud de las personas.

A manera de preámbulo, se puede mencionar que con la internacionalización y reconocimiento de los derechos humanos han surgido diversas normas enfocadas a proteger la esfera privada de los individuos; es así que en diciembre de 1948, en la Declaración Universal de los Derechos Humanos, se estableció en el artículo 12 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*".[1] El Pacto Internacional de Derechos Civiles y Políticos de 1966 abundó sobre el tema al señalar en su artículo 17 que:

> 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.[2]

En ese contexto, la protección de los datos personales garantiza el derecho al honor y a la intimidad de las personas y las defiende del uso indebido de sus datos. Por eso, este derecho ha sido consagrado por

---

* Elaborado con el apoyo de los licenciados Juan Antonio García Villa, Armando Arias Díaz Barriga y Aidé Lovera Ramírez.

[1] Departamento de Información Pública de las Naciones Unidas. *Declaración Universal de los Derechos Humanos*. <http://www.un.org/es/comun/docs/?path=/es/documents/udhr/index_print.shtml> [25 de noviembre de 2011>.

[2] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *Pacto Internacional de Derechos Civiles y Políticos*. <http://www2.ohchr.org/spanish/law/ccpr.htm> [25 de noviembre de 2011].

normas constitucionales, leyes, reglamentos y lineamientos. Pero nada de ello tendría sentido si los particulares no pudieran protegerse ante los abusos, por parte del gobierno o de particulares, en el tratamiento de sus datos. Esta protección se ha venido regulando al paso que marca el inexorable avance de la tecnología, la cual ha dado origen a la nueva sociedad del Siglo XXI, denominada por algunos autores como la *sociedad de la información* en la que se debe atender de manera simultánea al tratamiento de datos personales, la velocidad y volumen de su transmisión, junto con una adecuada protección de las personas.

El derecho a la protección de los datos personales surge así como una necesidad en el Estado de Derecho, de dotar a los ciudadanos de herramientas para ejercer facultades de control sobre sus datos en poder del gobierno o de los particulares, a través de cuatro dimensiones: *acceso*, *rectificación*, *cancelación* y *oposición* de tales datos; mejor conocidas como Derechos ARCO.

Actualmente no se puede pasar por alto que cualquier tratamiento de bases de datos que contenga información personal representa un factor de riesgo para los particulares, toda vez que puede dar lugar a la generación de daños y perjuicios que afecten la seguridad de las personas, su identidad, patrimonio y sobre todo su privacidad; por ello, ante esta posibilidad, es que surge el derecho a la protección de datos personales. Esta necesidad, que se ha presentado a nivel mundial, de tutelar los derechos de todo individuo respecto a la recopilación y tratamiento de sus datos personales, propició que el llamado derecho a la autodeterminación informativa pasara a formar parte del elenco de los Derechos Humanos incluidos en nuestra Carta Magna, y disposiciones que de ella emanan; en este punto es preciso aclarar que estos derechos no conceden a la persona un definitivo y absoluto poder sobre sus datos, sino el derecho a estar informado del procesamientos de éstos y de los fines que se pretenden alcanzar, junto con el ejercicio de los Derechos ARCO y la correlativa obligación del Gobierno y de los particulares de su pleno respeto y acatamiento.

Reconocimiento normativo del derecho a la protección de datos personales

Esta limitación ha sido regulada en diversas disposiciones internacionales, citando a manera de ejemplo, lo que establece el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales en su artículo 8, en alusión al derecho a la intimidad, al señalar que éste no goza de un carácter absoluto en las sociedades democráticas, por cuento su contenido puede ser restringido, en aras de un interés prevalente.

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.[3]

Los supuestos en los que el ciudadano debe admitir esa "limitación", implica la necesidad de un ejercicio estricto de los mismos. Además, los Estados no disponen de libertad para aplicar indiscriminadamente tales injerencias, sino que deberán, como regla general, usar el instrumento menos lesivo, y establecer garantías adecuadas frente a los abusos.

Si bien dichas limitaciones han de ser aceptadas en aras de salvaguardar intereses superiores definidos en un Estado de Derecho, las mismas están sujetas a determinados requisitos que, desde lo señalado en la Sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983 (Ley del Censo. Derecho de la personalidad

[3] Secretaría del Tribunal Europeo de Derechos Humanos. *Convenio para la Protección de los Derechos Humanos de las Libertades Fundamentales. Revisado de conformidad con los Protocolos No. 11 y 14*. Versión en Español. Junio de 2010. <http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf> [24 de noviembre de 2011].

y dignidad humana) pueden sistematizarse en dos ineludibles y concretas exigencias:

> a) Un fundamento legal, del que pueda deducirse con claridad y de forma inteligible para el ciudadano los supuestos y el ámbito de las limitaciones, y que responda, por tanto, al imperativo de claridad normativa inherente al Estado de Derecho.
> b) Ha de utilizarse el principio de proporcionalidad en la restricción de estos derechos fundamentales; es decir, que la medida sea adecuada -necesaria en una sociedad democrática- y, además, indispensable para la consecución de los respectivos y predeterminados fines. La interferencia que lleve aparejada no puede ser desproporcionada a la importancia del objeto y a las cargas que imponga al ciudadano.[4]

De una manera sucinta podemos pues concluir que las diferentes disposiciones y ordenamientos internacionales que abordan el tema de los derechos humanos han establecido como denominador común el hecho de que el Estado, a través de sus diferentes órganos de gobierno, tiene la obligación de tutelar la seguridad e intimidad de los individuos en dos supuestos: en primer lugar, debe impedir intromisiones de todo tipo en la vida privada e intimidad de la persona, provengan de autoridades o de particulares, y en segundo plano, debe garantizar que el individuo pueda verificar qué datos de sí mismo se encuentran en cualquier archivo o base de datos a efecto de ejercer plenamente el derecho a la autodeterminación informativa, entendido éste como el derecho a conocer quién, cuándo y para qué pueden utilizar sus datos personales.

A pesar del reconocimiento, casi universal, del derecho a la protección de los datos personales, no fue sino hasta en las últimas décadas que los gobiernos decidieron incluir o reformar a nivel constitucional normas tendientes a proteger la esfera de uno de los derechos fundamentales de los individuos, el de la privacidad, el cual se ha visto cada día más vulnerable, sobre todo a partir de este nuevo

[4] Instituto Español de Informática y Derecho. Sánchez Bravo, Álvaro A. *"Espionaje en el Ciberespacio".* <http://www.ieid.org/congreso/ponencias/Sanchez%20Bravo,%20Alvaro%20A.pdf>. [28 de noviembre de 2011].

siglo, en el que se empieza a dar un despliegue tecnológico, hasta hace pocos años inconcebible para muchos de nosotros.

En la actualidad, no es posible concebir la vida de los seres humanos ni su interacción, sin el uso de tecnologías informáticas, lo que conlleva el intercambio de flujos de información de todo tipo, incluida la relativa a las personas. Hoy en día se puede acceder a información sobre millones de seres humanos y sus actividades en prácticamente cualquier parte del planeta, por lo se puede afirmar, sin temor a equivocarse, que los avances tecnológicos irrumpen silenciosamente en el ámbito de lo privado de los individuos.

Ante este panorama, diremos que los horizontes de la privacidad se están transformando en tierra desconocida para quienes la habitan, debido a que sin que las personas se enteren, ni mucho menos otorguen su conocimiento, terceros –ya sean entes públicos o privados- recaban y transmiten información sobre sus datos personales a través de todo tipo de procedimientos que brindan las tecnologías de punta.

Si bien es cierto que los avances tecnológicos generalmente repercuten de forma positiva en la calidad de vida del ser humano, no debemos soslayar que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho, en su objetivo último de ordenar la convivencia social, debe dar respuesta. La tecnología no puede permanecer ajena al Derecho, por más que la velocidad con la que ocurren las innovaciones tecnológicas amenace con hacer obsoleto cualquier esfuerzo por regular su impacto sobre el derecho a la vida privada (Guerrero, 2006).

La probabilidad de que se susciten abusos a la vida privada aumenta hoy como consecuencia del desarrollo de la llamada "sociedad de la información". La expansión global de las redes informáticas y de comunicación hace cada vez más frecuente los casos de robo de identidad o de discriminación a través de la obtención de perfiles que hacen identificables a las personas en sus patrones de consumo y de ahorro, o en sus inclinaciones y preferencias, e incluso por sus estados de salud.

Dado que los medios tradicionales de protección de la vida privada son insuficientes en la actualidad, cada vez más países han aprobado leyes de protección de datos personales. Varias organizaciones a nivel internacional se han preocupado por el manejo de datos, como ejemplo citaremos a la *Cumbre Mundial sobre la Sociedad de la Información*, misma que ha reaccionado ante la constante vulnerabilidad de la privacidad de las personas, ocasionada por la falta de regulación de las nuevas tecnologías, convocando *"…a todas las partes interesadas a que garanticen el respeto por la privacidad y la protección de los datos e informaciones personales, ya sea mediante la adopción de medidas legislativas y la aplicación de marcos de cooperación, o bien mediante el intercambio entre las empresas y los usuarios de las prácticas idóneas, los mecanismos de autorregulación o las medidas tecnológicas pertinentes. Instamos a todas las partes interesadas, en particular a los gobiernos, a que reafirmen el derecho de acceso a la información por los particulares, en virtud de la Declaración de Principios de Ginebra, así como de otros instrumentos internacionales en esta materia convenidos de mutuo acuerdo, y a que establezcan la coordinación adecuada a escala internacional".*[5]

Con este marco de referencia, surge en nuestro país la necesidad de contar con disposiciones legales que regulen la protección de los datos personales, entre los que se incluyen los *relativos al estado de salud*, los cuales tienen internacionalmente una concepción de *datos sensibles*, con el fin de brindar certeza al ciudadano, para que éste conozca qué datos son recabados y con qué fin, así como la posibilidad de ejercer los derechos ARCO, es decir, el derecho de acceder a su información y en caso de ser inexacta de rectificarla, el derecho a cancelar el dato cuando ya no sea pertinente o ha perdido vigencia y el derecho a oponerse a su utilización por parte de un tercero.

Antecedentes en México

La primera legislación en México que contempló de manera precisa la protección de los datos personales, aunque limitada al ámbito

[5] Comunidad Iberoamericana de Asociaciones de Usuarios de Internet. Cumbre Mundial sobre la Sociedad de la Información. *Programa de Acciones de Túnez para la Sociedad de la Información. Ginebra 2003 – Túnez 2005.* <http://www.diadeinternet.org/2011/IMG/pdf/programa_acciones_tunez_SI.pdf> [24 de noviembre de 2011]

público, fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el Diario Oficial de la Federación el 11 de junio de 2002.

Con esta Ley, el Gobierno Mexicano atiende dos exigencias de la vida democrática del país. Por un lado, que el espacio gubernamental sea efectivamente público, y de esta manera se obligue a abrir sus archivos y entregar la información sobre su forma de trabajo, el uso de los recursos públicos y sus resultados, entre otras cuestiones, y por otro lado, cumplir con un reclamo de carácter universal, el respeto al derecho a la privacidad de las personas a través de la protección de sus datos personales. Uno de los objetivos de la LFTAIPG en términos de lo dispuesto en el artículo 4, fracción III, es garantizar la protección de los datos personales en posesión de los sujetos obligados (Poderes de la Unión, órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal).

En el artículo 3, fracción II, de la LFTAIPG se define a los *Datos Personales* como *"La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad".*

La LFTAIPG, en su artículo 18, fracción II, considera a los datos personales, como información confidencial, la cual, para su difusión, distribución o comercialización, requiere el consentimiento de los individuos, titulares de los mismos.

En el Capítulo IV denominado *"Protección de Datos Personales",* conformado por siete artículos, se establece la responsabilidad de los sujetos obligados en el tratamiento de los datos que obren en su poder, así como disposiciones sobre los derechos de acceso y corrección de los datos personales y los procedimientos para hacerlos efectivos.

En ese apartado de la LFTAIPG destaca por su importancia, y considerando el tema que nos ocupa, el ejercicio del derecho de acceso a los datos de la salud de las personas por parte de su titular o sus

representantes y las implicaciones o repercusiones que el mismo ha generado en el sector salud, de conformidad con lo que establece el artículo 24, que a la letra dice:

> "Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante…"

El acceso al expediente clínico por parte de su titular ha sido uno de los temas más controversiales desde que entró en vigor esta Ley; tema que abordaremos más adelante.

El Reglamento de la LFTAIPG,[6] que tiene por objeto reglamentar la Ley en lo relativo a la Administración Pública Federal (APF), solamente dedica dos artículos (47 y 48) a la protección de datos personales.

Ante la necesidad de regular de una manera más precisa y completa el tema de los datos personales, el Pleno del entonces Instituto Federal de Acceso a la Información Pública (IFAI),[7] expidió los Lineamientos de Protección de Datos Personales,[8] mismos que tienen por objeto, en términos del Numeral Primero:

> "…establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y

[6] Publicado en el Diario Oficial de la Federación el 11 de junio de 2003.

[7] Actualmente Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

[8] Publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

> lesiva para la dignidad y derechos del afectado.
> Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la Administración Pública Federal en el ejercicio de sus atribuciones."

El IFAI, como órgano de control, para garantizar el derecho a la protección de datos personales en poder de las dependencias y entidades de la APF, utiliza dos herramientas: la primera, la emisión de criterios específicos para fijar políticas y procedimientos de observancia obligatoria, como es el caso de los *Lineamientos* antes citados, y la segunda, la resolución de los recursos de revisión que los ciudadanos interponen para hacer efectivos sus derechos de acceso y corrección de datos personales.

La CONAMED y los datos personales en salud

Por otra parte, refiriéndonos al papel que la Comisión Nacional de Arbitraje Médico (Conamed), ha desempeñado en relación con la protección de los datos personales de la salud de los usuarios de los servicios médicos, pacientes y familiares de éstos, así como de los profesionales de la salud, resulta necesario recordar su objeto y atribuciones. La Conamed se creó mediante Decreto del Ejecutivo Federal,[9] como un órgano desconcentrado de la Secretaría de Salud, dotado de autonomía técnica para recibir quejas, investigar las presuntas irregularidades en la prestación o negativa de prestación de servicios médicos y para emitir sus opiniones, acuerdos y laudos.

Tiene por objeto contribuir a resolver los conflictos suscitados entre los usuarios de los servicios médicos y los prestadores de los mismos, a través de mecanismos alternativos a la vía judicial, como la conciliación y el arbitraje.

La tarea de la Conamed en el derecho a la protección de la salud, se desprende de las atribuciones que le fueron concedidas, entre otras, brindar asesoría a pacientes y prestadores de servicios médicos, del

[9] Publicado en el Diario Oficial de la Federación el 3 de junio de 1996.

ámbito público y privado, sobre sus derechos y obligaciones; para seguir el procedimiento correspondiente frente a la presentación de una queja por probables irregularidades en la prestación del servicio; así como para fungir como conciliador o como árbitro.

También le fueron conferidas atribuciones para actuar en el marco del derecho a la protección de la salud en favor de los pacientes. Entre las que destacan, la posibilidad que tiene para intervenir de oficio, esto es, sin que medie petición alguna, en aquellos casos de interés general que se encuentren dentro de su esfera de competencia; informar a las autoridades, colegios, academias, asociaciones, consejos de médicos, comités de ética u otros similares, del incumplimiento de sus resoluciones por parte de los prestadores de servicios, así como hacer del conocimiento de las autoridades competentes hechos, que en su caso, pudieran llegar a constituir la comisión de algún ilícito.

La Conamed, tiene un doble propósito: atender las inconformidades que resultan de la prestación de servicios médicos y, con su análisis, contribuir a elevar la calidad de la atención.

Para llevar a cabo los servicios que brinda la Conamed, entre los que se encuentran: orientación; asesoría especializada; conciliación; arbitraje; emisión de dictámenes médicos, y en general para cumplir con las atribuciones que le confiere su Decreto de Creación, requiere conocer, recabar y promover, información y datos personales de usuarios y prestadores de servicios médicos, pero principalmente datos sensibles, como lo son los relativos al estado de salud de las personas.

La Conamed, en sus más de 15 años de existencia, así como la mayoría de las instituciones públicas y privadas que prestan servicios de atención médica, han observado y aplicado, como un pilar fundamental de su quehacer, el pleno respeto al derecho a la protección de la intimidad y privacidad de los individuos que acuden a ellas, a través de la confidencialidad de los datos personales, sean éstos sensibles o no.

Para asegurar la confianza de sus usuarios, la Conamed garantiza la no intromisión de terceros no autorizados en los procedimientos que realiza, así como en los servicios que brinda, al mantener la secrecía de los asuntos que conoce y de las resoluciones que emite.

En ese sentido, el *Reglamento de Procedimientos para la Atención de Quejas Médicas y Gestión Pericial* de la Comisión Nacional de Arbitraje Médico, en su artículo 7 establece: *"Todo servidor público de la Comisión está obligado a guardar reserva de los asuntos que se tramiten y sustancien en la misma, así como respecto de los documentos públicos o privados que formen parte de los expedientes de queja y al igual que de las opiniones y resoluciones que se adopten en cada caso. Las partes estarán obligadas a guardar confidencialidad durante el proceso arbitral; al efecto se otorgarán los instrumentos y cláusulas correspondientes."* [10]

Así también, desde diciembre de 2001, antes de la entrada en vigor de la LFTAIPG, la Conamed publicó y promovió la difusión de la *Carta de los Derechos Generales de las Pacientes y de los Pacientes*,[11] como parte de las estrategias para mejorar la calidad de la atención médica en México, en la que predomina la importancia del respeto a los derechos de los pacientes, el fomento de una cultura de servicio orientada a satisfacer sus demandas, lo que entraña respetar su dignidad y autonomía, garantizar la confidencialidad de la información generada en la relación médico-paciente y brindar una atención que minimice los múltiples puntos de espera.

Dicha Carta, en su Numeral 6, *"Ser tratado con confidencialidad"*, señala: *"La paciente o el paciente tiene derecho a que toda la información que exprese a su médico, se maneje con estricta confidencialidad y no se divulgue más que con la autorización expresa de su parte, incluso la que derive de un estudio de investigación al cual se haya sujetado de manera voluntaria; lo cual no limita la obligación del médico de informar a la autoridad en los casos previstos por la ley."*

La entrada en vigor de la LGTAIPG, reforzó la posición institucional de la Conamed en torno a la protección de los datos personales que

[10] Disposición que apareció por primera vez en el *Reglamento de Procedimientos para la Atención de Quejas* de la Comisión Nacional de Arbitraje Médico, publicado en el Diario Oficial de la Federación el 29 de abril de 1999, ordenamiento que fue abrogado por el *Reglamento de Procedimientos para la Atención de Quejas Médicas y Gestión Pericial* de la Comisión Nacional de Arbitraje Médico, publicado en el aludido órgano informativo el 21 de enero de 2003, mismo que fue reformado el 25 de julio de 2006.

[11] Comisión Nacional de Arbitraje Médico. *Carta de los Derechos Generales de las Pacientes y de los Pacientes*. <http://www.conamed.gob.mx/publicaciones/cartas/cartapacientes.php?seccion=22>. [24 de noviembre de 2011].

recaba para el desahogo de sus procedimientos, ya que invariablemente este tipo de información se clasifica como confidencial, en términos de lo dispuesto por el artículo 19 de este ordenamiento, limitando el acceso a la misma solamente al titular o a sus representantes con fundamento en el artículo 24 de la Ley en comento.

Se puede afirmar, que el derecho a la intimidad está garantizado en las instituciones gubernamentales que prestan servicios de atención médica, e incluso nos atreveríamos a aseverar que también en las del ámbito privado, así como en aquellas que tienen incidencia en esta materia, como es el caso de la Conamed, al asegurar el no acceso a la información que les ha sido confiada a terceros no autorizados. Desde este punto de vista, la protección de datos personales atiende a la satisfacción del derecho fundamental de protección a la intimidad, a la confidencialidad y, en general, a la privacidad del ser humano.

Partiendo del supuesto antes mencionado, la protección de datos personales en materia de salud, al amparo de la LFTAIPG, no ha representado grandes dificultades para su cumplimiento por parte de las instituciones de la Administración Pública Federal que manejan este tipo de información; el debate surge en torno al acceso a tales datos, como parte del derecho a la información, concebido como un derecho humano fundamental consagrado en nuestra Constitución.

La vigencia de la LFTAIPG, propició que el tema de los datos personales de salud, en función del derecho que puede tener el paciente de acceder a la totalidad de la información contenida en su expediente clínico, diera lugar a diversos cuestionamientos por parte de las instituciones públicas de salud y la consecuente resistencia a la entrega del mismo.

Tratamiento del expediente clínico

Algunos de estos cuestionamientos parten del hecho de que mientras los prestadores de servicios médicos privados atienden las peticiones de sus pacientes en términos de las disposiciones sanitarias, principalmente la Norma Oficial Mexicana 168. *Del Expediente Clínico*,[12]

[12] Publicada en el Diario Oficial de la Federación el 30 de septiembre de 1999, y que en sus

mediante la entrega de un resumen clínico, el IFAI, determinó, a través de la resolución de diversos recursos de revisión, la obligación de entregar copia integra del expediente clínico, emitiendo, incluso, para estos casos, el *Criterio 04-09 Expediente Clínico. Por regla general su confidencialidad no es oponible al titular de los datos personales o su representante legal.* [13] Lo anterior, propició un régimen diferenciado, y de alguna manera discriminatorio, en el tratamiento de los datos clínicos, con un efecto desigual en lo que respecta a los derechos del paciente, que por atenderse en el sector público adquirió un mayor derecho en comparación al que lo hizo en el servicio privado (Ramírez, 2006: 19-21).

Otra de las cuestiones, quizá la de mayor peso, que han argumentado las instituciones públicas es la de que no hay derechos absolutos, y en el caso de información sobre el estado de salud de una persona, es indispensable resguardar cierta información contenida en el expediente clínico, en especial aquella que pueda afectar a terceros o incluso la propia salud del paciente.

No obstante estos argumentos, la mayoría de las instituciones públicas del sector salud se han ajustado al criterio del IFAI, fundado en el derecho que le concede la Ley a toda persona de conocer y tener acceso a sus datos personales contenidos en su expediente personal, médico, clínico u otro sin distingo del ramo o de la institución y en beneficio de su dignidad y derecho a la protección a la salud y a la vida; máxime que sus resoluciones son definitivas para las dependencias y entidades de la Administración Pública Federal. Aun así, persiste cierta resistencia del sector salud, pues se sigue insistiendo en que debe prevalecer la finalidad terapéutica y, que por ello, lo ideal sería proteger cierta información contenida en el expediente clínico, ya que el acceso total, irrestricto o indiscriminado al mismo, puede repercutir

Numerales 5.3. y 5.5. respectivamente, señala: "Los expedientes clínicos son propiedad de la institución y del prestador de servicios médicos, sin embargo, y en razón de tratarse de instrumentos expedidos en beneficio de los pacientes, deberán conservarlos por un periodo mínimo de 5 años, contados a partir de la fecha del último acto médico".

"Los prestadores de servicios otorgarán la información verbal y el resumen clínico deberá ser solicitado por escrito, especificándose con claridad el motivo de la solicitud, por el paciente, familiar, tutor, representante jurídico o autoridad competente."

[13] Instituto Federal de Acceso a la Información y Protección de Datos. Criterios del Pleno del IFAI. <http://www.ifai.org.mx/Criterios> [24 de noviembre de 2011].

negativamente en la actividad médica, generando un esquema en el que prive la desconfianza y se propicie el ejercicio de la medicina defensiva.

El ámbito local de aplicación

Retomando las disposiciones de la LFTAIPG, cabe destacar que el H. Congreso de la Unión, tomó la decisión de que fuera una ley de aplicación exclusivamente federal, y no una ley general, lo que abrió la puerta a una variedad de versiones estatales y municipales sobre un mismo derecho, generando una heterogeneidad manifiesta y perjudicial para el pleno ejercicio del derecho de acceso a la información.

Así también, a efecto de consolidar la concepción de que el acceso a la información es un derecho fundamental que debe ser reconocido en la Constitución como una garantía de los individuos frente al Estado Mexicano, en todos sus niveles, poderes, órganos y entidades, así como establecer un mínimo a nivel nacional que hiciera congruente y coherente el ejercicio de este derecho,[14] se reformó el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, mediante Decreto por el que se adiciona un segundo párrafo con siete fracciones, quedando, en lo que respecta a la protección de datos personales, de la siguiente forma:

> Artículo 6º … El derecho a la información será garantizado por el Estado.
> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
> …
> La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
> …
> …

[14] Instituto Federal de Acceso a la Información Pública. *Reforma al artículo 6º constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos.* Quinta Edición, México, D. F. Noviembre de 2008. Págs. 23 y ss.

VII.
…

Siguiendo con los cambios al marco jurídico de la protección de datos personales, el 1º de junio de 2009, se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona un segundo párrafo al artículo 16 Constitucional, en los siguientes términos:

> Artículo 16. 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.
> 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 públicas o para proteger los derechos de terceros…

Con esta reforma se reconoce el derecho a la protección de datos personales como un derecho fundamental y autónomo, así como los derechos de acceso, rectificación, cancelación y oposición (ARCO) que podrán ejercer los titulares de dichos datos, conforme a los principios y excepciones que se prevean en la ley reglamentaria.

Así también, el 30 de abril de 2009 se publicó en el Diario Oficial de la Federación el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, que faculta al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de los particulares. En esta enmienda constitucional se destacó la necesidad de contar con un instrumento legal que permita encauzar de manera uniforme las relaciones jurídicas que se produzcan al amparo del derecho a la protección de datos, en virtud de su estrecho vínculo con el comercio nacional e internacional.[15]

[15] Instituto Federal de Acceso a la Información Pública. 7º Informe de labores al H. Congreso de la Unión 2009. Primera Edición. México, D. F. Julio 2010. Pág. 72.

En el artículo Segundo Transitorio de este Decreto se fijó un plazo de 12 meses para que ese órgano colegiado emitiera la ley en la materia.

En cumplimiento a este mandato, el 5 de julio de 2010 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y se reforman los artículos 3, fracciones II y VII y 33, así como la denominación del Capítulo II, del Título Segundo, de la LFTAIPG.

La LFPDPPP en su artículo 1º, establece que se trata de una Ley de orden público y de observancia general en toda la República, que 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.

Mediante este Decreto y de acuerdo con la expedición de la LFPDPPP, se modifica el concepto de datos personales que aparece en la LFTAIPG, para quedar como sigue:

> Artículo 3. Para los efectos de esta Ley, se entenderá por:
> …
> Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

En la fracción VI de este artículo, se establece lo que se debe entender por datos personales sensibles, al señalar que son: *"Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual."*

La LFPDPPP recoge principios reconocidos internacionalmente en el tratamiento de datos personales, como son los de licitud, lealtad, consentimiento (tratándose de datos sensibles deberá ser expreso y por escrito), calidad, finalidad, proporcionalidad e información;

establece las responsabilidades y deberes que tienen las personas que traten datos personales, así como los derechos de acceso, rectificación, cancelación y oposición que asisten a los titulares de los mismos. De esta forma, por una parte garantiza el poder de decisión y control que detenta una persona sobre la información que le concierne, y por la otra, dispone la obligación del responsable del tratamiento de velar por el efectivo cumplimiento de dichos principios.

En la Ley se prevé un régimen especial para el tratamiento de los datos personales sensibles, como son los referentes a los estados de salud, designando al IFAI como la autoridad garante de la observancia de los derechos y principios mencionados en la misma, cambiando su denominación a *Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).*

Cabe mencionar que la LFPDPPP dispone en el artículo 40 que las dependencias que regulan sectores en los que se tratan datos personales como parte de la actividad sustantiva que desarrollen, tendrán la facultad de emitir regulación secundaria en materia de protección de datos personales con la coadyuvancia del IFAI; a manera de ejemplo se pueden citar los casos de las Secretarías de Salud; Educación Pública; Comunicaciones y Transportes; Hacienda y Crédito Público, entre otras (IFAI, 2011).

Ante el incumplimiento de las obligaciones que dispone la LFPDPPP, el IFAI, como autoridad garante de la protección de datos en posesión de los particulares, así como de los que se encuentran en poder de la Administración Pública Federal, tiene la facultad de imponer sanciones que van desde el apercibimiento hasta multa de 320,000 días de salario mínimo; tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces los montos establecidos, según la gravedad de la infracción.[16]

Reflexiones finales

La protección de datos personales en México tiene dos ámbitos de regulación diferenciados: el público, a través de la *Ley Federal de*

[16] Art. 64 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Transparencia y Acceso a la Información Pública Gubernamental, y el privado, mediante la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, no obstante, se trata de las dos caras de una misma moneda, cuyo objetivo final es defender la privacidad e intimidad de las personas.

En este contexto, es de suma importancia profundizar en el análisis del impacto que puede tener el acceso, total o indiscriminado, al expediente clínico, a efecto de no desvirtuar el valor de la confianza que por siglos ha caracterizado a la relación médico-paciente, por lo que será conveniente promover reformas, principalmente a la Ley General de Salud, con el fin de determinar la modalidad, la profundidad del acceso y sus límites, incluso ante la solicitud del propio paciente, aplicables tanto en el ámbito público como en el privado, evitando así un comportamiento defensivo del gremio médico.

Algunos de los retos que el propio IFAI ha reconocido y que debe enfrentar conjuntamente con las dependencias involucradas en el tema de protección de datos personales, giran en torno a la necesidad de definir el tratamiento más adecuado de los datos personales sensibles; cómo abordar el tratamiento de datos en la era digital y qué medidas preventivas y correctivas tomar al respecto; cuáles deben ser las medidas de seguridad mínimas que se observarán por los responsables del tratamiento de datos para la protección de los mismos; cómo garantizar una transferencia de datos sin afectar el flujo eficiente y legítimo de la información; cómo desarrollar un modelo de corresponsabilidad con los responsables del tratamiento de datos, a fin de generar una cultura preventiva y no sancionadora en torno a la protección.

Por consiguiente, se debe admitir que la tecnología avanza más rápido que la regulación. Por lo tanto, la legislación en la materia debe permitir la flexibilidad necesaria para promover la autorregulación y certificación, así como utilizar a la tecnología en su favor, reconociendo a ésta como uno de los motores en la protección de los datos personales.

La protección efectiva de los datos personales en el sector salud puede conducir a mejorar los procedimientos médicos; evitar un uso discriminatorio o lesivo de la intimidad; brindar información falsa, inexacta o desactualizada en perjuicio de los pacientes; establecer

estándares que coadyuven a la investigación en la ciencia médica, así como a integrar de una mejor manera la historia clínica y su interoperabilidad por las instituciones del sector salud.

Referencias

Constitución Política de los Estados Unidos Mexicanos.

Comisión Nacional de Arbitraje Médico. *Carta de los Derechos Generales de las Pacientes y de los Pacientes*. Disponible al 24 de noviembre de 2011 en http://www.conamed.gob.mx/publicaciones/cartas/cartapacientes.php?seccion=22> [24 de noviembre de 2011].

Comunidad Iberoamericana de Asociaciones de Usuarios de Internet. *Cumbre Mundial sobre la Sociedad de la Información. Programa de Acciones de Túnez para la Sociedad de la Información. Ginebra 2003 – Túnez 2005.* Disponible al 24 de noviembre de 2011 en http://www.diadeinternet.org/2011/IMG/pdf/programa_acciones_tunez_SI.pdf>.

Decreto de Creación de la Comisión Nacional de Arbitraje Médico.

Departamento de Información Pública de las Naciones Unidas. *Declaración Universal de los Derechos Humanos*. Disponible al 25 de noviembre de 2011 en http://www.un.org/es/comun/docs/?path=/es/documents/udhr/index_print.shtml>.

Guerrero Picó, María del Carmen (2006). *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*. Colección Estudios de Protección de Datos. Editorial Thomson Civitas, S. A. Pamplona, España.

Instituto Español de Informática y Derecho. Sánchez Bravo, Álvaro A. "*Espionaje en el Ciberespacio*". Disponible al 28 de noviembre en http://www.ieid.org/congreso/ponencias/Sanchez%20Bravo,%20Alvaro%20A.pdf.

Instituto Federal de Acceso a la Información Pública (2008) *Reforma al artículo 6º constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos*. Quinta Edición, México, D. F. Noviembre.

Instituto Federal de Acceso a la Información y Protección de Datos. *Criterios del Pleno del IFAI*. Disponible al 24 de noviembre de 2011 en http://www.ifai.org.mx/

Criterios.

Instituto Federal de Acceso a la Información Pública (2010) *7º Informe de labores al H. Congreso de la Unión 2009.* Primera Edición. México, D. F. Julio. Pág. 72.

Instituto Federal de Acceso a la Información y Protección de Datos (2011) *8º Informe de Labores al H. Congreso de la Unión.* 1ª. Edición. México, D. F.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Lineamientos de Protección de Datos Personales.

Norma Oficial Mexicana 168. Del Expediente Clínico.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *Pacto Internacional de Derechos Civiles y Políticos*. Disponible al 25 de noviembre de 2011 en http://www2.ohchr.org/spanish/law/ccpr.htm.

Ramírez Ramírez, Agustín (2006) Impacto del acceso al expediente clínico. Revista CONAMED. Vol. 11. Núm. 7. Julio-septiembre. México, D. F. 2006.

Ramírez Ramírez, Agustín (2004) *Régimen Patrimonial de los Datos Clínicos en México*. Revista Lex. Difusión y Análisis. No. 111. Tercera Época. Año VIII. Septiembre 2004. México, D. F.

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Reglamento de Procedimientos para la Atención de Quejas Médicas y Gestión Pericial de la Comisión Nacional de Arbitraje Médico.

Secretaría del Tribunal Europeo de Derechos Humanos. *Convenio para la Protección de los Derechos Humanos de las Libertades Fundamentales. Revisado de conformidad con los Protocolos No. 11 y 14.* Versión en Español. Junio de 2010. Disponible al 24 de noviembre de 2011 en http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf.

La protección de datos personales en materia político - electoral

Jorge Bustillos Roqueñí

Jorge Bustillos Roqueñí

Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, con experiencia en temas de transparencia, rendición de cuentas, desarrollo de políticas públicas, gestión de conflictos y concertación social. En la administración pública se ha desempeñado como Director General de Enlace con el Poder Legislativo en la Secretaría de Medio Ambiente Recursos Naturales y Pesca; Director de Enlace Federal en la Secretaría de Relaciones Exteriores; Asesor de la Dirección de la Capacitación y Formación Profesional en el Instituto Federal Electoral y Secretario Técnico del Consejo de Información Pública del D.F.

Es integrante de las Comisiones de Educación y Vinculación con la Sociedad de la Conferencia Mexicana para el Acceso a la Información Pública (COMAIP). Licenciado en Administración de Empresas por la Universidad Autónoma de México con estudios de Maestría en Psicología Organizacional en el Instituto de Estudios Universitarios. Cuenta con estudios de especialización en transparencia y acceso a la información pública, ecología y desarrollo sustentable, así como en materia de relaciones exteriores.

Es autor de diversos libros y ensayos, entre los que se encuentran la “Transparencia y acceso a la información de los partidos políticos”, “Máxima publicidad y la reserva de información como excepción”, entre otros. Además ha impartido múltiples cursos, conferencias y talleres en materia de transparencia y rendición de cuentas.

Introducción*

Bien sabemos que democracia es mucho más que estar simplemente ante el ejercicio de elección del gobierno de las mayorías; implica, entre otros elementos, estar en la presencia de un concierto de derechos que limitan al poder público respecto de las personas; de derechos que les son intrínsecos y que les garantizan libertades que a su vez posibilitan su participación política y social en un marco de respeto e igualdad.

Hoy estamos ante un escenario en que el Estado debe garantizar una gama amplia de nuevos derechos a los gobernados, de derechos de tercera generación (Pérez Luño 2006, citado por García González 2007), entre los cuales se ha venido posicionado en un lugar cada vez más importante el derecho a la protección de datos personales; esto es así, en parte, debido a los enormes flujos de información y de datos de toda persona que gracias a los avances tecnológicos tienen lugar en nuestra sociedad y al riesgo que encierra su uso y difusión sin consentimiento de los titulares de los mismos y sin un marco normativo que lo regule.

El Estado mismo, es un gran recopilador, ordenador y difusor, en sus diferentes niveles, de datos personales, por lo que es doblemente relevante la observación de las garantías individuales, como el derecho fundamental a la privacidad, y su debido cuidado, por parte de todas las instancias estatales. En México se han dado pasos importantes en esta materia, orientados a salvaguardar este derecho fundamental de las personas. Las reformas que se han llevado a cabo en los últimos años a la Constitución y a diversas leyes dan cuenta de esto.

Sin embargo, este desarrollo normativo no ha agotado las posibilidades de debate y controversia en la materia, más aún, como en muchos de los planos políticos y sociales, han aumentado al incrementarse los escenarios y las posibilidades de confluencia y tensión con otros derechos, particularmente con el derecho de acceso a la información, y con demandas legítimas en el contexto del desarrollo democrático.

* El autor agradece a Víctor García Cruz su apoyo en las tareas de investigación para este artículo.

Con el objetivo de contribuir al desarrollo de criterios interpretativos y enriquecer el debate sobre las posibles tensiones existentes en materia de protección de datos personales y acceso a la información pública en el ámbito electoral, el presente trabajo se estructurará de la siguiente manera: En un primer momento se hará un esbozo de la naturaleza y relevancia que tiene la información que se procesa en el espacio electoral, posteriormente se entra al estudio de las características de los datos personales que recaban los organismos electorales en el ejercicio de sus funciones; para finalmente hacer recuento de un par de casos en los que se refleja precariedad e insuficiencias en los esquemas de gestión y administración de los datos bajo resguardo de un organismo electoral.

Información pública y datos personales en el ámbito electoral

Es justo en el terreno político-electoral, en donde se han puesto de manifiesto importantes debates sobre el carácter dual que puede guardar el gran universo de información y de datos personales que en él se concentran.

Por una parte, tenemos aquellos datos que se acopian con fines propios de la gestión de los procesos electorales y de las funciones de las instituciones electorales y los partidos políticos y que son materia y del interés del escrutinio público; y, por otra, tenemos que dentro de dicho conjunto de datos se encuentran algunos que por su naturaleza solamente deben estar sujetos a la vista de las autoridades en el legítimo ejercicio de sus funciones y debidamente resguardados por estas.

Un ejemplo de esto, lo encontramos en el padrón de militantes y el padrón electoral. Estos son instrumentos registrales en torno a los cuales se debate intensamente sobre los límites de su publicidad y de su confidencialidad.

Ambos encierran información que acreditan la legalidad de los actos registrales de las instituciones electorales, o bien, información útil para fiscalizar el ejercicio de la función pública y da certeza y credibilidad a todos los procesos en materia electoral. Ambos registros

poseen información que se reclama como sujeta al escrutinio público e información de la que se exige su máxima protección.

Es en este contexto que pueden concurrir competencias de los dos derechos fundamentales, a la privacidad y al acceso a lo público. El funcionamiento de los procesos político-electorales requiere que las instituciones electorales y los partidos políticos se alleguen de información diversa para el ejercicio de sus funciones, incluyendo de manera destacada en este conjunto, diversos datos personales de los ciudadanos, necesarios para su ejecución.

La veracidad y legalidad en la organización y disposición de esta información, juega un papel crucial a lo largo de estos procesos. La vigilancia sobre la administración de esta información va mas allá de la tarea de los órganos jurisdiccionales; es una tarea que ocupa además a la sociedad como actor vigilante de la legalidad y transparencia con la que se comportan todos los actores en estos procesos. Y esto lo va a realizar a través del ejercicio y defensa de los derechos de acceso a información pública y de protección de datos personales.

No podemos olvidar que a pesar de los innegables avances en materia democrática ocurridos en nuestro país, aún no se ha dejado atrás por completo la desconfianza de la ciudadanía hacia las instancias involucradas en los procesos político-electorales; desconfianza originada en que hasta hace unos cuantos años, la percepción de las personas de que el voto no era respetado, que las instituciones eran primordialmente ornamentales, que los padrones electorales y de militantes estaban cargados de falsos datos y que el poder era ilegítimo desde su origen.

El respeto al ejercicio del derecho de acceso a información pública y de protección de datos personales, es la mejor apuesta para abonar a la confianza en los procesos electorales. En este escenario nace el interés de establecer el alcance de cada uno de los derechos mencionados, para el mejor resultado en función del interés público y la consolidación democrática, en torno a la gestión y resguardo de la información y de los datos personales en el ámbito político-electoral.

Es sin duda un escenario que exige armonizar las demandas sociales de transparencia en los procesos electorales, con la obligación de

proteger la esfera de intimidad de los distintos actores que directa o indirectamente están inmersos en los procesos mencionados.

Esto nos lleva ahora a revisar la situación en la que se encuentran las instancias electorales, el manejo que hacen de los datos personales y las disposiciones normativas que atienden en esta materia. Igualmente veremos algunos casos emblemáticos del riesgo al que se exponen los datos personales mal protegidos y casos en donde está presente la tensión entre derechos fundamentales.

La protección de datos personales en el ámbito político electoral

A finales del siglo pasado y después de largas controversias y cuestionamientos a algunos procesos comiciales, el Estado mexicano y la sociedad civil orientaron sus esfuerzos hacia la construcción de organismos electorales ciudadanizados, capaces de ofrecer garantías de credibilidad, certidumbre y eficacia a los procesos electorales.

Actualmente, los organismos político-electorales se enfrentan a una multiplicidad de retos, entre los que se encuentra el de mantener la buena marcha en la conducción de los comicios y consolidar la confianza ciudadana en ellos, para lo que les ha sido imprescindible atender tanto al ejercicio transparente de sus funciones, como a la custodia de la información personal que ponen los ciudadanos a su resguardo.

Estas instituciones, en el ejercicio de sus funciones poseen y generan un gran cúmulo de información, entre la que se encuentran inmersos una amplia variedad de datos personales. Por ejemplo, los órganos jurisdiccionales electorales, al resolver controversias electorales y de protección de derechos políticos, pueden allegarse de los padrones de militantes, de donadores y aportantes a los partidos políticos y por supuesto, de los actores involucrados.

En tanto que las autoridades administrativas tiene bajo su resguardo la información contenida en el padrón electoral y en la lista nominal de electores, los cuales contienen datos personales que la ciudadanía proporciona al Registro Federal de Electores (domicilio completo, lugar

y fecha de nacimiento, sexo) quien está obligado normativamente a administrar y resguardar la información a partir del principio de confidencialidad.

En este ámbito de competencia de las autoridades electorales, converge la necesidad de tratar y proteger la información de las personas, con el consentimiento de ellas para otorgar esos datos al órgano electoral para poder participar en los procesos comiciales, en los que intervienen los partidos políticos, tanto para la consulta como para la revisión constante de dichos datos.

Esto refleja la complejidad y relevancia de la información de la que se allegan, administran y resguardan, en el ejercicio de sus funciones así como de la importancia que reviste proteger los datos que le son confiados, mismos que resultan en instrumentos esenciales para la celebración de las elecciones.

En el caso del Distrito Federal, la Ley de Protección de Datos Personales establece una serie de disposiciones encaminadas a garantizar el correcto tratamiento de los datos personales en posesión de las autoridades electorales y los partidos políticos así como la adecuada protección de los mismos.

En su artículo 8, se establece que los sistemas de datos personales en posesión de los entes púbicos, deben inscribirse en el registro habilitado por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF); órgano garante de este derecho fundamental, el cual es en un instrumento que sirve para la tutela de los datos personales que son tratados por las instituciones públicas y los partidos políticos locales.

En ese sentido los siete partidos políticos con registro local han asumido este mandato legal, identificando la importancia que reviste su adecuada protección. De esta manera, a fin de tutelar la integridad y confidencialidad de los datos personales que detentan, ya cuentan con 24 sistemas de datos personales inscritos, de los cuales el 75 % es protegido con nivel de seguridad básico, el 4% con nivel de seguridad medio y el 21% con nivel alto.

Por su parte, el Instituto electoral del Distrito Federal tiene registrados 36 sistemas de datos personales, mientras que el Tribunal electoral del Distrito Federal tiene 17.

En el siguiente cuadro se presenta la información con mayor detalle:

Cuadro 1. Sistemas de datos personales inscritos en el REDSP y nivel de seguridad aplicable.

Ente Obligado	Registrados	Nivel de Seguridad							
		Básico	%	Medio	%	Alto	%	Total	Total %
Convergencia	5	3	60	0	0	2	40	5	100
Instituto Electoral del Distrito Federal	36	18	50	15	42	3	8	36	100
Nueva Alianza	4	3	75	0	0	1	25	4	100
Partido Acción Nacional	5	1	20	1	20	3	60	5	100
Partido de la Revolución Democrática	3	3	100	0	0	0	0	3	100
Partido del Trabajo	3	3	100	0	0	0	0	3	100
Partido Revolucionario Institucional	5	3	60	1	20	1	20	5	100
Partido Verde Ecologista de México	4	4	100	0	0	0	0	4	100
Tribunal Electoral del Distrito Federal	13	2	15	9	69	2	15	13	100
Total	78	40	64	26	17	12	19	78	100

Fuente: Elaboración del autor con base en la información contenida en el Registro Electrónico de Sistemas de Datos Personales (RESDP).

El cumplimiento de identificar y registrar los sistemas de datos personales que tienen las instituciones político-electorales y los partidos en la Ciudad de México, favorece el debido resguardo de la información confidencial contenida en ellos, en el contexto de una tendencia incremental en el ejercicio del derecho de acceso a la información en la materia, misma que en ocasiones condiciona a los entes obligados a actuar en el sentido de satisfacer ambos derechos, sin que se actualice algún tipo de menoscabo a alguno de ellos.

Algunos casos emblemáticos de riesgo

El resguardo y administración segura de los datos personales en el tema político-electoral se ha puesto a prueba e incluso se ha cuestionado abiertamente en sus medidas de seguridad, en varias ocasiones. Ello debido a la complejidad que encierra el manejo de millones de datos personales cuyo ordenamiento y disposición debe de atender las mayores medidas de integridad, seguridad y veracidad, pues es con esta con la que se va a operar el ejercicio democrático de los diferentes procesos electorales. En otras palabras, la implementación de medidas inadecuadas de seguridad ha puesto en riesgo el resguardo y adecuada administración de los datos personales, además de comprometer la confiabilidad de las instituciones electorales ante la ciudadanía. En las siguientes líneas haré referencia a dos casos que son emblemáticos de lo anterior.

IFE - Venta del padrón electoral

En mayo de 2003, a través de publicaciones en diversos medios de comunicación, se reveló que la empresa Choice Point había vendido al gobierno de Estados Unidos una serie de bases de datos con información relacionada con la función registral electoral, desde 2001. De las investigaciones sobre esta situación, se desprendió que una empresa mexicana, Soluciones Mercadológicas en Bases de Datos, había comercializado en 335 mil dólares a Choice Point la base de datos del padrón electoral del Instituto Federal Electoral, en el que se incluía información de 58 millones de ciudadanos mexicanos. La vertiente penal del caso derivó en el ejercicio de la acción penal en contra de los involucrados, por la probable comisión de los delitos

de revelación de secretos, delitos electorales y traición a la patria; sin embargo, al final se les encontró responsables únicamente del delito de revelación de secretos[1].

Este caso nos mostró el potencial de riesgo en el que se encuentran nuestros datos, cuando no existen los protocolos de seguridad en el resguardo y manejo de los mismos, en el desarrollo de los diversos trámites y actividades que de manera cotidiana realizan los tenedores de datos.

Sin duda alguna, los datos personales contenidos en el padrón, por su volumen y detalle, constituyen información sumamente delicada, pero también útil y atractiva para fines comerciales y hasta de seguridad nacional. Por ello, el IFE y los órganos electorales de todo el país, no solamente deben contar con sistemas de seguridad que garanticen el debido resguardo y la confidencialidad de la información acerca de los votantes y de sus funciones sustantivas, sino también deben estar comprometidos con la actualización y revisión continua de sus controles y procedimientos en ese ámbito, particularmente considerando la rápida evolución tecnológica que hace necesario actuar de manera preventiva en cuestiones de seguridad.

El siguiente caso al que se hará referencia, es el de los registros múltiples de una misma persona, con diferentes datos, en el padrón electoral. Es pertinente aclarar que la credencial para votar emitida por el Instituto Federal Electoral se ha convertido en el medio de identificación más importante de nuestro país, por lo que es usada en diferentes trámites oficiales, bancarios y comerciales.

El adecuado tratamiento de los datos personales que sirven de sustento para la emisión de la credencial adquiere particular relevancia, ya que adicionalmente a haberse constituido en el principal medio de identificación en nuestro país, se trata de un documento fundamental para la credibilidad de los procesos comiciales, lo que obliga a la puntual observancia de los principios rectores en materia de protección de datos, en un tema en el que se destaca el principio de Calidad, que exige que los datos recabados sean ciertos y adecuados.

[1] Sobre el caso se puede consultar la siguiente nota de prensa del 17 de diciembre de 2006: http://www.jornada.unam.mx/2006/12/17/index.php?section=politica&article=010n2pol

Registros múltiples de una misma persona en el padrón electoral

El padrón electoral, por su relevancia y centralidad en los procesos electorales, debe ser capaz de dar certidumbre a la ciudadanía en cuanto a su conformación, validez, actualización y seguridad. La posibilidad de que en el padrón electoral existan datos inexactos, incongruentes o de plano falsos pone en riesgo la credibilidad de la totalidad de los procesos electorales, al ser el padrón uno de sus insumos básicos e indispensables.

La laxitud en los controles y requisitos para inscripción en el padrón electoral se puso en evidencia cuando se empezaron a detectar casos en que personas con diferentes nombres, habían obtenido varias credenciales para votar y que habían hecho mal uso de los documentos, tramitando créditos que dejaban sin pagar. Un par de casos paradigmáticos revelaron que dos personas habían tramitado cada una 15 y 16 credenciales para votar, con las cuales defraudaron a múltiples establecimientos comerciales adquiriendo créditos para realizar compras[2]. Si bien en este caso se logró detectar la vulneración a las medidas de seguridad que deben implementarse en la conformación del padrón electoral, es claro que esta circunstancia de multiplicidad en los registros puede tener incidencia en los procesos comiciales; permitiendo eventualmente que una misma persona pudiera votar en más de una ocasión, por ejemplo.

Son conocidos los esfuerzos que el IFE ha puesto en marcha para detectar y sancionar irregularidades como las que se han expuesto, sin embargo, la reseña de los casos refleja la necesidad de la revisión, adecuación y actualización de los protocolos y procedimientos que den a la ciudadanía la certeza sobre la confiabilidad de los datos contenidos en el padrón electoral.

[2] Al respecto véanse los boletines de la PGR 359/08 y 513/08, disponibles respectivamente en: http://www.pgr.gob.mx/prensa/2007/bol08/May/b35908.shtm y http://www.pgr.gob.mx/prensa/2007/bol08/Jun/b51308.shtm

Escenarios de tensión

En el terreno político-electoral es relativamente fácil advertir que se presenten situaciones en las que se advierta la tensión entre el derecho de acceso a la información y el derecho a la protección de datos personales, ello debido al interés público, la certidumbre y legitimidad que se demandan de los procesos electorales, que converge con la necesidad de proteger los datos de las personas.

Se debe resaltar que en estos y otros casos, no es correcto hablar de choque o conflicto de derechos fundamentales, sino de la presencia de una tensión entre ellos. Al respecto, debe decirse que en el ejercicio de los derechos, la idea de límites tajantes e inamovibles entre ellos tampoco es concebible, ya que en la realidad con frecuencia tienen lugar fricciones, roces y encuentros entre derechos; algo que desde ninguna teoría del derecho se puede negar. Para este tipo de situaciones tenemos como salida la ponderación o balance entre los derechos en cuestión, para determinar cuál es el que debe prevalecer (Comanducci, 2005:114); esto es, se deben valorar los derechos que se encuentran en tensión y las particularidades del caso, esto es, como señala Salvador Nava (2011), deben resolverse a partir de un juicio de proporcionalidad o ponderación para establecer los alcances de un derecho frente a otro u otros.

Dos caso de tensión que actualmente son motivo de estudios, criterios, dictámenes y discusiones, son los relacionados con la publicidad de la información sobre los militantes y de las personas que aportan recursos a los partidos políticos. Sobre estos dos temas abundaré en el siguiente punto.

Los datos personales en los padrones de militantes de los partidos políticos

Los padrones de militantes son instrumentos registrales que en extenso contienen información susceptible de ser resguardada del escrutinio público, correspondiente a datos personales, sin embargo, al mismo tiempo contienen datos, que están en la esfera de los datos personales (nombre, sexo, domicilio, ideología, afiliación política)

y si son susceptibles de hacerse del conocimiento público bajo determinadas condiciones, en aras de favorecer la veracidad y la legitimidad de los mismos.

Estos padrones, son sin duda uno de los cuerpos de información más relevantes en poder de los partidos políticos. En ellos se expresa la voluntad de los ciudadanos que deciden adherirse por simpatizar, identificarse o encontrar afinidad en un determinado programa de acción política de un partido.

Para entender de mejor manera el papel de los partidos políticos en nuestro escenario democrático, vale la pena examinar su naturaleza en el contexto de nuestras instituciones político-electorales.

Si bien no podemos señalar que los partidos sean autoridades públicas, tampoco podemos decir que sean simples particulares; en la Constitución se les señala como entidades de interés público, que además de promover la participación del pueblo en la vida democrática, hacen posible el acceso de los ciudadanos al ejercicio del poder público, de acuerdo con los programas, principios e ideas que postulan y mediante el sufragio universal, libre, secreto y directo[3].

Aunado a lo anterior, a partir de su función como actores centrales para la celebración de elecciones y como vías únicas para la postulación de candidatos para los cargos de elección popular, y considerando que reciben financiamiento público para el cumplimiento de sus funciones, los partidos políticos deben ser sujetos al escrutinio público y al mismo tiempo garantes de los datos personales que poseen, atendiendo así a los principios democráticos y jurídicos que rigen la vida política del país.

[3] La fracción I del artículo 41 de la Constitución establece: *Los partidos políticos son entidades de interés público; la ley determinará las normas y requisitos para su registro legal y las formas específicas de su intervención en el proceso electoral. Los partidos políticos nacionales tendrán derecho a participar en las elecciones estatales, municipales y del Distrito Federal.*
Los partidos políticos tienen como fin promover la participación del pueblo en la vida democrática, contribuir a la integración de la representación nacional y como organizaciones de ciudadanos, hacer posible el acceso de éstos al ejercicio del poder público, de acuerdo con los programas, principios e ideas que postulan y mediante el sufragio universal, libre, secreto y directo. Sólo los ciudadanos podrán formar partidos políticos y afiliarse libre e individualmente a ellos; por tanto, quedan prohibidas la intervención de organizaciones gremiales o con objeto social diferente en la creación de partidos y cualquier forma de afiliación corporativa (.)

En este terreno de concurrencia de ambos derechos, se debe advertir que los ciudadanos que deciden adherirse formalmente a un instituto político, adquieren características particulares relacionadas de manera estrecha con el funcionamiento de la institucionalidad democrática. En este sentido, los militantes se hacen sujetos de derechos y obligaciones vinculados con los partidos, como entidades de interés público y sustento con la vida democrática del país. Esta situación hace que la información que poseen los partidos políticos respecto a sus militantes se convierta en un elemento que da garantía del cumplimiento de los principios de legalidad y certeza jurídica implícitos en el funcionamiento político de nuestro país; al mismo tiempo que constituye un conjunto de datos susceptibles de ser protegidos.

En este escenario de convergencia entre los principios de máxima publicidad y máxima protección, han tenido lugar diversas controversias ante los órganos jurisdiccionales, de las que, tanto a nivel local como federal, se han emitido resoluciones al respecto, mismas que, a partir de argumentaciones que coinciden esencialmente, han derivado en soluciones a la tensión en la que entran estos derechos, ordenando la publicidad parcial de elementos contenidos en los referidos padrones como son el nombre, entidad federativa, sexo y municipio, sin vulnerar la esfera de derechos de los particulares y al mismo tiempo salvaguardando los principios de transparencia y acceso a la información. Esto es, resoluciones que han definido los límites y los alcances de ambos derechos fundamentales.

A manera de ejemplo podemos referir el caso del Tribunal Electoral de la Federación, al resolver el expediente SUP-RAP-28/2008, sobre la impugnación que hiciera el Partido de la Revolución Democrática ante el requerimiento que le dirigió el Órgano Garante de la Transparencia y el Acceso a la Información en el IFE, para que entregara una versión pública y legible de su padrón de militantes, para satisfacer una solicitud de acceso a la información[4].

Al resolver la cuestión, el Órgano Jurisdiccional señaló que al entregar el padrón de afiliados al partido, incluyendo nombres y apellidos, así como la Entidad Federativa a la que pertenecían, no se afectaba el

[4] La sentencia SUP-RAP-28/2008 se emitió el 5 de marzo de 2008 por la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación.

principio de confidencialidad respecto del domicilio, y sí se tutelaba el derecho de acceso a la información:

> (...) en el caso se garantiza la eficacia conjunta de los derechos fundamentales a la información y a la intimidad, porque permite su coexistencia y eficacia plena, al permitir que un ciudadano ejerza el derecho a ser informado del padrón de integrantes de un partido en la forma pedida, sin que se afecte la privacidad o intimidad de los afiliados, en relación a que se conozca su domicilio, precisamente, porque, como se indicó, dar a conocer la entidad federativa del domicilio de una persona, no implica, por sí, revelar éste.

En este caso, se debe resaltar que la resolución del Tribunal dio publicidad a una serie de datos que abonan a la legalidad y certeza en la integración de un partido político sin que por ello se deba entender que se afecta la confidencialidad de sus datos.

Otro caso relevante es la resolución dada a la impugnación del Partido Revolucionario Institucional con respecto del acuerdo del Consejo General del IFE, por el que se reformó su Reglamento en materia de Transparencia y Acceso a la Información Pública (SUP-RAP-137/2008[5]), esto porque a consideración del partido, con dicho acuerdo se vulneraban los principios de reserva de ley, jerarquía normativa y legalidad, al incluir los padrones de afiliados y militantes de los partidos políticos dentro de la información pública que debe difundir el citado organismo[6].

Al resolver el asunto, el Tribunal Electoral nuevamente refirió que si bien el nombre de los ciudadanos constituye un dato personal; su difusión de manera aislada, no revela ningún otro dato personal que

[5] La sentencia SUP-RAP-137-2008 fue emitida el 18 de septiembre de 2008 para resolver el recurso de apelación presentado por el Partido Revolucionario Institucional, en contra de la aprobación por parte del Consejo General del IFE del Acuerdo G307/2008, por el cual se reformó el Reglamento del propio Instituto en materia de Transparencia y Acceso a la Información Pública.

[6] El acuerdo impugnado establecía en el Reglamento de Transparencia del IFE , en su artículo 5, fracción XXXIX, como obligación de transparencia del Instituto publicar ( ) *El padrón de afiliados o militantes de los partidos políticos, que deberá contener, al menos, el nombre completo del afiliado o militante y la entidad federativa a la que pertenezca.*

afecte la vida privada o intimidad de un individuo, por lo que no tiene el carácter de información confidencial y por lo tanto, no se requiere del consentimiento expreso de su titular para su publicación. El Tribunal Electoral remarcó la importancia de dar acceso a la información de los padrones de militantes, señalando que "… no debe perderse de vista que la difusión de la afiliación partidista lejos de producir una afectación a la vida privada de los militantes, se traduce en un beneficio a su propio interés y la sociedad en general, dado que con esto es posible identificar casos de doble afiliación o transfuguismo político, de tal suerte que, debe garantizarse la transparencia de los partidos políticos en un aspecto medular como es su militancia.

Es evidente que la materia político-electoral requiere de garantías de credibilidad, objetividad y transparencia, para ello, es relevante que se pueda verificar que no existan casos de personas que estén consideradas como militantes al mismo tiempo en distintos partidos, situación a todas luces contraria a la legalidad, dado que es con el padrón de militantes que el partido político acredita un grado de representatividad social necesario para obtener y mantener su registro como tal; de igual manera, conocer la trayectoria de militancia partidista de una persona que potencialmente puede llegar a ocupar un cargo de elección popular, al transparentarse su movilidad entre distintos partidos, sin duda favorece la toma de decisiones informada por parte de la ciudadanía a la hora de expresar su voluntad en las urnas.

En el caso reseñado, el Tribunal resolvió de tal manera que, sin vulnerar la esfera de privacidad de los militantes, favoreció las garantías mencionadas, haciendo prevalecer además el interés general en el asunto, favoreciendo la certidumbre que debe prevalecer en la integración de los padrones de militantes, al establecer un alcance de fiscalización sobre ellos en aras de evitar los padrones inflados o la doble militancia en los partidos políticos.

Otro asunto relacionado es el SUP-JDC-8/20097, en el que un ciudadano impugnó la resolución del el Órgano Garante de la Transparencia y Acceso a la Información del IFE, con la que se confirmaba la respuesta emitida por el Partido Acción Nacional a una

[7] La resolución SUP-JDC-8/2009, fue emitida por la Sala Superior del Tribunal electoral del Poder Judicial de la Federación, el 28 de enero de 2009.

solicitud de información relativa al padrón de militantes, en la que se negaba el acceso a la información sobre el sexo, la fecha de ingreso como miembro activo y el municipio en el que se inscribieron los afiliados.

En este caso los integrantes de la Sala Superior del Tribunal tuvieron como errado que los datos sobre el sexo, fecha de ingreso como miembro activo y municipio de cada ciudadano afiliado al PAN, fueran considerados datos personales imposibles de ser proporcionados, por lo que ordenó a la autoridad recurrida que dictara otro acuerdo, en el que se estableciera que los datos mencionados no son personales, al no afectar su difusión el principio de confidencialidad y, por tanto, el derecho a la intimidad.

Como distintivo de este caso tenemos el dato correspondiente a "sexo" del afiliado, del cual se razonó lo siguiente:

La experiencia enseña que culturalmente este aspecto de la vida personal, por lo general, es público o socializable en la medida en que existen aspectos físicos que ordinariamente lo revelan y que no se ocultan en las relaciones sociales.

Incluso, se trata de un aspecto que puede inferirse a partir de los nombres propios de los sujetos, salvo excepciones en los que estos se usan neutralmente.

Se advierte de la argumentación del Tribunal un razonamiento en torno a las razones por las cuales no se vulnera la esfera de protección de los datos de las personas al revelarse el sexo de los afiliados a un partido político, en tanto que se atiende a un rasgo que de suyo es evidente e incluso susceptible de ser inferido a partir del nombre del militante, lo que lleva implícita su naturaleza pública. En los asuntos que se han reseñado, los magistrados del Tribunal Electoral atienden a la necesaria ponderación de derechos, congruente con la interpretación del derecho de acceso a la información, en la cual debe prevalecer el principio de máxima publicidad.[8]

[8] A partir de los tres casos referidos, en marzo de 2009 la Sala Superior estableció la jurisprudencia 4/2009: INFORMACION PUBLICA SE CONSIDERA COMO TAL LA CONCERNIENTE AL NOMBRE PROPIO RELACIONADO CON LA ENTIDAD FEDERATIVA O MUNICIPIO DE LOS MIEMBROS DE UN PARTIDO POLÍTICO.

Un aspecto notable del SUP-RAP-28/2008, es el razonamiento que en la resolución se hace sobre la relación entre ideología y militancia en un partido político. Al resolverse dicho expediente, se estableció que cuando un ciudadano se afilia a un determinado partido político, él asume diversos derechos y obligaciones, entre otros, que su militancia sea pública y transparente: (…) a partir del momento en que un ciudadano se afilia formalmente a determinado partido político, que constituye una entidad de interés público, la militancia de éste y, por ende, la ideología política que ello supone, se traslada de lo privado a lo público, como consecuencia de su voluntad externada de querer pertenecer a una entidad de interés público.

En este contexto, es válido mencionar que incluso, si un ciudadano al afiliarse a un partido político tiene como derecho, la posibilidad de ser postulado a algún cargo de elección popular, esto lo distingue del común de personas y por ende la publicidad de su militancia es un aspecto que no vulnera su privacidad.

En el ámbito local, el InfoDF atendió un recurso de revisión derivado de la clasificación como información confidencial que hizo un partido político, respecto a su padrón de militantes, ante una solicitud de información en la que básicamente se le requería pronunciarse sobre si eran militantes un conjunto de 63 personas.

En armonía con las líneas argumentativas en que ha resuelto la autoridad jurisdiccional electoral, para el Pleno del InfoDF revelar la afiliación a un partido político no es violatorio de la protección de los datos personales de las personas, en tanto que se debe atender a los partidos políticos como entidades de interés público, así como a la libre voluntad del ciudadano de adherirse a ellos como militante, lo que le genera derechos y obligaciones específicas. Al respecto, en la resolución al RR. 1448/2011[9] se señaló (…) al momento de que un ciudadano decide afiliarse a un partido político, asume los derechos y obligaciones correlativas, entre otros que su militancia sea transparente, en tal virtud, su afiliación partidista no se mantiene en secrecía, pues constituye una carga inherente a su decisión de pertenecer formal y

[9] El expediente RR 1448/2011 fue resuelto por mayoría de votos del Pleno del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, el 1 de noviembre de 2011, atendiendo a la inconformidad de un solicitante de información con la respuesta que le otorgó el Partido Revolucionario Institucional.

activamente a un partido político. Esta argumentación se refuerza si se considera que los partidos y sus militantes, por su propia naturaleza, tienden a la participación en el espacio público, en aras de comunicar sus postulados y programas, de captar más afiliados y de dar apoyo a sus candidatos en épocas electorales. De esta manera la decisión de militar en un partido conlleva también implícitamente una voluntad que se materializa con frecuencia en expresiones públicas de adhesión y apoyo en mítines, en eventos partidistas e incluso en funciones de representantes en procesos electorales.

Asimismo se señala en dicha resolución que (…) es claro que ninguna persona está obligada a integrarse a un partido político, por lo tanto, el acto de afiliación es voluntario y se encuentra regulado por una serie de disposiciones normativas propias de los institutos políticos, las cuales son del conocimiento de los ciudadanos que pretenden afiliarse, de tal forma que en dicho acto, el particular expone públicamente su afinidad ideológica con un partido político concreto.

A partir de estos razonamientos, se reitera la naturaleza pública del acto de afiliación a un partido político, en función de la voluntad para llevarlo a cabo y del carácter de los partidos políticos como instituciones de interés público; acto que sujeta al militante a diversas obligaciones y que le dota de derechos al mismo tiempo.

Abundando respecto al padrón de militantes, podemos señalar que existen disposiciones normativas que hacen que su publicidad se convierta en un factor de utilidad para verificar la legalidad de su cumplimiento, en tanto que, por ejemplo, el Código Federal de Instituciones y Procedimientos Electorales (COFIPE) en su artículo 24, establece como requisito para la constitución de partidos políticos un cierto número de afiliados, así como de entidades federativas en las que se tenga presencia y/o el número de distritos electorales, mismos que deben ser mantenidos y acreditados para conservar el registro correspondiente. La publicidad de los padrones de militantes permiten a las autoridades y partidos políticos verificar con datos ciertos el cumplimiento de este requisito.

Como lo hemos mencionado anteriormente, la decisión de un individuo de participar políticamente mediante la afiliación a un partido, es expresión de su voluntad de adherirse a un determinado programa

político, y conlleva la posibilidad de participación en actividades públicas en diferentes planos, como lo son las expresiones públicas de adhesión, apoyo en actividades externas y presencia en actos de campaña; de ahí que no sea posible darle un carácter de secretos a los datos relativos a la afiliación política.

Quiero hacer en este punto una breve reflexión sobre la relación entre la noción de ideología y su relación con la militancia en un partido político.

Si bien en las disposiciones legales en materia de protección de datos se enuncia a la ideología de las personas como información susceptible de ser protegida, considero que cabría preguntarnos si el dato de pertenencia a un partido político podría considerarse dentro de esa esfera. Habría que considerar que los partidos políticos enuncian una serie de postulados en sus programas y documentos básicos, que sin embargo no constituyen marcos absolutos y totales que puedan abarcar de manera íntegra la ideología de un individuo, sino cierta empatía o correspondencia con parte de la misma. Incluso se debe partir de las condiciones específicas de nuestro país en la cuestión; sin pretender abundar en el marco sociológico de la militancia partidista, si se puede apuntar a que en ocasiones la decisión de afiliarse a un partido político obedece a circunstancias coyunturales de conveniencia que no necesariamente se vinculan con la cuestión ideológica.

Avances o retrocesos en las preferencias electorales, propuestas de acción vinculadas a temas emergentes, conveniencia personal o comunitaria, son solamente algunos de los factores que pueden influir en la decisión de sumarse formalmente a la membresía de un instituto político.

En México la adhesión partidista en alguna época era incluso una condicionante expresa para laborar en ciertos ámbitos; algo que afortunadamente se ha venido superando.

Sin embargo, el punto central de la argumentación es la necesidad de pensar a la militancia como un dato que sí puede hacerse del conocimiento público, en tanto que su divulgación no puede constituir un perjuicio a la intimidad de las personas o a su vida ciudadana y sí constituye un factor a favor de la consolidación democrática.

Los datos de donadores de recursos a los partidos políticos

Es bien sabido que la manera como las personas decidan hacer uso de su patrimonio es información que pertenece a la esfera de su vida privada y que por ende debe ser tutelada en aras de evitar injerencias sobre ella. Sin embargo, en el caso de las aportaciones que se hacen a los partidos políticos, esta información debe hacerse pública y atenerse a la observancia de una norma que ve por el interés público y los principios de certeza jurídica y legalidad que deben primar en la cuestión político-electoral.

Como es conocido, los partidos políticos operan fundamentalmente con la provisión de recursos públicos por parte del Estado, esto derivado de la disposición constitucional que estable la prevalencia del financiamiento público sobre el privado[10]. Sin embargo, también se dispone la posibilidad de que los partidos políticos se alleguen recursos a través de las aportaciones militantes y simpatizantes, siempre dentro del marco de limitaciones que se establece en las leyes adjetivas y sujetos a una fiscalización detallada.

Ante esto, revelar los nombres de las personas que aportan recursos a los partidos políticos no puede entenderse como una indebida difusión de datos personales, sino como una acción orientada a dar certeza a la ciudadanía y a auxiliar a las autoridades a verificar que montos y aportantes no rebasan los límites y se transgreden las limitaciones establecidos en la legislación. Esto en convivencia armónica con la idea de la transparencia como un elemento fundamental en el carácter de los partidos políticos como entidades sujetas a un régimen de rendición de cuentas, en tanto que son instituciones de interés público.

En este tema, la transparencia como herramienta de fiscalización institucional y social sobre las vías y métodos por los cuales los partidos políticos obtienen financiamiento, representan barreras importantes para evitar el riesgo de su captura y manipulación, y al mismo

[10] Al respecto, el artículo 41 de la Constitución, en el primer párrafo de la fracción II, establece: *La ley garantizará que los partidos políticos nacionales cuenten de manera equitativa con elementos para llevar a cabo sus actividades y señalará las reglas a que se sujetará el financiamiento de los propios partidos y sus campañas electorales, debiendo garantizar que los recursos públicos prevalezcan sobre los de origen privado.*

tiempo constituye una respuesta a los muchos años de suspicacias y sospechas que en este tema prevalecieron en el México de la transición a la democracia.

En este sentido, existen diversas disposiciones legales que, al regular el financiamiento privado a los partidos políticos, hacen necesaria la transparencia en ese rubro, para que el funcionamiento de esas instituciones se inscriba en el marco de la legalidad, de la certeza y de la rendición de cuentas.

Al respecto, el COFIPE establece, dentro de su Capítulo Segundo, las restricciones que en materia de financiamiento privado deben regir, entre las cuales se encuentra la prohibición de recibir recursos por parte de los poderes del Estado, de las dependencias y paraestatales, de personas físicas y morales extranjeras, organizaciones internacionales y religiosas, así como de ministros de culto, personas que vivan o trabajen en el extranjero y empresas mercantiles. Por su parte, el Código de Instituciones y Procedimientos Electorales del Distrito Federal establece limitaciones en términos muy similares, añadiendo la prohibición a los partidos de recibir financiamiento de las personas morales mexicanas de cualquier naturaleza y de personas no identificadas, con excepción de las obtenidas mediante colectas realizadas en mítines o en la vía pública.

Estas disposiciones normativas nos permiten reiterar la importancia de poder conocer de manera puntual, la relación de personas, tanto físicas como morales, que aportan recursos en moneda o en especie a los partidos políticos. Esto además de ayudar a la verificación del cumplimiento de las diversas disposiciones que he referido, sin duda también contribuye a evitar el desencanto democrático que acontece cuando tienen lugar malas prácticas por parte de los actores políticos.

En este contexto, es pertinente traer a colación el expediente RR. 724/2008, resuelto por el Pleno del InfoDF, mismo que resolvió sobre la omisión del Partido Revolucionario Institucional en el Distrito Federal en responder a una solicitud de acceso a la información, en la cual, entre otros planteamientos, se le requirió la información relativa al "desglose de aportaciones" de simpatizantes y militantes. Una vez analizado el marco normativo correspondiente, el InfoDF determinó ordenar al partido político la entrega de la información solicitada,

considerando, entre otros aspectos, que la misma era información pública que contribuye a la transparencia y rendición de cuentas.[11]

No se debe perder de vista que la actual coyuntura nacional demanda una estricta vigilancia en el origen de los recursos, en previsión a que dinero de origen dudoso pudiera infiltrarse en las finanzas de los partidos políticos. Como señala José Woldenberg (2002:337), la fiscalización no puede entenderse como una afrenta a los partidos políticos, sino como un ejercicio que legitima y fortalece la competencia democrática en el sistema de partidos.

Conclusiones

La protección de datos personales es un tema de la mayor importancia en la materia político-electoral. Sin embargo, la tutela de este derecho fundamental puede armonizarse adecuadamente con la garantía del funcionamiento de los procesos e instituciones electorales a partir de las ideas de transparencia y rendición de cuentas.

La protección de datos personales en ningún supuesto se puede convertir en un obstáculo para la confiabilidad, la certidumbre y la confianza ciudadana en las elecciones y en la actuación de los partidos políticos; por el contrario, tal como lo hemos visto, puede constituirse en un elemento que da evidencia de que las instituciones se conducen en apego a la ley y que los procesos electorales son realizados en condiciones de legalidad.

La venta del padrón electoral y las duplicidades en los registros del mismo, son casos que deben servir como advertencia sobre la necesidad de construir de manera proactiva, sistemas de salvaguarda y gestión de los datos personales que den garantía del cumplimiento de los principios rectores en la materia, establecidos tanto en la normativa federal como en la local.

[11] El expediente RR. 724/2008, fue resuelto por unanimidad de votos en lo general, incluyendo lo relativo a las aportaciones de simpatizantes y militantes, por el Pleno del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, el 1 de noviembre de 2011.

La convergencia de la protección de datos personales y la transparencia en el terreno político electoral tiene que ser una fortaleza de nuestro sistema democrático, que en conjunto den garantía del cumplimiento cabal de las disposiciones legales y constitucionales en la materia, así como del procesamiento veraz y confiable de la voluntad ciudadana expresada en las urnas. La historia de la consolidación democrática en nuestro país exige la armonización de la publicidad y la salvaguarda de los datos personales, la desconfianza generada por muchos años de malos manejos en los padrones de militantes, del desaseo en los procesos electorales. Para la vida democrática de nuestro país, los espacios en los que se permitan restricciones al acceso a la información tienen que ser reducidos al máximo, en aras del fortalecimiento de los procesos de gobernabilidad democrática y de su credibilidad. Las instituciones y los actores de la materia político electoral son sin duda alguna elementos centrales de la democracia y por tanto deben ser sujetos de los extremos de publicidad y privacidad, siempre teniendo claro que el conjunto de elementos que componen la vida privada de las personas debe quedar al margen del escrutinio público. Como señalan Ackerman y Ayres (2008:287) sobre el ideal democrático: éste está construido sobre el principio de responsabilidad pública, y en general, no puede haber rendición de cuentas sin grandes cantidades de información. Por ello, la obligación de los partidos políticos y de las instituciones político-electorales de informar de manera veraz, oportuna y detallada sobre su funcionamiento y acciones, siempre garantizando la protección de los datos personales en su poder, abona a favor de una ciudadanía con más herramientas y con más poder para ejercer sus derechos.

Referencias

Ackerman, Bruce y Ayres, Ian, (2008) *Transparencia y financiamiento de campañas políticas*. En Ackerman, John, coord., 2008. *Más allá del acceso a la información. Transparencia, rendición de cuentas y estado de derecho*, México: Siglo XXI, IIJ-UNAM.

Comanducci, Paolo, (2005) *Problemas de compatibilidad entre derechos fundamentales*.

Carbonell, Miguel y Salazar Pedro, eds. 2005. *Garantismo, Estudios sobre el pensamiento jurídico de Luigi Ferrajoli*. Madrid: Trotta, IIJ-UNAM.

Constitución Política de los Estados Unidos Mexicanos.

Código Federal de Instituciones y Procedimientos Electorales.

Código de Instituciones y Procedimientos Electorales del Distrito Federal.

García González, Aristeo, (2007) *La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. Boletín Mexicano de Derecho Comparado*, No. 120, pp. 743-778.

Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Ley de Protección de Datos Personales para el Distrito Federal.

Nava, Salvador O., s.f., *Colisión de derechos fundamentales: Acceso a la información y protección de datos personas desde la perspectiva de la jurisdicción electoral*. [en línea] Disponible al 27 de noviembre de 2011 en http://www2.scjn.gob.mx/red/IVTransparencia/Docs/Materiales/Presentaci%C3%B3n%20Magdo%20%20Nava%20Gomar.pdf,

Pérez Nuño, Antonio Enrique (2006) *La tercera generación de derechos humanos*, Navarra: Aranzadi.

Procuraduría General de la República. Boletín 359/08, disponible al 12 de diciembre de 2011 en: http://www.pgr.gob.mx/prensa/2007/bol08/May/b35908.shtm.

Procuraduría General de la República. Boletín 513/08, disponible al 12 de diciembre de 2011 en: http://www.pgr.gob.mx/prensa/2007/bol08/Jun/b51308.shtm.

Woldenberg, José (2002) *La construcción de la democracia*, México: Plaza y Janés.

Sentencia del Tribunal Electoral del Poder Judicial de la Federación del expediente SUP-RAP-28/2008, del 5 de marzo de 2008.

Sentencia del Tribunal Electoral del Poder Judicial de la Federación del expediente SUP-RAP-137/2008, del 18 de septiembre de 2008.

Sentencia del Tribunal Electoral del Poder Judicial de la Federación del expediente SUP-JDC-8/2009, del 28 de enero de 2009.

Resolución del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, del expediente RR. 1448/2011, del 1 de noviembre de 2011.

Protección de datos personales en los programas sociales

Pablo Yanes Rizo

Alejandro López Mercado

Rocío Aguilar Solache

Pablo Yanes Rizo

Director General del Consejo de Evaluación del Desarrollo Social del Distrito Federal. En la administración pública se ha desempeñado como Coordinador de Asesores de la Secretaría de Desarrollo Social del Gobierno del Distrito Federal; Director General de Equidad y Desarrollo Social del Gobierno del Distrito Federal y como Director de Atención a Indígenas y Director de Atención a Personas con Discapacidad, Personas Adultas Mayores, Indígenas y Minorías en la misma. También como Subdirector de Antropología Jurídica del Instituto Nacional Indigenista.

Licenciado en Economía por la Facultad de Economía de la UNAM. Maestro en Gobierno y Asuntos Públicos por la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México. (UNAM). Diplomado en Políticas Públicas y Perspectiva de Género por la Facultad Latinoamericana de Ciencias Sociales. Diplomado en Políticas Sociales Urbanas por el Instituto de Investigaciones Sociales de la UNAM. Ha sido ponente y conferencista en diversos cursos, diplomados, seminarios y congresos nacionales e internacionales.

Fue Presidente de la Reunión Mundial de Expertos sobre Ciudades, Migración y Pueblos Indígenas, organizada por la ONU y celebrada en la sede de CEPAL en Santiago de Chile. Consultor de la ONU-Hábitat y el Alto Comisionado de Naciones Unidas para los Derechos Humanos sobre políticas y pueblos indígenas en ciudades. Miembro de la Basic Income Earth Network (BIEN). Presidente de la Asociación Civil Ingreso Ciudadano Universal-México. Integrante del Comité Organizador del Foro Social Mundial 2008 en la Ciudad de México. Integrante de la Red de Investigadores en Gobiernos Locales (IGLOM). Coordinador y coeditor de diversos libros sobre derechos indígenas y política social.

Alejandro López Mercado

Es Licenciado en Antropología Social por la Escuela Nacional de Antropología e Historia. Dentro de su experiencia en la Administración Pública se ha desempeñado como JUD de Atención a Comunidades Étnicas, en la Secretaría de Desarrollo Rural y Equidad para las Comunidades del Distrito Federal; Director de Atención a Población Indígena; Subdirector de Atención a Población Indígena y Minorías, en la Secretaría de Desarrollo Social del Distrito Federal; Subcoordinador del Programa de Apoyo al Registro Civil para Población Indígena y Subdirector de Apoyo a Organizaciones Civiles en el Instituto Nacional Indigenista, entre otros cargos. Actualmente es Subdirector de Planeación del Consejo de Evaluación del Desarrollo Social del DF. Ha impartido diversas ponencias y talleres en distintas instituciones académicas. También ha participado como asesor y evaluador de becarios indígenas de liderazgo, en la Fundación Macarthur, y como profesor de asignatura impartió la cátedra Historia de México de México, Historia de la Cultura Occidental y Métodos de Investigación a nivel medio superior.

Rocío Aguilar Solache

Es Licenciada en Derecho por la Universidad del Valle de México. Actualmente se desempeña como Subdirectora de Información Pública en la Secretaría de Desarrollo Social del Distrito Federal. Ha sido Jefa de Unidad Departamental de Asuntos Jurídicos y Responsable de la Oficina de Información Pública de la Secretaría de Desarrollo Social del Distrito Federal; Enlace en la Dirección General del Centro de Control de Confianza de la Secretaría de Seguridad Pública del Distrito Federal; Representante del Jefe de Gobierno del Distrito Federal en la Coordinación Territorial de Seguridad y Procuración de Justicia Gustavo A. Madero-4 "Quiroga".

Ha participado en los siguientes seminarios y diplomados: Seminario Internacional: "Acceso a la Información y Protección de Datos Personales: Dos Derechos en un Mismo Rostro" Universidad Nacional Autónoma de México, Instituto Federal de Acceso a la Información Pública, Comisión de Derechos Humanos del Distrito Federal y el Instituto de Acceso a la Información Pública en el Distrito Federal; Seminario Internacional: "Hacia una Nueva Generación de la Transparencia" Universidad Nacional Autónoma de México, Instituto Federal de Acceso a la Información Pública, Comisión de Derechos Humanos del Distrito Federal y el Instituto de Acceso a la Información Pública en el Distrito Federal; Seminario Internacional: "Transparencia en las políticas económicas y sociales" Universidad Nacional Autónoma de México, Instituto Federal de Acceso a la Información Pública, Comisión de Derechos Humanos del Distrito Federal, FUNDAR y el Instituto de Acceso a la Información Pública en el Distrito Federal; Curso "Ley de Transparencia y Acceso a la Información Pública del Distrito Federal" Instituto de Acceso a la Información Pública en el Distrito Federal; Taller Nacional, "Tecnologías de la Información y el Aseguramiento de Datos Personales en el Sector Público Mexicano" Asociación Civil. Política Digital.

Introducción

El presente artículo hace un repaso de las implicaciones que supone la protección de datos personales de los beneficiarios de los programas sociales, y las contradicciones que surgen con el derecho de acceso a la información pública. Para ello se hace una revisión de la normatividad aplicable en esas materias y un somero análisis de su correlación y la problemática que enfrentan las instituciones públicas en la construcción de los padrones de los programas sociales, y se da cuenta de los retos y rezagos que todavía existen en este rubro. Finalmente se hace un análisis de las interrelaciones que existen en los sistemas de datos personales de los programas sociales mediante instrumentos físicos y electrónicos, que aunque son los menos desarrollados hasta ahora, es hacia donde necesariamente se tienen que encaminar las instituciones para garantizar la protección de los datos de los beneficiarios de programas y el cumplimiento de las obligaciones de transparencia. Por ello, se enuncian algunos de los desafíos y ventajas que supone la conformación de un Sistema Único de Padrones de beneficiarios de Programas Sociales.

El supuesto dilema entre la protección de programas sociales y la protección de los datos personales de los beneficiarios

Desde hace varios años era, y sigue siendo, una demanda recurrente de diversos actores sociales y políticos la protección de programas para evitar su uso electoral en todos los niveles de gobierno en México. Por ello surgieron diversas iniciativas y modificaciones legislativas, que aunque se hicieron con más de una década de retraso con relación a las directrices de las Naciones Unidas,[1] dieron como resultado, a nivel nacional, la publicación en junio de 2002 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y en julio de 2007 se publica la reforma constitucional que incorpora el acceso a la información como un derecho fundamental. Incluso el Programa de Naciones Unidas para el Desarrollo reconoció el Proyecto

[1] La Directrices para la regulación de los archivos de datos personales informatizados de las Naciones Unidas fueron adoptadas mediante la resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

de Protección de Programas Sociales Federales (PNUD, 2007:3). En el Distrito Federal también se inició con la adopción de una serie de medidas para proteger los programas sociales que ejecuta la Administración Pública local, entre las que destacan la reforma a la Ley de Desarrollo Social para el Distrito Federal, de mayo de 2005, que incluyó al principio de exigibilidad, así como la prohibición expresa de utilizar los padrones de beneficiarios de los programas sociales con propósitos de proselitismo político, religioso o comercial, y el uso de los programas con fines políticos, electorales, de lucro y otros distintos a los establecidos en la ley, estableciendo que quien haga uso indebido de los recursos de los programas será sancionado. Asimismo, se publicó en marzo de 2008 la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF).Sin embargo, muy pronto se vio que no bastaba la sola protección de los programas sociales, sino que había que avanzar en la protección de los datos personales contenidos en los programas sociales.[2] A decir de diversos actores políticos, existe cierta opacidad en lo que se refiere a la publicación de los padrones de beneficiarios de programas sociales de todos los niveles de gobierno. En el caso del Distrito Federal, algunos diputados y diputadas han señalado en diversos medios de comunicación que los padrones de beneficiarios de los programas sociales "*no dicen nada*", y que incluso los entes públicos se escudan en la Ley de Protección de Datos Personales para el DF, a objeto de no publicar la información completa de dichos padrones. Esta percepción tiene su fundamento en diferentes valoraciones y evaluaciones, dando lugar a un falso dilema entre la obligación de publicar los padrones de beneficiarios de programas sociales y la obligación de las autoridades (y el derecho de los ciudadanos) de proteger los datos personales de los beneficiarios. Por un lado, según datos del InfoDF en los años que van desde 2008 hasta el primer semestre de 2011, la información pública de oficio de la fracción XXI del artículo 14 de la LTAIPDF, que se refiere la publicación de los padrones de las personas beneficiarias de los programas de apoyo o subsidio, ha sido la que más baja calificación ha obtenido en las evaluaciones anuales del propio instituto, lo cual quiere decir que es la parte de la información pública en la que más se incumple.

[2] En ese sentido en junio de 2009 se reformó la constitución para incorporar el derecho de toda persona a la protección de sus datos. Antes de esta reforma el Distrito Federal había promulgado en octubre de 2008 la Ley de Protección de Datos Personales para el DF.

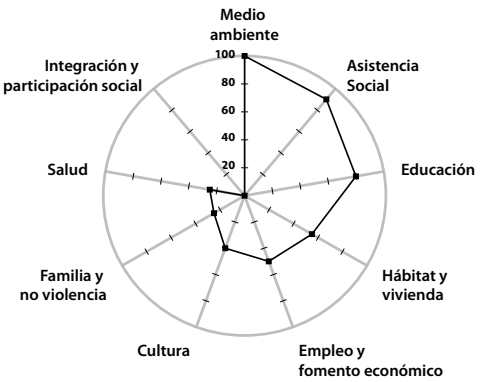
Cuadro 1. Calificación a los portales de transparencia por fracciones del art. 14.

Fracción	Tema	Entes a los que les aplica la fracción	Evaluación-Diagnóstico 2008	Evaluación 2009	1ª Evaluación 2010	2ª Evaluación 2010	1ª Evaluación 2011	Diferencia 1ª Ev'11 y 2ª Ev'10
Fracción XX	Servicios y programas	103	64	74.8	77.9	89.7	88.1	**-1.6**
Fracción X	Presupuesto asignado y ejecución	103	55.4	70	75.8	90.8	87.6	**-3.2**
Fracción XXII	Convocatorias y montos entregados	103	59.1	75.2	79.1	88.8	87.2	**-1.6**
Fracción XXV	Información financiera	103	66.8	78.2	73.2	87.9	86.9	**-1**
Fracción XIX	Informes y calendario de publicación	103	60.7	80.8	72.5	89.1	86.1	**-3**
Fracción XXVII	Adjudicaciones, invitaciones y licitaciones	103	46.8	69.6	66.6	85.3	85.4	**0.1**
Fracción III	Indicadores de gestión	103	69.3	82.6	76.8	90.9	85.3	**-5.6**
Fracción XVII	Convenios y contratos	103	59.8	76.4	72.5	90.5	84.8	**-5.7**
Fracción XXIV	Programas operativos anuales	103	73.9	79.1	80.3	91.3	84.3	**-7**
Fracción XIII	Instrumentos archivísticos	103	72	71.1	67.9	82.4	82.5	**0.1**
Fracción XVIII	Concesiones, licencias, permisos y autorizaciones	33	59.5	71.6	64.9	88.5	76.7	**-11.8**
Fracción XXI	Programas de apoyo o subsidio	49	29.6	54.2	54.9	77.7	70.4	**-7.3**
Índice de los Criterios Sustantivos del Artículo 14			**68.8**	**81.8**	**78**	**91.3**	**89**	**-2.3**

Fuente: InfoDF (2011).

Por su parte, en los resultados de la Evaluación de los Programas y Políticas Sociales en el Distrito Federal, realizada por la Facultad de Economía de la UNAM, se consigna que en el año 2009 "*sólo 36 de los 70 programas evaluados contaron con padrón de beneficiarios hechos públicos*"[3] y lo ilustran con la siguiente gráfica.

Gráfica 1. Programas que cuentan con padrón de beneficiarios.



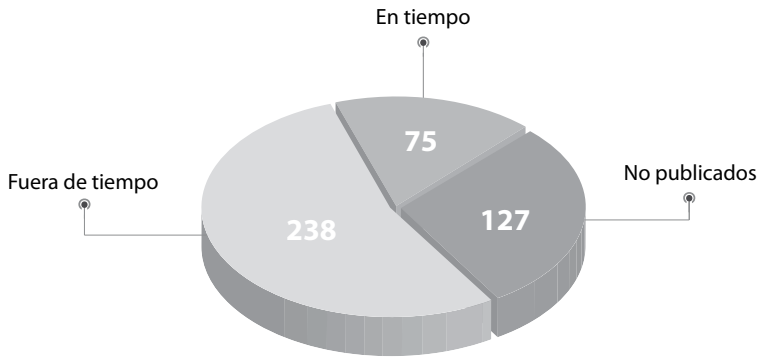
Fuente: Universidad Nacional Autónoma de México (2011).

En ese mismo tenor, el Consejo de Evaluación del Desarrollo Social ha constatado, mediante el Programa de Verificación de Padrones de Beneficiarios de Programas Sociales, que de los 440 programas sociales o acciones de beneficio social que se ejecutaron en 2009 (y que contaron con reglas de operación), sólo se publicaron 313 padrones de beneficiarios (71%), mientras que para el año 2010, de los 407 programas sociales o actividades institucionales de beneficio social sólo se publicaron 245 padrones de beneficiarios (60%).[4]

[3] Numeral 8 Transparencia, participación social y exigibilidad de la política social, del Capítulo I.

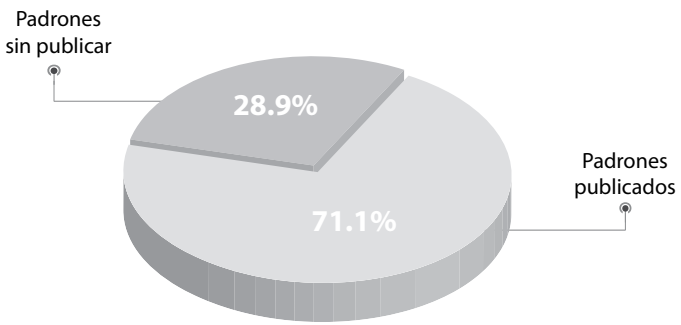
[4] Elaboración del Consejo de Evaluación a partir de las publicaciones en la Gaceta Oficial del DF.

Gráfica 2. Número de padrones publicados en 2010 de programas ejecutados en 2009.



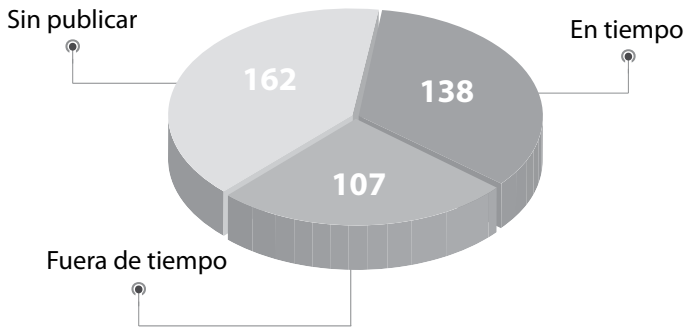
Fuente: Evalúa-DF. Elaboración de los autores.

Gráfica 3. Porcentaje de padrones publicados en 2010.



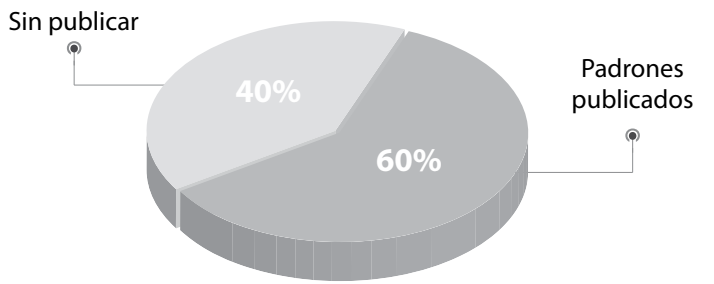
Fuente: Evalúa-DF. Elaboración de los autores.

Gráfica 4. Número de padrones publicados al 30 de septiembre 2011 de programas ejecutados en 2010.



Fuente: Evalúa-DF. Elaboración de los autores.

Gráfica 5. Porcentaje de padrones publicados y sin publicar al 30 de septiembre de 2011.



Fuente: Evalúa-DF. Elaboración de los autores.

Como lo demuestran los datos anteriores, efectivamente existe todavía un alto porcentaje de programas sociales que no hacen públicos sus padrones de beneficiarios, a pesar de ser una obligación de ley. El problema es particularmente grave en las delegaciones. Sin embargo, la justificación no puede ser que se debe a la protección de datos personales de los beneficiaros.

Aunque se debe proteger en forma efectiva la privacidad de las personas frente a la transparencia de la información pública por parte de los entes obligados (Hollrah, 2005:105), la publicación de los padrones de beneficiarios de programas sociales no supone una violación a ese derecho, salvo que se publicaran datos personales o sensibles de las personas.

La publicación de los padrones de beneficiarios es una obligación establecida por la LDSDF, mientras que la Ley de Protección de Datos Personales para el DF establece excepciones para el consentimiento de las personas en cuanto al tratamiento de los datos personales, como lo es su difusión, cuando así lo disponga expresamente una ley, o cuando el tratamiento se haga en ejercicio de atribuciones legales, circunstancias que encuadran en el caso de la publicación de padrones. Asimismo, establece los casos en los que se deberán otorgar diferentes niveles de protección para los datos sensibles, como es el caso de la salud de las personas, programas en los que efectivamente no se deben publicar padrones de beneficiarios, como se hace en el Programa de Atención Integral de Cáncer de Mama.

Esto es, no existe contradicción entre ambos ordenamientos, por lo que, en los casos procedentes, se debe cumplir con la obligación de publicar los padrones de beneficiarios de programas sociales, protegiendo los datos personales.

Problemática en la construcción de padrones de beneficiarios de programas sociales

De la revisión de los padrones de beneficiarios que ha realizado el Consejo de Evaluación se puede inferir que no todos los padrones cumplen con lo dispuesto en el Reglamento de la LDSDF. Esto es, en alrededor del 80% de los casos sólo se cuenta con los padrones de

beneficiarios elaborados con los datos que establece el artículo 34 de la LDSDF, como son el nombre, edad, sexo, unidad territorial y delegación en la que habitan los beneficiarios de programas sociales, pero no se cuenta en las bases de datos con toda la información que dispone el artículo 58 del Reglamento.

Asimismo, se detectó la entrega de padrones de beneficiarios que no fue posible correlacionarlos con las reglas de operación de los programas sociales respectivos. De la misma manera, se encontraron programas sociales que no publicaron en la Gaceta Oficial sus padrones de beneficiarios, pero que sí cuentan con los padrones y las bases de datos respectivas para efectos de verificación.

Dentro de estos casos se puede señalar el Programa de Atención Integral de Cáncer de Mama en el DF, que lleva a cabo el Instituto de las Mujeres del Distrito Federal, en el que no se publica el padrón de beneficiarias por considerar que contiene datos personales sensibles, los que, de conformidad con la ley de la materia, requieren de protección.

Es el mismo caso del Programa de Reinserción Social para Mujeres Egresadas de Refugios y Albergues de la Ciudad de México, y del Programa de Seguro Contra la Violencia Familiar, que lleva a cabo la Dirección General de Igualdad y Diversidad Social de la Secretaría de Desarrollo Social, que no publica padrones sociales de estos programas, para no poner en riesgo a las beneficiarias de los mismos.

Uno de los problemas más recurrentes que presenta la conformación de los padrones es la falta de infraestructura informática y de personal para integrar las bases de datos de los padrones. En muchos casos sólo se cuenta con los formatos impresos, llenados a mano por los beneficiarios de los programas, sin estar digitalizados o capturados en medios electrónicos.

Otro problema menos grave es el retraso en la actualización de las bases de datos de los padrones, particularmente cuando se trata de programas de cobertura amplia, como es el Programa de Servicios Médicos y Medicamentos Gratuitos, los Programas de Uniformes Escolares y Útiles Escolares Gratuitos, entre otros, aunque con el tiempo se ha regularizado su publicación.

Los retos de la protección de los datos personales en instituciones operadoras de programas sociales

Los programas pueden estar protegidos, pero ahora el reto es cómo proteger los datos personales para evitar, entre otros riesgos, el clientelismo y su posible uso electoral. Varios autores y evaluadores de programas sociales han alertado sobre dichos riesgos. Irma Méndez lo describe de la siguiente manera:

> De acuerdo a la hasta ahora escasa evidencia sobre la verdadera magnitud y naturaleza del clientelismo político actual, el mejor escenario parecería ser por ahora la extinción paulatina del monopolio de la intermediación. Garantizar la pluralidad en los servicios de gestión y trabajar a la vez en varios frentes para erosionar no tanto la intermediación partidista sino el clientelismo en tanto intercambio de votos por favores. Ello requiere acciones en al menos el ámbito de lo económico, con más desarrollo que se traduzca en mejores oportunidades, menos desigualdad y pobreza; en lo social para dotar a la ciudadanía de mayores competencias que le permitan una participación más efectiva en la protección de los programas sociales, y en lo político, contribuyendo a crear las condiciones para una competencia electoral justa, equitativa, transparente que haga efectiva la alternancia y pluralice los espacios de intermediación partidista y limite las prácticas clientelares.[5]

Es necesario avanzar en fortalecer e institucionalizar mecanismos de exigibilidad dentro de los programas sociales, que prevengan el mal uso de la información que contienen, y eviten el clientelismo. Particularmente es necesario avanzar en la protección de los datos de las personas beneficiarias.

[5] El papel del Gobierno y partidos en la Protección de los Programas Sociales. Méndez de Hoyos, Irma, 2007. Ponencia presentada en el Seminario Internacional Candados y Derechos: Protección de Programas Sociales y Construcción de Ciudadanía.
http://www.seminarioprotecciondeprogramas.org.mx/ponencias/Conference_Paper_Irma_Mendez_de_Hoyos.pdf

Otra propuesta es avanzar en la homologación del conjunto de la normatividad, ya que varias leyes, aunque tienen el propósito de transparentar el uso de los recursos públicos, particularmente en lo que se refiere a transparentar los padrones de programas sociales, tienen disposiciones con diferentes mecanismos que, lejos de aumentar la transparencia, la dificultan e incluso pueden llegar a contradecirse.

Por un lado están las disposiciones de la Ley de Transparencia y Acceso a la Información Pública del DF, que establecen la obligación de publicar los padrones de programas en los portales de Internet de los entes públicos pero, por otro lado, están la Ley de Desarrollo Social del DF, que establece en su artículo 34 la obligación de publicar en la Gaceta Oficial del DF los padrones de beneficiarios, a más tardar el 31 de marzo de cada año, y en el Sistema de Información del Desarrollo Social del DF. Por su parte, la Ley de Presupuesto y Gasto Eficiente establece en su artículo 97 la obligación de publicar padrones de beneficiarios de aquellos programas o acciones que otorguen ayudas, apoyos o subsidios, aunque no establece temporalidad ni medio de publicación.

Ante este panorama, consideramos que lo óptimo es que todos los programas sociales publiquen sus padrones en un solo sitio, por ejemplo los portales de transparencia, y simplemente dar avisos legales y crear los enlaces respectivos con el resto de los ordenamientos. De esta manera, se daría mayor transparencia a este tema en particular y cualesquier persona, incluyendo las instituciones públicas, podría supervisar el cumplimiento de las obligaciones de dar a conocer los padrones respectivos.

Programas sociales con injerencia de múltiples entes públicos

Existen programas sociales vinculados a diversos entes públicos, como el Programa de Coinversión Social, en el que participan diferentes instituciones, donde cada una de ellas publica por separado sus respectivos padrones. Lo mismo sucede con los programas vinculados a la educación, esto es, los programas de otorgamiento de útiles escolares, uniformes escolares, desayunos escolares, becas escolares, entre otros.

Aunque esta situación es entendible, consideramos que sería mejor establecer la coordinación necesaria para publicar un sólo sistema de padrones de beneficiarios, con campos necesarios adicionales que dieran cuenta de los diversos apoyos recibidos, o de las diversas instancias participantes.

Esto ayudaría particularmente a tener mayor claridad y certeza en las coberturas de la población beneficiaria y, sobre todo, en mejorar los procesos de planeación de toda la Administración Pública, no solamente de aquellos entes que tienen programas vinculados entre sí.

Un sistema electrónico de padrones de beneficiarios, que diera cuenta de manera geo-referenciada de las coberturas de programas y, por lo tanto, de la satisfacción de las necesidades de la población de la Ciudad de México, puede ser fácilmente entrelazado con otros sistemas de información como el Índice del grado de desarrollo social del Distrito Federal, las mediciones de pobreza o el cumplimiento de derechos sociales y/o del programa de derechos humanos del Distrito Federal.

Control y evaluación de los programas sociales y protección de datos personales

A lo largo de poco más de una década, en la Ciudad de México se ha construido un sistema de derechos sociales y una nueva concepción de la política social. Por ello, resulta fundamental mejorar el control y la evaluación de los programas sociales, con el fin de garantizar la transparencia en el manejo de los recursos públicos, así como la protección de los datos personales en los programas.

Los programas sociales deben contar con diseños que contribuyan al fortalecimiento de las políticas de desarrollo social de la Ciudad de México, además de la implementación de un sistema de monitoreo y evaluación interna y externa, que institucionalice y profundice la transparencia y la rendición de cuentas. También resulta indispensable avanzar en la definición de mecanismos y procedimientos, que garanticen la protección de los derechos sociales y de los datos personales que recaban las dependencias del Gobierno del Distrito Federal en el marco de sus atribuciones, toda vez que en ocasiones

se obtienen datos que no son indispensables para acceder a algún programa social.

Es por ello que se deben elaborar mecanismos que garanticen que cada uno de los órganos, dependencias, delegaciones y entidades de la administración pública, ejecutores de programas sociales, cumplan con la responsabilidad que les corresponde en el desarrollo social de la Ciudad de México.

La base principal para alcanzar una protección real de los datos de las personas en los programas sociales, es la armonización de las leyes relacionadas con la materia social, con la Ley de Protección de Datos Personales para el Distrito Federal y la Ley de Transparencia y Acceso a la Información Pública, ya que esto permitirá tener definiciones y límites claros sobre lo que debe ser público y lo que debe ser protegido.

Resulta necesario establecer y conciliar en las leyes, reglamentos y lineamientos y mecanismos de operación de los programas sociales, cuáles son los datos personales que se deben solicitar de acuerdo con el programa social; es decir, qué datos no se deben solicitar porque no representan un requisito forzoso para otorgar el beneficio a quien lo solicita, puesto que, en ocasiones, la información recabada invade la privacidad de las personas, con datos que nada tienen que ver con los requisitos del programa social.

La protección de los datos personales en los programas sociales debe entenderse como una obligación de las dependencias, delegaciones y entidades de la administración pública, quienes con responsabilidad, y apegados a lo que indica la ley, deben implementar acciones para que, al momento de recabar datos personales, éstos sean los mínimos indispensables, en formatos comprensibles para las personas, siempre con la certeza de que la información será protegida y no se utilizará para otros fines que los establecidos en el programa.

La Ley de Desarrollo Social para el Distrito Federal (reforma de mayo de 2005) establece que todos los programas sociales deberán contar con un padrón de beneficiarios, y precisa que sólo será pública la información general sobre el número de participantes, el monto de los recursos asignados, su distribución por sexo y grupos de edad y su distribución por unidades territoriales. Partiendo de esta disposición,

se debe limitar a las dependencias que recaban datos personales que no representan un requisito para otorgar el beneficio. Es muy importante que los controles establecidos para realizar las evaluaciones de los programas sociales contengan un apartado específico, en el que se revisen los mecanismos con que cuentan las dependencias para la protección de los datos personales de los beneficiarios de los programas, mismos que deben articularse y apagarse a lo dispuesto en la Ley de Desarrollo Social y la Ley de Protección de Datos Personales, ambas para el Distrito Federal.

Las evaluaciones que se realicen a los programas sociales deben contemplar la revisión de los formatos y documentos con los que se recaban los datos de las personas que requieren el beneficio, ya que de acuerdo con la Ley de Protección de Datos Personales para el Distrito Federal, ninguna persona está obligada a proporcionar datos personales considerados como sensibles, tal y como son, entre otros: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual. Algunos de estos datos están considerados en la Ley de Desarrollo Social para el Distrito Federal, razón por la cual es apremiante armonizar las leyes y sus reglamentos, con la finalidad de solicitar sólo los datos indispensables, y no aquellos que ponen en riesgo la privacidad de las personas.

Interrelación de sistemas de datos personales de programas sociales mediante instrumentos electrónicos

Los programas sociales implementados por las distintas entidades que conforman la administración pública requieren de instrumentos físicos y electrónicos, que faciliten la protección de los datos personales recabados para otorgar el beneficio de los programas sociales, documentos que deben apegarse a lo establecido en la Ley de Protección de Datos Personales para el Distrito Federal.

Actualmente, es casi desconocido para los habitantes de la Ciudad de México que el llenado de un formato con datos personales implica serias responsabilidades. La dependencia, órgano, delegación ó entidad de la administración pública que recaba información relativa

a datos personales tiene la obligación de asegurar que la misma será tratada y utilizada de forma adecuada, es decir, que solamente será usada para los fines por los que fue recolectada.

Por ello, es indispensable que exista un aviso de protección en todos los formatos y hojas en los que se recopilan datos personales.

Es a través de éste, que el titular de los datos conoce quien será responsable de su tratamiento, con qué fines se recolectan y cuáles son los medios para ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la Ley en la materia.

En el documento físico, electrónico o en cualquier otro formato generado por el responsable de recabar datos personales, y que es puesto a la vista de la persona que los proporciona, se debe contener el aviso ó leyenda de que los datos están protegidos.

Lo anterior, dada la obligación de informar a los titulares de los datos, los fines por los que se solicita los datos.

En los lineamientos de protección de datos personales emitidos por el Instituto de Acceso a la Información Pública y Protección de Datos Personales (InfoDF), se encuentra un modelo de leyenda para informar al titular de los datos acerca de las prevenciones establecidas en la Ley. Lo anterior, sin perjuicio de que las dependencias y entidades elaboren sus propios formatos para informar al titular de los datos lo establecido por el lineamiento respectivo.

En general, los formatos a través de los cuales se recaban los datos personales de beneficiarios y beneficiarias de programas sociales son físicos; esto representa acumulación de archivos y un doble trabajo para las dependencias, ya que para realizar versiones públicas de los padrones de los programas y publicarlos en el portal de Internet, se debe proceder a la captura de los datos.

Sin duda, es necesario que, de manera paulatina, los servidores públicos que recopilan datos personales cuenten con instrumentos adecuados para realizar la captura de los datos en forma electrónica, y así evitar la acumulación de información en papel.

En otras palabras, es indispensable contar con instrumentos que permiten capturar los datos de las personas de manera electrónica para facilitar el resguardo, la protección y la seguridad de los datos proporcionados a los Entes Públicos.

Desafíos y ventajas para la construcción de un Sistema Único de Padrones de los Programas Sociales

A lo largo de poco más de una década, en la Ciudad de México se ha avanzado en el goce de los derechos sociales y una nueva concepción de la política social. El Gobierno del Distrito Federal tiene a los derechos sociales como tema fundamental de sus políticas públicas, es por ello que es indispensable lograr una coordinación de todos los programas sociales creados desde hace trece años, con las ventaja y desafíos que derivan de esta acción, ya que se pretende otorgar atención directa e información a los ciudadanos, a fin de evitar duplicidades por la falta de articulación entre los programas, además de establecer de un Sistema de Información para el registro de padrones de los programas sociales de la administración pública del Distrito Federal.

Es en la actual administración donde se inicia el proceso de transparencia con respecto a los padrones, los lineamientos y los mecanismos de operación de los programas sociales, a través de reglas de operación. A continuación de da una breve cronología de este proceso.

- **2005.** La Ley de Desarrollo Social obliga a tener padrones y reglas de operación;
- **2006.** El Reglamento de Desarrollo Social indica que deben tener los padrones y reglas de operación;
- **2007.** Decreto de Presupuesto. Obliga a publicar reglas de operación y padrones (en el 3er mes del año);
- **2008.** La Reforma a la Ley de Desarrollo Social obliga a publicar reglas de operación y padrones:

De acuerdo con lo que establece la Ley de Desarrollo Social para el Distrito Federal, cada uno de los programas sociales que implementa la administración pública del Distrito Federal debe tener un padrón de participantes o beneficiarios. Por ello, a través de los años se han realizado esfuerzos por sistematizar la información de los padrones, que representa el proceso de un sin fin de formatos físicos y electrónicos por cada programa social. Si a esto se suma que cada dependencia utiliza diversos mecanismos para recabar información, se da lugar a un mundo interminable de archivos, poco prácticos para su consulta y protección.

Instituir toda esta red de programas sociales en un solo sistema es fundamental, ya que permitiría sistematizar y transparentar la información en poder de las dependencias, además de facilitar la consulta, los diagnósticos y las evaluaciones sobre la eficacia de las políticas sociales instrumentadas en la capital del país.

La sistematización de la información permitirá contar con un registro ordenado y por rubros, ya sea por tipos de programas y/o de acuerdo con el grupo vulnerable que se apoya, por ejemplo:

Padrones de programas dirigidos las y los niños

- Programa niño talento
- Programa útiles gratuitos
- Programa uniformes gratuitos
- Programa de educación garantizada

Padrones de programas dirigidos a las mujeres

- Programa de seguro contra la violencia
- Programa de reinserción social para mujeres víctimas de violencia familiar
- Programa de detección oportuna de cáncer de mama

Lo anterior permitirá contar con una base de datos para la identificación del tipo de apoyo, el monto otorgado, la ubicación por unidad territorial, delegación, etc.; además de la protección y resguardo de los datos personales, con el fin de evitar el mal uso de la información. Esta sistematización es un proceso participativo que

posibilita ordenar y recuperar la memoria histórica de cada programa social, en un sólo sistema en el que se proteja la información.

El registro y la sistematización rigurosa, con técnicas y estrategias adecuadas, posibilita poner en orden el cúmulo de información de las y los beneficiarios de programas sociales, recopilando y generando un proceso ágil y eficiente de los datos, así como la recuperación de aquellos que se consideren pertinentes y la socialización de los mismos entre las dependencias de la administración pública del Gobierno del Distrito Federal.

La sistematización de la información tiene como objetivo principal la articulación de los programas sociales y el conocimiento sobre cómo se está distribuyendo el gasto social en la Ciudad de México, cuáles son las zonas más beneficiadas, y si éstas coinciden con las unidades territoriales de más alta marginación, además de delimitar el objeto principal sobre la información que nos interesa conocer, registrar y proteger.

La creación de un Sistema de Información para el registro de padrones de programas sociales de la administración pública del Distrito Federal representa un desafío, ya que lograr que todas las dependencias, órganos y delegaciones articulen y se apeguen a un solo formato físico ó electrónico, resulta un verdadero reto y un compromiso de todos para el intercambio de información.

Para implementar el Sistema de Información para el registro de padrones de programas sociales, es necesario que las dependencias cuenten con las herramientas tecnológicas y operativas mínimas, así como con los recursos humanos suficientes para alcanzar el objetivo del sistema, esto es, la sistematización de la información de las personas que acceden a los programas sociales.

Un reto más para lograr que el Sistema se ponga en marcha, es la obligatoriedad de integrarse y realizar los trabajos, es decir, resulta indispensable una adición o modificación a la Ley de Desarrollo Social para el Distrito Federal, con la finalidad de que sea un deber y un compromiso de toda la administración pública del Distrito Federal incorporar la información que se requiera, para que el sistema funcione adecuadamente.

Finalmente, nada de lo anterior será efectivo si no se establecen mecanismos efectivos de control y seguimiento a estas obligaciones de ley, y si no existe, en su caso, un procedimiento claro y efectivo de sanción por su incumplimiento. A pesar de los avances logrados, una parte del problema tiene que ver con el contenido de la norma, pero la problemática central, nos atrevemos a señalar, tiene que ver con su cumplimiento y materialización. Cerrar la brecha de implementación de la legislación en materia de padrones y datos personales es una tarea fundamental.

Referencias

Evalúa-DF (2011) *Informe de actividades a diciembre de 2010, del Programa de Verificación de Padrones de Programas Sociales del DF*, México.

Evalúa-DF (2011) *Informe de actividades a septiembre de 2011, del Programa de Verificación de Padrones de Programas Sociales del DF*, México, 7 pp.

Hollrah, Rachel, (2005) *La protección de la privacidad frente a la transparencia gubernamental* en Derecho Comparado de la Información, UNAM, México.

Instituto de Acceso a la Información Pública del Distrito Federal (2011) *Resultados de la primera evaluación 2011 de la información pública de oficio que deben dar a conocer los Entes públicos en sus portales de Internet*, México,

Programa de las Naciones Unidas para el Desarrollo (2007) *Buenas Prácticas en la protección de programas sociales*, México, 184 pp.

Universidad Nacional Autónoma de México (2011) *Informe final de la Evaluación de los Programas y Políticas Sociales en el Distrito Federal*, México, (versión electrónica).

Difusión y protección de datos personales por parte de los órganos de impartición de justicia: diez años de publicidad

Carlos G. Gregorio

Carlos G. Gregorio

Desde 1999 es investigador del Instituto de Investigación para la Justicia. Ha escrito numerosos trabajos sobre internet, transparencia y protección de datos personales aplicados a la justicia. Ha trabajado desde 2008 como consultor para la Asociación Mexicana de Impartidores de Justicia, y el Proyecto Presunción de Inocencia en México, y ha sido consultor en distintos organismos internacionales como Unicef y el Banco Mundial, además de ser profesor en universidades de España, Chile, Uruguay y Argentina.

Es Doctor por la Universidad de Buenos Aires, cuenta con entrenamiento como Mediador, Ministerio de Justicia (Argentina), además estudió en la École-Colloque d'Analyse des Données, Université des Antilles et de la Guyane, Pointe-a-Pitre. Obtuvo la Beca de la Université Paul Sabatier (Toulouse). Licenciado en Ciencias Matemáticas, Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires.

Introducción

En julio de 2001, luego de una rápida expansión de las aplicaciones en Internet de los poderes judiciales de Iberoamérica, surge el primer conflicto vinculado a la protección de datos personales en el contexto de la información judicial, que debió ser resuelto por una Corte Suprema: se trata del caso de una mujer que ve publicados en el sitio en Internet del Poder Judicial de Chile los detalles del proceso de investigación de paternidad de su hija.[1] Desde allí en adelante los poderes judiciales han sido jueces y parte en este tipo de ponderación de derechos, en la mayoría de los casos huérfanos de una legislación adecuada e intentando llenar —en la medida de sus posibilidades— las lagunas axiológicas provocadas por la incorporación de las nuevas tecnologías.

El debate judicial se centró en la ponderación de los derechos a la intimidad, vida privada y protección de los datos personales por un lado, con la creciente tendencia a reconocer múltiples derechos de acceso a la información pública y el derecho de audiencia por el otro.[2] No estaban ajenos a esta cuestión jurídica, en gran parte teórica, los años —y quizás siglos—de críticas por decisiones judiciales tomadas en la oscuridad y con un débil control ciudadano, que se sumaban también a la insatisfacción por la ineficiencia y retardo en la administración de justicia. No es raro entonces que los poderes judiciales de la región buscaran rápidamente en las nuevas tecnologías la posibilidad de incrementar su eficiencia, así como ampliar sus políticas de transparencia.

[1] Paula Jervis Ortiz, 'Comentario jurisprudencial. Intimidad y tratamiento de datos personales en el portal del Poder Judicial', 1 *Revista Chilena de Derecho Informático* (2002).

[2] Se usa aquí el concepto de derecho de audiencia (uno de los varios derechos que conforman la "libertad de expresión"). Rebecca Tushnet encuentra que la discusión teórica sobre la libertad de expresión se centra en la implicaciones de "enfocarse en quien habla" *versus* "enfocarse en la audiencia". También Jerome Barron señala un profundo interés en proveer a los ciudadanos de un amplio acceso a puntos de vista conflictivos y a asuntos poco corrientes, no solo porque quienes tienen ideas disruptivas tengan derecho a ser oídos, sino porque la sociedad tiene un especial interés en oírles. Rebecca Tushnet, *Power Without Responsibility: intermediaries and the First Amendment*, 76 *Geo. Wash. L. Rev.* 101 (2008), disponible en SSRN: http://ssrn.com/abstract=1205674; Jerome A. Barron, *Access to the Press—a new First Amendment right*, 80 *Harv. L. Rev.* 1641, 1641, 1653–54 (1967).

En julio de 2003 —aun dentro de una atmósfera académica—surgen las *Reglas de Heredia*, un instrumento internacional no vinculante (*soft law*) en el que se intentó encontrar reglas con cierto nivel de generalidad, para restablecer el equilibrio entre la publicidad de las actuaciones judiciales y protección de los datos personales. Las *Reglas de Heredia* fueron un aporte con visión de futuro, que incorporó algunos criterios que luego serían adoptados progresivamente por algunos poderes judiciales de la región; pero obviamente su simpleza no logró atrapar toda la casuística que se iría suscitando en los años siguientes. No obstante, las *Reglas* son hoy un documento vigente visto como una referencia obligada, a las que se van adicionando y reconociendo excepciones y casos particulares.

El problema de fondo es ciertamente complejo y compromete visiones difíciles de conformar: quienes —por un lado— creen que con la tecnología la privacidad debe reducirse a una esfera íntima muy reducida, porque estiman que el flujo absolutamente libre de la información provocará múltiples beneficios;[3] portan como bandera aquella frase de Louis Brandeis: "nada desinfecta mejor que la luz del sol". Por el otro lado están quienes aún recuerdan los crímenes cometidos utilizando bases de datos personales sensibles, y continúan viendo hoy muchos riesgos en los sistemas políticos, quizás mucho más débiles frente a las tensiones del mercado.

La información judicial vista como el complejo resultado de distintos tipos de información

La información judicial es por naturaleza un término extremadamente amplio que se desarrolla en muchos documentos que concurren ocasionalmente en el "expediente judicial", pero que también incluye

[3] Cada día descubrimos que el flujo de la información no nos hace más libres, y que la neutralidad de los operadores de Internet es cada vez más discutible. Hasta hace poco tiempo filtrar a un ciudadano su acceso a la información se denominaba "censura previa", hoy se usa el eufemismo "facilitar al usuario de su propia burbuja"; con ese concepto Eli Parisier sostiene que los buscadores –la puerta de acceso a la información— nos crean una burbuja personalizada y deciden a que porción de la realidad tendremos acceso, ver: www.thefilterbubble.com/author/eli-pariser Tim Berners-Lee, 'Long Live the Web: A Call for Continued Open Standards and Neutrality: the Web is critical not merely to the digital revolution but to our continued prosperity—and even our liberty. Like democracy itself, it needs defending', www.scientificamerican.com/article.cfm?id=long-live-the-web, *Scientific American Magazine*,Diciembre 2010

otro tipo de documentos con diferentes propósitos, niveles de uso, difusión y entidad. Este concepto de información judicial ha ganado hoy relevancia en particular con la generación del expediente electrónico. En este punto es necesario hacer una acotación tecnológica para distinguir dos soportes de información: cuando se almacena en imágenes y cuando está digitalizada; mientras que la primera es un resabio del pasado con algunas diferencias como ser transmisible, replicable e incluso digitalizable con mayor facilidad, la información digitalizada tiene la propiedad fundamental de facilitar las búsquedas por pertinencia.

Si bien contra el éxito de una búsqueda atenta la cantidad de información puesta a disposición,[4] siempre es posible desarrollar mecanismos para facilitar o desincentivar las búsquedas en función de las finalidades definidas. Todo este cambio obliga a analizar cuidadosamente cuáles son los derechos y cuáles los riesgos antes de difundir información judicial en formato digital.

Sin embargo, la realidad muestra que los primeros pasos —en casi todos los países— han tenido lugar por vía de la publicidad. Los órganos de impartición de justicia continúan difundiendo e inundando la Internet con los mismos formatos de publicación que antes se hacían en papel (como por ejemplo las listas de acuerdos), y publican nuevos documentos tomando en consideración que determinados textos —ahora con las herramientas informáticas— están ahora fácilmente (o sea a bajo costo) disponibles.[5]

La evolución en México no ha sido marcadamente diferente a la de otros países de la región (quizás con la única variante en el sentido de mostrar cierta reticencia a la publicación de textos íntegros de sentencias judiciales). Al analizar los sitios web de los órganos de impartición de justicia en México, y de otros países, es posible encontrar preliminarmente varios tipos de documentos, como los siguientes:

[4] Susan W. Brenner, *Precedent Inflation,* Transaction Publisher, *1992,* donde sugiere que la saturación de información con precedentes redundantes crea también una forma de opacidad.

[5] Tanto la Corte Suprema de Chile en *REMTE vs. Corporación Administrativa del Poder Judicial* (3 de Julio 2001) como el Tribunal Constitucional español, en la Sentencia 114/2006 (5 de Mayo) sostienen que los criterios de publicacion son los mismos sean "en soporte papel, electrónico o cualquier otro".

- Jurisprudencia y textos íntegros de sentencias judiciales
- Listas de Acuerdos (i.e. la publicación diaria de las decisiones tomadas en cada paso procesal)
- Acuerdos del Pleno (en asuntos administrativos)
- Notificaciones (las que se realizan en los estrados o cuando una parte tiene domicilio desconocido)
- Convocatorias a Audiencias
- Edictos
- Sistemas de seguimiento de causas (expediente electrónico en línea)
- Otros tipos de información judicial

La publicación de los textos íntegros de las sentencias hace a una política de transparencia judicial y promoción de la seguridad jurídica, porque se difunden aun cuando no se les reconoce un valor jurisprudencial, especulando que los ciudadanos tienen un legítimo interés en conocer cómo los jueces deciden los conflictos de la sociedad.

En este sentido, la Corte Suprema de Justicia de la Nación ha comenzado a publicar y dar acceso a los textos íntegros de las sentencias; en las entidades federativas el tema es más controvertido, mientras algunos opinan que al no tener valor jurisprudencial no es necesario publicarlas, otros tribunales han comenzado a publicar sentencias (aunque no todas, ni de todas las instancias).

Por ejemplo el Tribunal de lo Contencioso Administrativo de Guanajuato mantiene un sitio de jurisprudencia que incluye decisiones de otras entidades federativas. En la presentación del sitio se dice:[6]

> La interpretación que de la ley hacen los diversos órganos jurisdiccionales, independientemente del nombre de su resultado (jurisprudencias o criterios), constituyen una importante fuente de Derecho, en nuestro caso, de la rama administrativa. Consiente de su importancia, más allá de lo vinculante o no de estas interpretaciones legales, el Tribunal de lo Contencioso Administrativo del Estado de Guanajuato, pone a disposición del estudioso

[6] http://jurisprudencia.tcagto.com/

del Derecho el presente disco compacto, el cual contiene 1,472 criterios y jurisprudencias emitidos por los tribunales administrativos locales de 13 entidades federativas de nuestro país.

El Tribunal Superior de Justicia del Distrito Federal publica los *Anales* en papel, sin embargo han sido digitalizados por el Instituto de Investigaciones Jurídicas de la UNAM hasta el año 2007.[7] Las Listas de Acuerdos (o el Boletín Judicial como se denomina en la mayoría de las entidades federativas) es una tradición en México, y son publicadas por la mayoría de los Poderes Judiciales de los estados. En algunos Estados se refieren (pero no se publican) acuerdos secretos o reservados: de hecho se hace pública la existencia de un acuerdo en un caso que ha sido clasificado como secreto, dándose eventualmente el número de caso, pero no el nombre de las partes ni el sentido del acuerdo. Esto se observa también en otros países, como por ejemplo en el Tribunal Superior de Justicia de San Pablo, Brasil, donde algunos abogados tienen por costumbre solicitar —en todos los casos que patrocinan— el secreto del expediente, para evitar la exposición de sus clientes.

Nayarit es el único estado que no publica el nombre de las partes como regla general. Tabasco era el único estado que publicaba el nombre de los ofendidos en los acuerdos en materia penal,[8] aun cuando la Ley Orgánica del Poder Judicial no obliga a tal publicación (el nombre del ofendido se publicaba sólo en la versión *web*, en la versión en papel hecha con destino a la biblioteca no aparecen los nombres de los ofendidos).[9] Existe cierta variabilidad, por ejemplo, en algunos casos se publica únicamente el nombre del promovente y no necesariamente los de partes (Zacatecas) y Aguascalientes publica el nombre del inculpado, pero no el delito.[10]

[7] Ver: www.juridicas.unam.mx/publica/rev/cont.htm?r=anjuris). Los textos íntegros se anonimizan dejando los nombres de pila de las partes e inicializando los apellidos.

[8] El sitio web de poder judicial de Tabasco fue modificado a mediados de 2011 y se publica ahora el Boletín Judicial sin mencionar a las víctimas de los delitos.

[9] Este detalle es muy revelador y se menciona aquí porque luego se argumentará que gran parte de los problemas se han generado por la incomunicación que existe entre las autoridades judiciales y los equipos de programadores que desarrollan las aplicaciones *web*.

[10] www.poderjudicialags.gob.mx/servicios/agenda/consagendapen.cfm

Hoy predominan dos vías de acceso, por día de publicación (tomando el estilo de origen de la publicación en papel), y por número de caso, mucho más razonable para la versión electrónica.

Obviamente la publicación en papel debía ser revisada a diario por los abogados litigantes para advertir algún acuerdo en uno de sus casos; si está habilitada la búsqueda por expediente, el procedimiento habitual para un abogado sería revisar solo sus expedientes. Los proyectos de *juicio en línea* esperan que los abogados acepten se les envíen automáticamente los acuerdos al correo electrónico del litigante, mientras tanto puede verse cómo Aguascalientes ha facilitado la consulta, permitiendo insertar una lista de expedientes.[11]

Una conclusión a la que permite arribar este último desarrollo es la necesidad de instalar como "método", que quienes diseñan estas aplicaciones deban identificar las necesidades de los usuarios, consultándolos y poniéndose en el lugar de quienes no pueden ser consultados, para evaluar sus intereses y riesgos. Como se analizará más adelante (al considerar la finalidad de las bases de datos personales) los usos secundarios de las listas de acuerdos se han centrado en la discriminación laboral y el análisis de riesgo en el acceso al crédito; en ambos confundiendo los criterios que forman la base de la igualdad de oportunidades (por ejemplo en Costa Rica llegó a la Sala Constitucional un caso de discriminación laboral por haber sido el postulante víctima de un delito, o en otro caso, se le negó un crédito a una persona por haber sido demandado su hermano en un juicio ejecutivo).Las Leyes de Transparencia y Acceso a la Información Gubernamental han generado la obligación de publicación espontánea de varios tipos de documentos judiciales. Si bien no siempre están incluidos en la letra de la ley, muchos poderes judiciales interpretan que deben publicar en su sitio *web* los acuerdos del Pleno del Tribunal.[12] Las notificaciones

[11] www.poderjudicialags.gob.mx/servicios/lista/listaexps.cfm

[12] Ver Puebla www.htsjpuebla.gob.mx/secciones/actividades_del_tribunal/all_acuerdos_de_pleno.php y Sinaloa www.stj-sin.gob.mx/index.php?option=com_content&view=article&id=169 (acuerdos "relevantes"). La publicación de Acuerdos del Pleno no es predominante en México, y cuando existe se limita a acuerdos destacados o elegidos como relevantes. En el ámbito de América Latina, Costa Rica ha mantenido una política de publicar las versiones taquigráficas de las reuniones del Pleno, se publican todas las sesiones y todas las decisiones tomadas en forma de "acta". En otros países se acostumbra dar forma a la decisión independientemente de la discusión y opinión de los magistrados, en estos casos se publican las llamadas "acordadas", como es el caso de Argentina y Paraguay.

por estrados son realizadas vía Internet para notificar cuando alguna parte tiene domicilio desconocido, aun cuando algunas veces esta modalidad se utiliza por no disponer de recursos para hacer todas las notificaciones en los domicilios.[13]

Deberían buscarse mecanismos complementarios para tomar ventaja de las comunicaciones electrónicas como, por ejemplo, enviar SMS a un celular o enviar un correo electrónico en forma concurrente y reiterada. Sería prudente que los programadores revisen otros sitios web de poderes judiciales y analicen cuidadosamente la información que se publica: la información debe ser mínima, pero también comprensible y autónoma al momento de interpretar los contenidos.

El acceso a la programación de audiencias (públicas) pone en juego la presunción de inocencia, el derecho de defensa y el principio de publicidad de las actuaciones judiciales. Su publicación debe contener los datos necesarios para que cualquier persona pueda determinar su interés en asistir a una audiencia en particular. Un tema delicado es la publicación de los nombres de los imputados en las listas de audiencias penales, pues estaría en colisión con la presunción de inocencia (al menos cuando se publica en Internet). Aquí sería posible un balance de derechos que podría ser una publicación "referencial" en Internet que se complemente con una publicación más amplia en estrados.[14] Podría ser como se hace en Aguascalientes, que no publica los nombres de los imputados (o incluso podrían publicarse iniciales para que sea identificable solo para aquellos que conocen el nombre del imputado).[15]

[13] Ver Puebla www.htsjpuebla.gob.mx/secciones/actividades_del_tribunal/notificaciones.php y Aguascalientes www.poderjudicialags.gob.mx/servicios/notificaciones/notif.cfm donde se pueden consultar por número de expediente.

[14] En Paraguay "según Acta Nº 34/09 del Consejo de Superintendencia de la Corte Suprema de Justicia, todos los procesos que formen parte del Calendario de Juicios Orales a ser publicados en el Sitio Web del Poder Judicial, llevarán sólo las iníciales de las personas que figuren en la carátula del expediente."

[15] Ver Aguascalientes www.poderjudicialags.gob.mx/servicios/agenda/consagenda.cfm (no publica los nombres) y www.poderjudicialags.gob.mx/servicios/agenda/consagendapen.cfm en penal publica solo el delito y el objeto de la audiencia.

Aguascalientes, ejemplo sobre la publicación de convocatoria a audiencias

Juzgado Primero Penal

Fecha	Hora	Expediente	Delito	Audiencia
29/08/2011	09:00 AM	72 / 2011	ROBO	FINAL DE JUICIO
30/08/2011	09:30 AM	98 / 2011	ROBO	FINAL DE JUICIO
30/08/2011	10:00 AM	153 / 2011	ROBO	PRUEBAS
30/08/2011	10:30 AM	153 / 2011	ROBO	PRUEBAS
30/08/2011	11:00 AM	153 / 2011	ROBO	PRUEBAS
31/08/2011	09:00 AM	7 / 2010	DESPOJO RURAL	PRUEBAS

Nota: Los datos aquí mostrados son únicamente de carácter informativo.

El problema con el diseño de Aguascalientes es que las listas se publican para las audiencias "del día", y no con mayor anticipación, como sí se hace –por ejemplo– en Costa Rica y Paraguay.[16]

En efecto, en Costa Rica se publican con más anticipación y suelen cancelarse (o ser retiradas de Internet) cuando ha pasado la fecha de la audiencia (entendiendo que a partir de ese momento ya carecen de sentido y que prevalece –entonces– la presunción de inocencia). Además, las listas de audiencias deberían excluirse de la indexación de los buscadores (*Robot Exclusion Standard*) o publicarse totalmente en imágenes.

[16] Ver www.pj.gov.py/noticia.asp?codigo=6014

Costa Rica, ejemplo sobre la publicación de convocatoria a audiencias.[17]

Tribunal de Juicio del Primer Circuito Judicial de San José - Septiembre 2011- Sección I

Expediente	Fecha	Hora	Imputados	Delito (s)	Grupo	Testigos
07-14-621-TP	01 AL 15/09/11	08:00	xxxxxxxxx xxxxxx xxxxxxx	ESTAFA	1	26
09-13-16-PE	19/09/2011	08:00	xxxx xxxx xxxxxx xxxxxx	INJURIAS, CALUMNIAS Y DIFAMACIÓN	1	2
94-1531-202-PE	20/09/2011	08:00	xxxx xxxx xxxxxxxxx	HOMICIDIO CULPOSO	1	6
10-809-994-PE	21/09/2011	08:00	xxxxx xxxxxxxx xxxxxxx xxxxxx	ABUSO SEXUAL	1	3
94-1531-202-PE	22/09/2011	08:00	xxxxxxxxx xxxxx xxxxxxxx	HOMICIDIO CULPOSO	1	6
08-2951-275-PE	23/09/2011	08:00	xxxxxx xxxxxxxxx xxxxx	ROBO AGRAVADO	1	4
05-21143-42-PE	26 AL 27/09/11	08:00	xxxxxxxxxx xxxx xxxx	POSESIÓN DE DROGA	1	10
07-703-609-PE	28/09/2011	08:00	xxxxxxxx xxxx xxxxxxx xxxxxx	ABUSO SEXUAL	1	3
04-2326-175-PE	29/09/2011	08:00	xxxx xxxx xxxxxxxxx xxx	FRAUDE DE SIMULACIÓN	1	2
09-110-16-PE	30/09/2011	08:00	xxxxxx xxxx xxxxxxxxxx xxxx	INJURIAS, CALUMNIAS Y DIFAMACIÓN	1	4
08-3461-275-PE	30/09/2011	08:00	xxxx xxxxxxxx xxxxxx	PORTACIÓN ILEGAL DE ARMA	1	2
10-20297-42-PE	30/09/2011	09:30	xxxxx xxxxx xxxxxxxxx	HURTO SIMPLE	1	5

No fue fácil llegar al sitio *www.poder-judicial.go.cr/servicios/juicios.html* donde se publican las audiencias (desde el "home", hay que seleccionar "servicios" y allí "programación de juicios orales") se pudo ver que el enlace correspondiente a cada juzgado solo arrojaba los juicios programados para Julio de 2011 (la consulta se hizo en agosto).

[17] Ver www.poder-judicial.go.cr/servicios/juiciosorales/2011/setiembre/circ1_sanjose.htm consultado el día 29 de Agosto de 2011.

Manipulando la URL pudo accederse a los juicios programados para agosto y septiembre, y también a los programados en 2010, aun cuando no existían "enlaces" publicados para estas fechas.

En la columna "Imputados" pueden leerse los nombres, aquí se suprimen (ocultados con marcador negro, que se dice "*caviarizados*" en la jerga judicial) para evitar una difusión innecesaria.

La publicación de los edictos en un sitio web del Poder Judicial es mucho más efectiva y racional que la publicación en periódicos de gran circulación. Sin duda buscar en un solo sitio garantiza más el acceso a un edicto que revisar cientos de periódicos a nivel nacional, por ello algunos tribunales están dirigiendo los edictos a los sitios web.

En México por ejemplo, el sitio web en Sinaloa permite tanto la búsqueda libre como acotar la fecha de publicación.[18] En ambos casos no están indexados en Google u otros buscadores.[19]

Se agrega la frase "Por tratarse de una trascripción electrónica que puede estar sujeta a error, la presente publicación es solo de carácter informativo, sin efecto legal alguno."

Frases como éstas han causado la ira de los académicos, aun así son muy frecuentes en otros sitios judiciales en América Latina.[20]

[18] www.stj-sin.gob.mx/edictos/consporfecha.php y www.stj-sin.gob.mx/edictos/consgral.php

[19] En estos casos el edicto es de máxima publicidad y podría permitirse la indexación.

[20] La información que se origina o procesa judicialmente puede tener diferente entidad y valor. Referencial: la información contenida en el sistema facilita el acceso o el proceso de identificación de documentos o personas necesarios para la gestión (Listas de Acuerdo son referenciales, tanto en papel como en la web). Documental: la información que tiene valor documental habilita para la toma racional de decisiones. Si las partes, por ejemplo, pueden informarse sobre una decisión del juez o una notificación por medio de una consulta al sistema de información, ese dato debe tener valor documental. En todos los datos clasificados como documentales debe garantizarse que la información no pueda ser modificada o, en su caso, deberá dejar rastros sobre el contenido anterior, quién los modificó y cuándo (en nuestro caso el "expediente" es documental y en el futuro el expediente electrónico). Registral: la característica más importante son sus efectos legales y su completitud; en un sistema registral la no existencia de información pertinente tiene valor documental.

Sinaloa, ejemplo de edicto publicado en el sitio web:

2011-08-08

Juzgado de Primera Instancia del Ramo Civil del Distrito Judicial de Navolato, Sinaloa.

E D I C T O

Exp. No. 797/2011

Convóquense quienes créanse con derechos a Juicio Sucesorio Intestamentario a bienes de: ●●●●● ●●●●● ●●●●●●●●●● y ●●●●● ●●●●●●● ●●●●●●●● ●●●●●, presentarse a deducirlos y justificarlos ante este Juzgado, término improrrogable treinta días a partir de hecha la última publicación del edicto.

Atentamente

Navolato, Sinaloa, Junio 09 de 2011

El Secretario Primero

En relación con los edictos, la evolución es tomar todas las ventajas de las aplicaciones informáticas a favor de la finalidad buscada: garantizar el derecho de defensa. En Ecuador las circunstancias llevaron a que el periódico *La Hora* desarrollara una aplicación informática que concentró todos los edictos en su sitio web, con la posibilidad de un buscador. En Brasil, al aprobarse la ley que regula el expediente electrónico, se estableció la publicación centralizada de los edictos en el Diario de Justica electrónico.[21]

[21] Lei Nº 11.419, www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm

Sin embargo la realidad no ha llegado a las expectativas. En Brasil los *Diarios da Justiça* fueron creados por los Tribunales Superiores estatales y aun no existe uno a nivel nacional. Como puede verse en el ejemplo del Estado de Goiás (ver instructivo para la búsqueda de un edicto),[22] la publicación electrónica no es más que un PDF de la publicación en papel, esto es, no existe un buscador donde cualquier persona pueda verificar regularmente si su nombre aparece en algún edicto. Los edictos deberían ser accesibles por medio de los buscadores más populares (*Google, Yahoo*, etc.), o sea, debería permitirse la indexación. Por el contrario, algunos académicos opinan que la información judicial debería ser accesible solamente en los sitios oficiales de los Poderes Judiciales. Un ejemplo de Ecuador pone de manifiesto algunas contradicciones. El siguiente edicto (citación) fue publicado en el periódico *La Hora*, pero encontrado en Google:

JUZGADO NOVENO DE LA NIÑEZ Y ADOLESCENCIA DE PICHINCHA

Citación judicial al señor ●●●●● ●●●●● ●● ●●●●●●●● padre de la menor ●●●●● ●●●●● ●● ●●●●● ●● ●●●●●

EXTRACTO CAUSA

No. DE JUICIO: 0039-2009- V.P.

DEMANDADO: ●●●●● ●●●●● ●● ●●●●●●●● padre de la menor ●●●●● ●●●●● ●● ●●●●● ●● ●●●●●

ACTOR: ●●●●● ●●● ●●●●●● ●●●●●● mandataria de su hija señora ●●●●● ●●●●●●● ●● ●●●●● ●●●●●

CUANTÍA: indeterminada

JUZGADO NOVENO DE LA NIÑEZ Y ADOLESCENCIA DE PICHINCHA.- Quito, martes 22 de diciembre del 2009, las 11h46. Avoco conocimiento

[22] www.tjgo.jus.br/docs/servicos/diariodajustica/INS_CONSULTAR.pdf

de la presenta causa en calidad de Juez Titular y del sorteo efectuado. Por cuanto la accionante señora ●●●●● ●●● ●●●●●● ●●●●●● , ha dado cumplimiento con lo solicitado en providencia anterior, la demanda de autorización de salida que antecede es clara y reúne los requisitos del artículo 67 del Código de Procedimiento Civil, en consecuencia se la acepta a trámite conforme lo dispuesto en el artículo 109 del Código de la Niñez y Adolescencia. En lo principal: Cítese, en legal forma, al señor ●●●●● ●●●●● ●● ●●●●●●●● , de conformidad con el artículo 82 del Código de Procedimiento Civil, mediante tres publicaciones por la prensa en uno de los periódicos de mayor circulación de esta ciudad, conforme lo solicitado por la señora ●●●●● ●●● ●●●●●● ●●●●●● , en calidad de Apoderada de la señora ●●●●● ●●●●●●● ●● ●●●●● ●●●●● , madre de la menor ●●●●● ●●●●● ●● ●●●●● ●● ●●●●●. Agréguese al proceso la documentación acompañada y téngase en cuenta el casillero judicial señalado. NOTIFÍQUESE Y CÍTESE. Lo que comunico a usted para los fines de Ley. Previniéndole de la obligación que tiene de señalar domicilio judicial o casilla judicial para posteriores notificaciones dentro del perímetro de Ley.

Atentamente,

DR. ●●●● ●●●●●● ●●●●●●●●●●

SECRETARIO

Hay firma y sello

Este tipo es muy frecuente en Ecuador y se relaciona con la condición de migrante ilegal del padre; o sea, el padre no puede visitar su familia (no puede salir del país en que está trabajando), pero sí puede costear el viaje de su familia. Al no poder ser parte en el proceso, la esposa le

reporta como desaparecido, el Juez le cita por edicto y, en ausencia, autoriza el viaje de los hijos menores de edad (a visitar a su padre).

La conclusión negativa es que un niño aparece en Google vinculado a una situación irregular falsa (abandonado por parte de su padre), que le estigmatiza y hace públicos aspectos de su vida privada.

En otros edictos relacionados con la "pérdida de la patria potestad" se ven algunos cuidados por parte de los jueces que no mencionan los nombres de los menores, argumento que da a entender que los nombres no son estrictamente necesarios a los fines de la citación.

Esto permite arriesgar algunas conclusiones, como que el texto debe ser mínimo y solo destinado a garantizar el derecho de defensa; su publicidad debería estar acorde a su finalidad (aun cuando no está claro que la indexación en Google garantice aun más su derecho de defensa). En conclusión "redactar documentos judiciales que van a publicarse en Internet" requiere de capacitación y visión.

Para el acceso a la información procesar electrónica en detalle (expediente electrónico o juicio en línea) existen en el contexto de los sistemas judiciales tres modalidades:

- Libre acceso a todos los expedientes electrónicos;
- Acceso con clave de usuarios que habilita a ver cualquier expediente;
- Acceso con clave de usuario, que habilita a ver sólo los expedientes de los que se es parte.

El modelo totalmente abierto es el predominante en Brasil, está prácticamente extendido a todas las jurisdicciones (federal, estatal y del trabajo) y es posible identificar el expediente con una multiplicidad de criterios de búsqueda, como el número de caso, nombre de las partes (aun parcialmente), nombre de los abogados (o su número de matrícula). Solo los tribunales de trabajo han restringido las búsquedas por nombre del empleado, pues han detectado que los empleadores utilizaban este recurso para verificar si un candidato a un empleo había ejercido acciones laborales contra algún empleador en el pasado: si los hallaban en las bases de datos simplemente no los contrataban por "molestos".

La otra salvedad, visible prácticamente solo en San Pablo, es la posibilidad de litigar en "secreto" con el hecho de pedirlo en la demanda inicial; aquí se observa que muchos abogados piden trámite secreto para "todos" sus procesos. Por ejemplo en Costa Rica existe cierto acceso público (limitado en contenido) y luego con clave de usuario:

> Para tener acceso a esta consulta, se debe de solicitar al despacho que se le habilite un usuario. Con el usuario asignado, podrán consultar cualquier causa judicial en cualquier parte del país en la que usted es parte. Con esto, usted como usuario y nosotros como institución nos aseguramos de la confidencialidad de su información. Si no posee usuario, está habilitada una consulta pública, mediante ella, sin necesidad de usuario, puede buscar sus expedientes, sin embargo, solo se muestra información muy general del expediente.

El bloqueo de robots para acceder a la información procesal pública fue introducido por primera vez por el Tribunal de Hong Kong; en América Latina está siendo usado en Brasil (estados de Rio Grande do Sul y Sao Pablo) y en Argentina en los Tribunales de Buenos Aires.

La modalidad de acceso con usuario y clave solo a los casos propios es la predominante en México, ver por ejemplo Aguascalientes[23] (y también en otros países de la región como Venezuela). En realidad, mientras se mantengan listas de acuerdo absolutamente públicas esta protección es ineficaz. En la medida que existe toda esta gama de acceso es posible entender que hay también argumentos para sostener cada una de ellas. Sin embargo, Brasil no tiene ley de protección de datos personales, aunque sí ha sancionado la Ley 11.111, que autoriza a los Poderes Judiciales a anonimizar cierta información.

Por su parte, existen en Costa Rica muchas demandas dirigidas contra el presidente de la Sala Constitucional y el Director de Informática por datos

[23] http://serviciosweb.poderjudicialags.gob.mx/MAJAT/MasterPage/Pages/Login/Login.aspx

sensibles publicados en el sitio *web*. Las decisiones tomadas por el resto de los magistrados de la Sala Constitucional —obviamente el presidente debe excusarse— es siempre ordenar que se retire la información y reconocerdaños y perjuicios.[24]

Otras publicaciones. Es fácil apreciar —a partir de la revisión de los sitios *web* de los Poderes Judiciales— que existen otras muchas posibilidades o aplicaciones en las que se publica información judicial —jurisdiccional o administrativa— con fines determinados. En algunos casos surgen de una ley (o de una jurisprudencia), como por ejemplo algunos antecedentes penales. En los EE.UU., Canadá y Reino Unido son cada vez más accesibles las personas condenadas por delitos sexuales contra niños (incluso en algunos casos con localizador de domicilio). También en Argentina y Chile se han aprobado leyes para abrir los registros de delincuentes sexuales (en Argentina en las Provincias de Neuquén y Mendoza, pero aun sin implementar y en Chile se permite solicitar los antecedentes "a cualquier persona que cuente con una autorización expresa".[25]

Los casos de incumplimiento de las obligaciones alimentarias también han sido motivo de desarrollo legislativo, originalmente en los EE.UU., y recientemente en Argentina (prácticamente todas las provincias) y en Perú.[26] En este caso se pretende que la publicación es el elemento disuasorio para el incumplimiento de la ley.

---

[24] Ver: Mario Antonio Lobato de Paiva, *Responsabilidade civil do estado - portadores de HIV-AIDS em processos judiciais*, www.legiscenter.com.br/materias/materias.cfm?ident_materias=229

[25] Ley 19.927 (www.dcsc.utfsm.cl/info/nua/Ley_19927_Pornografia_Infantil.pdf), artículo 7 que modifica el Registro Nacional de Condenas en su Artículo 6º *bis*. "Toda institución pública o privada que por la naturaleza de su objeto requiera contratar a una persona determinada para algún empleo, cargo, oficio o profesión que involucre una relación directa y habitual con menores de edad, podrá solicitar que se le informe, para fines particulares, si ésta se encuentra afecta a la inhabilitación establecida en el artículo 39 bis del Código Penal. La misma información podrá ser entregada a cualquier persona que cuente con una autorización expresa de aquel cuyos antecedentes se solicitan, para los fines señalados en el inciso anterior.".

[26] En Argentina el nivel de acceso varía según la provincia, en Mendoza es un registro que lleva el Poder Judicial en el que hay que registrarse personalmente y acceden solo los empleadores, en la provincia de Salta con búsqueda por nombre o numero de documento (www.justiciasalta.gov.ar/deudores-alimentarios-poder-judicial-salta.php) es un sistema web público e irrestricto, al igual que en Perú (http://casillas.pj.gob.pe/redamWeb/) con búsqueda, relación y fotografía del deudor.

En general se discute ampliamente el acceso a los registros de antecedentes penales, por ejemplo en Francia la accesibilidad a una condena en el registro es parte de la decisión judicial, o sea el juez decide según las circunstancias —en cada caso— si el antecedente es accesible o no. También en Argentina la Corte Suprema de Justicia entendió en el caso K.131.XXXIX *Kook Weskott, Matías, sobre abuso deshonesto* que la publicación de la condena es parte del reproche que hace la sociedad a una conducta delictiva.[27] Por ejemplo en varias entidades federativas de México es un derecho de la víctima pedir al tribunal la publicación de la sentencia condenatoria como parte de la pena.

Otras modalidades de publicación que han sido decididas por las autoridades judiciales, son:

- Videoteca de audiencias orales en Nuevo León, México;
- Consulta de Incompetencias, Excusas, Recusaciones y Rogatorias en Jalisco;28
- Procesos disciplinarios, en Uruguay acceso público al registro de abogados suspendidos (en el sitio web del Poder Judicial) y en Costa Rica procesos disciplinarios a jueces y empleados judiciales (también en el sitio web del Poder Judicial;
- Evaluación de los jueces, en el estado de Paraíba, Brasil (últimamente inaccesible);
- Registro de personas privadas de libertad, en el estado Rio Grande do Norte, Brasil (acceso libre con búsqueda por nombre) y en la provincia de Mendoza (acceso por número de caso y el nombre nunca es visible;
- Registro de personas fugitivas de la justicia (sustraídos a la justicia) en el estado de Paraíba, Brasil;

[27] Otro ejemplo es el Registro de Obstructores de los vínculos de los hijos con su progenitor no conviviente y familia extendida que lleva el Poder Judicial de la Provincia de Santa Cruz, en Argentina.

[28] www.stjjalisco.gob.mx/incompetencias/brw_incompetencia.aspx

- En Argentina, Eslovenia y Trinidad & Tobago, acceso a fichas estructuradas sobre casos de daños corporales;29

- Acceso a "juicios universales" (sucesiones, quiebras y concursos) con búsqueda por nombre en el sitio del Poder Judicial de Mendoza (Argentina).

La información judicial como parte de los modelos de negocios en la actualidad

Como se ha dicho, los poderes judiciales han visto la necesidad de ser instituciones transparentes y más eficientes. Para ello han desarrollado muchas aplicaciones en Internet, entendiendo que hacer disponible información cumple inmediatamente con esos objetivos.

Por ejemplo, los Boletines Judiciales o Listas de Acuerdos exponen una gran cantidad de información sensible —como las imputaciones de delitos, conflictos familiares y hasta los conflictos mercantiles en algunos casos— sin embargo ¿garantizan transparencia? ¿contribuyen a la eficiencia? Si se admite que un documento judicial es la suma de distintos tipos de información, la publicación de los acuerdos es en sí misma una "disociación", en la que se publicita la existencia del caso, los nombres de las partes y una decisión parcial generalmente reducida a un descriptor de unas pocas palabras. De hecho la "transparencia esperada" que consistiría en difundir "cómo deciden los jueces, y con qué fundamentos" continua insatisfecha. Si la información procesal difundida "carece de valor legal" —como se dice en algunos sitios— y tiene problemas de calidad, tampoco se ha dado un paso hacia la eficiencia.

En México, varias leyes estatales de transparencia y protección de datos establecen la obligación para los órganos públicos de definir explícitamente la finalidad de sus bases de datos (por ejemplo Colima, Guanajuato, Michoacán, Sinaloa). Pero las aplicaciones informáticas se crean —generalmente— por iniciativa de proyectos informáticos que

[29] Por ejemplo, en Eslovenia: www.sodisce.si/znanje/sodna_praksa/nepremozenjska_skoda/, en Argentina: www.iijusticia.edu.ar, y en Trinidad Tobago www.ttlawcourts.org/digest_index.htm.

son presentadas a los jueces como reemplazos del uso del papel; y no partiendo de una decisión administrativa (un acuerdo del Pleno) que defina los criterios de publicación y la finalidad para generar y difundir bases de datos (y cuando sea necesario reinterpreten las leyes vigentes que ordenan la publicación de acuerdos para diferenciar la publicación que se hace en papel —aun cuando sólo sea para los estados o para la biblioteca— con la que se hace en Internet, y que puede generar otro tipo de riesgos).

En efecto, existen empresas que diariamente descargan la información procesal publicada por los tribunales, la reorganizan y la venden para finalidades poco claras, pero seguramente distintas de las que fundamentarían una decisión formal de un poder judicial. Las finalidades son implícitas, pero al consultar el sitio *web* de una de estas empresas se puede ver:[30] *¿Quieres conocer el historial legal del novio de tu hija?*

Surgen muchas preguntas: ¿Cuando se inicia un proceso judicial ceden las partes sus datos personales? ¿Cuando un poder judicial publica información en Internet, está cediendo datos para que puedan ser utilizados con cualquier otra finalidad? ¿Es la publicación en Internet una cesión indiscriminada? Si se admite que la información judicial es una entidad compleja, cada uno de sus componentes pueden requerir diferentes tratamientos y ser motivo de cesiones condicionadas a determinadas finalidades. Pero es posible publicar en Internet y esperar que la información mantenga su finalidad, o no sea reutilizada. Existen pocas respuestas judiciales a estas preguntas. Una de ellas es la decisión de la Sala Constitucional de la Corte Suprema de Costa Rica que analizando la publicación de los nombres de los condenados en sentencias penales dice: *"La Sala ha desarrollado ese contenido ampliamente y ha considerado violatorio de esos derechos fundamentales la incorporación de antecedentes penales en bases de datos privadas, accesibles al público"*.[31] ¿Es ingenuo pensar que una

[30] Información obtenida en www.bil.com.mx, visitado el 27 de noviembre de 2011.

[31] Sentencia 15421-2008 del 14 de Octubre: "La inclusión de sentencias penales en páginas web es, en efecto, una consecuencia de la publicidad del proceso penal, la cual constituye una garantía fundamental en esta materia, así reconocida en la el artículo 8.5 de la Convención Americana sobre Derechos Humanos. Además, responde al principio de transparencia de las actuaciones públicas y, en particular, de las judiciales pero, lo que es más importante, en el presente caso, es que esa incorporación de las sentencias no resulta contraria al derecho a

vez que la información esté accesible no entre en el "mercado" y pueda entonces ser utilizada con otras finalidades? Cuando la información es el producto, es difícil distinguir entre "mercado" y "mercado negro": si la información se usa para discriminar quien discrimina no necesita "información documental", la discriminación no se fundamenta (un empleador puede recibir un informe telefónico —verbal— que relaciona un candidato a un empleo con un divorcio, una acción legal contra su empleador anterior o incluso vincularlo con un proceso penal o un juicio ejecutivo mercantil).

Aun cuando no todas las discriminaciones son injustas, el problema consiste también en que si la información fluye en el mercado negro, no hay cómo defenderse. Además si la información es incompleta, es muy fácil hacer una interpretación falsa: estar imputado por un delito no hace a una persona un delincuente, no solo está en juego la presunción de inocencia, está también en juego que los poderes judiciales publican en Internet la imputación pero no publican la conclusión del proceso. Hay quienes predican una apertura de las condenas penales; sin duda es mucho más justo y razonable abrir el acceso a los registros penales, que abrir solo el acceso a las imputaciones y mantener en la opacidad las condenas.

Los dilemas y las conclusiones

Del análisis realizado en en parágrafo anterior es posible concluir que el acceso y publicación en Internet de información judicial abre muchas posibilidades de transparencia, eficiencia y seguridad jurídica; y que al mismo tiempo es necesario tener en cuenta y garantizar ciertos derechos como el de protección de datos, el de presunción de inocencia y el de defensa en juicio. También puede verse que deben tenerse especialmente en cuenta los riesgos y las necesidades de información de los justiciables.

la autodeterminación informativa. La Sala ha desarrollado ese contenido ampliamente y ha considerado violatorio de esos derechos fundamentales la incorporación de antecedentes penales en bases de datos privadas, accesibles al público, lo que no ocurre en el presente caso. La sentencia es un hecho histórico, cierto; la información es veraz, por cuanto se transcribe el texto literal de la sentencia y su publicación respondo a las exigencias constitucionales desarrolladas por la Sala."

Las *Reglas de Heredia* definieron un conjunto de criterios que parecen haber sido seguidos por algunos tribunales, aunque también existen posiciones que optan por alguno de los extremos: publicar todo a costa de exponer datos sensibles, o perder transparencia con la excusa de proteger los datos. Una de las conclusiones presentes en la jurisprudencia es la consideración de situaciones particulares, en la que se analiza la ponderación de derechos, la proporcionalidad de la publicación, la necesidad de una ley que determine ciertos casos de disociación, los riesgos y consecuencias de la publicación de datos personales, y los intereses públicos en juego.

También se ve que no es posible una sola modalidad de acceso a la información judicial, ni una única forma de publicación. El sitio en Internet del Poder Judicial de la Provincia de Mendoza en Argentina es un ejemplo interesante, al establecer al menos cuatro formas de acceso según los derechos e intereses en juego. Cuando los tribunales deciden disociar uno de los problemas que encuentran deviene una tarea que requiere personal especializado, que toma tiempo y que no siempre se logra hacer cumpliendo las reglas definidas. Aparte de los costos de contar con un equipo que analice las sentencias y aplique las reglas, siempre existe el riesgo de no disociar un caso que debió disociarse, y que se generen daños cuyo resarcimiento es una responsabilidad del Estado, o sea, un costo adicional no despreciable. Tanto en la raíz del problema como en la solución están presentes los equipos de desarrollo informático. En sus inicios por la incomunicación entre ellos y las autoridades judiciales, que provocó aplicaciones sin un compromiso o aceptación de los jueces. La brecha generacional también tuvo su impacto, muchos jueces no conocían las aplicaciones en Internet o entendían que no había diferencia alguna con el papel. Hoy la comunicación ha mejorado y es esperable que se inviertan los papeles: que sean los jueces los que definan los criterios de publicación y acceso, que realicen una definición explicita de la finalidad de las bases de datos y de las aplicaciones en Internet, y que los programadores e informáticos no excedan sus competencias y no alteren o modifiquen derechos, sin que las autoridades estén advertidas.

Los costos de disociación pueden ser reducidos casi totalmente en la medida que las aplicaciones de procesamiento de texto y los sistemas de seguimientos de casos se vinculen para que las sentencias —y

otros documentos— generen automáticamente marcas en los archivos originales con las características de cada persona mencionada; sean por ejemplo testigos, víctimas, niños o adolescentes, empleados, o incluso figuras públicas. Si los textos contienen marcas invisibles para quien redacta una sentencia, el procedimiento de disociación puede ser rápidamente decidido por el juez firmante, o automáticamente por reglas establecidas por el tribunal. Disponer de una legislación adecuada parece también una necesidad, los jueces no se sienten cómodos creando reglas generales e incluso pueden sentir que no son competentes para decidir en abstracto. Es difícil llegar a conclusiones definitivas y es muy fácil tener una opinión personal; pero hoy es casi imposible apreciar cual será la tendencia definitiva. Los criterios han ido cambiando en los últimos diez años, se pueden apreciar algunas tendencias pero permanece la sensación que mucho está aun por decir. Internet está siendo reevaluado, ya no es posible pensar que es el espacio idílico de libertad que muchos soñaron, porque quedó en evidencia que los intereses económicos y los modelos de mercado han sido determinantes. Si se debilita la neutralidad de la red y el derecho de audiencia resulta violado, ya no puede ser igual la ponderación de derechos que se hizo inicialmente, deberá ajustarse al ambiente real en el que fluye la información. Sin lugar a duda habrá que mantener la expectativa, analizar e interpretar los eventos por venir y repensar el problema una y una vez más.

Referencias

Berners-Lee, Tim (2010) Long Live the Web: A Call for Continued Open Standards and Neutrality Scientific American Magazine,Diciembre, disponible al 13 de diciembre en www.scientificamerican.com/article.cfm?id=long-live-the-web.

Brenner, Susan W. (1992) Precedent Inflation, Transaction Publishers, New Brunswick, Nueva Jersey.

Lobato de Paiva, Mario Antonio Responsabilidade civil do estado - portadores de HIV-AIDS em processos judiciais, disponible al 13 de diciembre en www.legiscenter.com.br/materias/materias.cfm?ident_materias=229.

Ortiz, Paula Jervis (2002) Comentario jurisprudencial. Intimidad y tratamiento de datos personales en el portal del Poder Judicial, 1 Revista Chilena de Derecho Informático.

Tushnet, Rebecca (2008) Power Without Responsibility: intermediaries and the First Amendment, 76 Geo. Wash. L. Rev. 101 disponible en SSRN: http://ssrn.com/abstract=1205674; Jerome A. Barron, Access to the Press—a new First Amendment right, 80 Harv. L. Rev. 1641, 1641, 1653–54 (1967). Disponible al 13 de diciembre en www.thefilterbubble.com/author/eli-pariser.

Elementos fundamentales para la protección de datos personales en la procuración e impartición de justicia

Areli Cano Guadiana

Areli Cano Guadiana

Es Licenciada en Derecho por la Facultad de Derecho de la Universidad Nacional Autónoma de México. Tiene estudios concluidos de Maestría en Administración Pública por el Instituto Nacional de Administración Pública y ha acreditado cuatro diplomados: Derecho Electoral Mexicano (Universidad de Xalapa), Responsabilidades de los Servidores Públicos (INAP), Derecho fiscal (ITAM) y Transparencia y Acceso a la Información Pública (UAM- CIPDF).

En el ámbito de la administración pública, colaboró en la Procuraduría General de la República como abogada instructora. Posteriormente, fue asesora jurídica y parlamentaria en la I Legislatura de la Asamblea Legislativa del Distrito Federal, y después, asesora y coordinadora de asesores de la Presidencia del Instituto Electoral del Distrito Federal. Desde marzo de 2006, se desempeña como Comisionada Ciudadana del Instituto de Acceso a la Información Pública del Distrito Federal.

Es autora de diversos artículos de divulgación en materia de acceso a la información pública, partidos políticos y transparencia. Asimismo, ha participado en calidad de ponente en diplomados, cursos y seminarios relacionados con el derecho de acceso a la información, la transparencia y rendición de cuentas.

Introducción

Los derechos humanos reconocen el derecho a la vida privada como una base sustancial para el respeto a la dignidad de las personas. En este sentido, los estados nación han tutelado normativamente el derecho a la intimidad a través del reconocimiento de las prerrogativas sobre la privacidad, consagradas desde 1948 en el artículo 12 de la Declaración Universal de Derechos Humanos[1], y que actualmente suponen el reconocimiento de un derecho de control y acceso de la información de cada individuo sobre su persona (García, 2007).

El derecho a la intimidad ha definido su ámbito de protección, particularmente a la luz de los avances en las tecnologías de la información y las comunicaciones (TIC), que implican un ritmo acelerado en el intercambio de datos, y que al mismo tiempo, conlleva el deber de estimular su impacto en las garantías que ofrece el Estado a los ciudadanos, a partir de la vulnerabilidad en el uso de la información personal.

En el caso de México, la regulación de datos personales ocurre paulatinamente a la par de los esfuerzos legislativos que tuvieron lugar desde la década de los '70, para garantizar el derecho de acceso a la información pública. En este sentido, al diseñar los mecanismos jurídicos que garantizaran el acceso a la información, se advirtió también la necesidad de proteger la información relativa a la vida privada de las personas que se encontraba en poder de los sujetos obligados por la Ley, por lo que las primeras legislaciones de transparencia[2] consideraron también lo relativo a la protección de datos personales.

Así, el desarrollo de las TIC y el ejercicio del derecho de acceso a la información junto con la protección de datos personales, llevaron a que en algunas entidades como el Distrito Federal, Guanajuato, Colima y Jalisco, buscaran crear una ley que atendiera exclusivamente

[1] Artículo 12 "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." Declaración Universal de los Derechos Humanos, 1948.

[2] Tales como la Ley Federal de Transparencia y Acceso a la Inormación (11/06/2002) o la Ley de Transparencia del estado de Sinaloa (25/04/2002).

la protección de los datos, garantizando el acceso a sus titulares y el adecuado tratamiento de los mismos por terceros.

De esta manera, en octubre de 2008 se publicó en el Distrito Federal la Ley de Protección de Datos Personales para el Distrito Federal, normatividad que se enfoca únicamente a los datos que obran en los archivos del sector público; meses más tarde, en octubre de 2009, se logra su reconocimiento en la Constitución Federal,[3] concibiendo a los individuos como titulares de sus datos personales, y confiriéndoles el control sobre los mismos. Finalmente, el 5 de julio de 2010, se publicó la Ley Federal de Protección de Datos Personales en Posesión de Particulares en el Diario Oficial de la Federación.

En todo, es preciso apuntar que a lo largo de este texto, se abordará la experiencia del tratamiento de los datos personales en el Distrito Federal, por lo que en lo sucesivo se atenderá a la definición de datos personales establecida en la Ley de Protección de Datos Personales del Distrito Federal (LPDPDF), por tratarse de un concepto amplio e incluyente que abarca distintas áreas en el ejercicio de la protección de datos. Así, los datos personales consisten en "la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN, el número de seguridad social, y análogos" (LPDPDF, 2008).

A partir de esta definición, será posible analizar algunos elementos para la protección de datos personales desde la procuración e impartición de justicia. Sin embargo, es preciso comenzar exponiendo un breve diagnóstico sobre el estado que guardan los poderes públicos

[3] Artículo 16, segundo párrafo: "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 públicas o para proteger los derechos de terceros." Y artículo 73, fracción XXXIX- O que faculta al Congreso para legislar en materia de protección de datos personales en posesión de particulares. Fuente: Constitución Política de los Estados Unidos Mexicanos, 2011.

con respecto a estas áreas de la justicia, con el objetivo de comprender el marco de garantías para el ejercicio del derecho fundamental a la vida privada, en el escenario de la construcción de un Estado democrático de derecho.

Procuración e impartición de justicia hacia un diagnóstico integral

La procuración e impartición de justicia, son labores extraordinariamente delicadas en el contexto del pacto social que sustenta la legitimidad del Estado, porque implican la observancia de derechos humanos de especial relevancia como la libertad, y diversos aspectos de la seguridad jurídica de las personas.

De esta manera, diversas instituciones nacionales e internacionales han analizado el estado que guardan la procuración e impartición de justicia en México, a fin de diagnosticar áreas de oportunidad que contribuyan a la construcción de un Estado más sólido y democrático en donde los ciudadanos ejerzan la plenitud de sus derechos.[4] En términos generales, la Organización de Naciones Unidas ha elaborado diagnósticos sobre la justicia en México, a través de distintas relatorías para la independencia de los magistrados y abogados. Así, algunos de los principales elementos que la relatoría especializada encontró durante su visita al país en 2002, señalaron la oportunidad de incidir en la independencia judicial, toda vez que apuntaba como obstáculos la falta de coordinación interinstitucional y la lentitud y burocratización excesiva en los procesos de impartición de justicia, como producto, entre otros elementos, de la falta de profesionalización de los abogados de oficio, y de graves irregularidades en los procesos de detención de presuntos culpables.

A estos factores, se sumaba la percepción de desconfianza y falta de fe de la ciudadanía en las instituciones de administración de justicia,

[4] Estos diagnósticos se presentan de manera más detallada en la ponencia "Elementos fundamentales para la procuración e impartición de justicia y sus desafíos para la transparencia", presentada por la autora en el contexto del 5º. Seminario Internacional *Transparencia y protección de datos personales en la procuración e impartición de justicia*, el cual tuvo lugar los días 20 y 21 de octubre de 2011 en la Ciudad de México, convocado por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, en coordinación con otras instituciones públicas. Memorias en prensa.

que la sociedad juzgaba como espacios en donde tenían lugar la impunidad y la corrupción (ONU, 2002).

Frente a los factores detectados por la relatoría especializada de las Naciones Unidas en su informe, a nivel nacional el máximo órgano de impartición de justicia, la Suprema Corte de Justicia de la Nación (SCJN), propuso estrategias para revertir los principales obstáculos para la impartición de justicia, las cuales fueron delineadas a partir de un diagnóstico sobre el estado de esta materia, redactados en el Libro Blanco de la Reforma Judicial (2006).

De este modo, la SCJN estimó la urgencia de contar con un sistema de impartición de justicia expedito y con capacidad para resolver los conflictos de los ciudadanos mediante la aplicación del derecho, generando seguridad jurídica para el conjunto de la sociedad. En este sentido, la estrategia principal de la SCJN, consideraba la importancia de promover una reforma judicial que atendiera a la reforma del amparo; el fortalecimiento de los poderes judiciales de las entidades federativas; y la reforma al sistema de impartición de justicia penal (Valencia, 2009:15). Un punto importante que arrojó el diagnóstico del Libro Blanco, fue la necesidad de contar con indicadores integrales (cuantitativos y cualitativos) que fuesen accesibles para todos los ciudadanos, y a partir de los cuales se pudiese observar el curso de la impartición de justicia en México, generando así, legitimidad y confianza de la ciudadanía en las instituciones, a través del conocimiento de un diagnóstico más completo. Sin embargo, existen otros elementos que fueron detectados a principios de 2011 por la Relatora especial sobre la independencia de los magistrados y abogados, que inciden en el curso de la interacción entre las instituciones y la sociedad, siendo principalmente el incremento de la violencia, el aumento de la corrupción, las deficiencias estructurales y orgánicas en el sistema judicial, y las violaciones a derechos humanos de quienes se enfrentan a procesos judiciales[5] (ONU, 2011: 9) algunos obstáculos que debe enfrentar el desarrollo del sistema judicial democrático e imparcial.

[5] Al respecto también puede verse el informe de Human Rights Watch (HRW), *Ni Seguridad, Ni Derechos Ejecuciones, desapariciones y tortura en la guerra contra el narcotráfico de México* (2011) en el cual se sostiene que "durante los procesos judiciales, los miembros de las fuerzas de seguridad aplican torturas sistemáticamente para obtener confesiones por la fuerza, y la evidencia sugiere que habría participación de soldados y policías en ejecuciones extrajudiciales y desapariciones forzadas en todo el país. (HRW, 2011:5).

En suma, a partir de estos diagnósticos, se encuentra que el clima de inseguridad y corrupción que prevalece en el país, aunado a elementos estructurales y organizativos relativos a la procuración e impartición de justicia, son factores a partir de los cuales puede reflexionarse sobre la protección de la vida privada desde el tratamiento de los datos personales, como a continuación se presenta.

Tratamiento y gestión de los datos personales

A diferencia de otro tipo de entes públicos, las instancias que atienden a la procuración e impartición de justicia, basan su actuar en gran medida en los datos personales que les proporcionan los particulares al acudir a ellos para dirimir una controversia; en este sentido surge la necesidad de la adecuada protección de esta información. Esto requiere fortalecer los mecanismos y medidas para su resguardo, especialmente considerando el contexto de inseguridad y corrupción que prevalece en el país, y que podría generar un escenario para la vulnerabilidad en el flujo de los datos personales. En este sentido, la eficacia de la protección de la información debe ubicarse fundamentalmente en los procedimientos preventivos no jurídicos, sin perjuicio de que tales procedimientos vengan impulsados o incluso impuestos por instrumentos jurídicos (Del Peso, 2002: 15), esto requiere del compromiso integral de las instituciones públicas para garantizar el buen uso de los datos y custodiar su destino.

Asimismo, la ciudadanía requiere contar con medidas de seguridad para el tratamiento de la información que incluye datos personales, y que en el caso que nos ocupa, radica en la aplicación de la Ley de Protección de Datos Personales del Distrito Federal (LPDPDF), que atiende a los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad,[6]

[6] Artículo 5.- Los sistemas de datos personales en posesión de los entes públicos se regirán por los principios siguientes:
Licitud: Consiste en que la posesión y tratamiento de sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada ente público y deberán obtenerse a través de medios previstos en dichas disposiciones.
Los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
Consentimiento: Se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales.
Calidad de los Datos: Los datos personales recabados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado.
Confidencialidad: Consiste en garantizar que exclusivamente la persona interesada puede

con los cuales se regularán los sistemas de datos en posesión de las instituciones públicas.

Al mismo tiempo, de acuerdo con Del Peso y Ramos (2002: 4-6), es preciso que el tratamiento de la información considere tres dimensiones: confidencialidad, integridad y disponibilidad de la información, es decir, que solamente determinadas personas autorizadas (encargados) pueden acceder al conjunto de datos personales registrados, y custodiarlos en función de los objetivos institucionales, procurando en todo momento, el respeto a la vida privada. En este contexto, conviene mencionar el curso que ha tenido la protección de datos personales desde la experiencia del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (InfoDF), en especial en lo relativo a las instancias de procuración e impartición de justicia del Distrito Federal, a partir la puesta en marcha de la LPDPDF en octubre de 2008.

Con esa base, la LPDPDF contempló una serie de medidas para la protección de este tipo de información,[7] las cuales fueron reforzadas

acceder a los datos personales o, en caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.
Los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.
Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.
El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.
Seguridad: Consiste en garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.
Disponibilidad: Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.
Temporalidad: Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados.
Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.
Únicamente podrán ser conservados de manera íntegra, permanente y sujetos a tratamiento los datos personales con fines históricos.

[7] Identificación o creación y registro de sistemas de datos personales, elaboración y aplicación del documento de seguridad correspondiente a cada sistema, determinación de responsables,

con la emisión de los Lineamientos para la Protección de Datos Personales en el Distrito Federal,[8] en donde se estableció un plazo[9] para que todos los entes públicos obligados por la Ley, registraran sus sistemas de datos personales y notificaran ante el órgano garante, la existencia de su documento de seguridad.

En el caso que nos ocupa, para diciembre de 2011, el Tribunal Superior de Justicia y la Procuraduría General de Justicia, ambos de esta ciudad capital, han registrado un total de cincuenta y seis sistemas de datos personales, que atienden a distintos niveles de seguridad (básico, medio y alto),[10] agrupados de la manera siguiente:

encargados y usuarios de sistemas, entre otras.

[8] Aprobados por el Pleno del InfoDF y publicados en Gaceta Oficial del Distrito Federal el 26 de octubre 2009,

[9] Con fecha límite del 11 de mayo de 2010.

[10] Los sistemas de datos personales, constituyen un conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso; que pueden ser físicos o automatizados, y se integra por los datos que son clasificados por su categoría como académicos, sensibles, identificativos, laborales, patrimoniales, de salud, electrónicos, de tránsito y movimientos migratorios; biométricos; de naturaleza pública; y datos sobre procedimientos administrativos y/o jurisdiccionales. A su vez, los niveles de seguridad de dichos sistemas, se clasifican según la información que contienen como básico, medio y alto, e implican la observancia de ciertos procedimientos como contar con un responsable, elaborar un documento de seguridad, o los controles de acceso, entre otras medidas para el tratamiento de los datos personales. El nivel de seguridad de un sistema lo determina el responsable del sistema en función del tipo de información que los integra, así un sistema puede contar con los uno, dos o con los tres niveles de seguridad. Fuente: Lineamientos para la Protección de Datos Personales en el Distrito Federal. Gaceta Oficial del Distrito Federal. 29 de octubre del 2009.

Cuadro 1. Sistemas de datos personales registrados en instancias de procuración e impartición de Justicia del Distrito Federal, según categorías y niveles de seguridad. 2011.

Ente Público	Sistemas	Categoría de Datos	Total	Nivel de Seguridad		
				Básico	Medio	Alto
Tribunal Superior de Justicia del Distrito Federal	22	Académicos	22	12	0	9
		Datos especialmente protegidos (sensibles)	5			
		Identificativos	132			
		Laborales	18			
		Patrimoniales	8			
		Salud	8			
		Datos sobre procedimientos administrativos y/o jurisdiccionales	9			
Procuraduría General de Justicia del Distrito Federal	34	Académicos	12	2	0	32
		Electrónico	1			
		Datos especialmente protegidos (sensibles)	17			
		Identificativos	416			
		Laborales	3			
		Patrimoniales	1			
		Datos personales de naturaleza pública	3			
		Salud	22			
		Datos sobre procedimientos administrativos y/o jurisdiccionales	14			
		Otra	31			

Fuente: InfoDF, Dirección de Datos Personales, información disponible al 5 de diciembre de 2011.

De lo anterior, destaca que la Procuraduría General de Justicia del Distrito Federal, clasifica la mayoría de sus sistemas de datos con un nivel de seguridad alto (32 sistemas), toda vez que la categoría de datos constituyen aspectos identificativos[11] de las personas que se encuentran sujetas a procesos de averiguaciones previas. Por su parte, el Tribunal Superior de Justicia del Distrito Federal (TSJDF) tiene doce sistemas clasificados con un nivel de seguridad básico, que

[11] Los datos se clasifican según su naturaleza. Así, el artículo 5 fracción I de los Lineamientos para la Protección de los Datos Personales en el Distrito Federal, clasifica dentro de los datos identificativos el nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, y demás análogos.

corresponden en su mayoría a procedimientos para la incorporación de profesionales del derecho para el ejercicio de funciones de impartición de justicia dentro del Tribunal, así como su capacitación a través de cursos y eventos que el TSJDF registra en sistemas de datos básicos.

Asimismo, con respecto al TSJDF, el órgano garante ha advertido que en el listado de sistemas de datos presentado por dicha instancia, no se identifica, por ejemplo, en dónde se resguardan los datos que le cede la PGJDF en materia penal; lo anterior, considerando que los asuntos que resuelve un juez, tienen como base la información entregada por el ministerio público en la averiguación previa.

Lo mismo ocurre con los datos contenidos en expedientes administrados por juzgados de paz, civiles, familiares y de arrendamiento, en ellos la información materia del juicio, constituye información de la vida privada de las partes que actúan en ellos, por lo cual, se advierte un área de oportunidad para la protección de los datos personales que son cedidos en este proceso.

En este contexto es importante señalar que a través de un diagnóstico realizado por el InfoDF al Tribunal, se debían inscribir los sistemas de datos relativos a los expedientes judiciales por cada una de las instancias judiciales a su cargo, a fin de dar cabal cumplimiento a la normatividad en la materia. Esto permite observar la oportunidad para que exista constancia de que la información en cuestión se proteja en todo momento, y se restringa el acceso a todos aquellos que no son los titulares.[12]

Al respecto, conviene mencionar que si bien según se deriva de las normas procesales,[13] el acceso a los expedientes se permite solamente a las partes involucradas, es importante destacar que esta

[12] Fuente: InfoDF (2011). Dirección de Datos Personales, Evaluación al Tribunal Superior de Justicia del Distrito Federal, Mimeo.

[13] Artículo 1. Sólo puede iniciar un procedimiento judicial o intervenir en él, quien tenga interés en que la autoridad judicial declare o constituya un derecho o imponga una condena y quien tenga el interés contrario. Podrán promover los interesados, por sí o por sus representantes o apoderados, el Ministerio Público y aquellos cuya intervención esté autorizada por la Ley en casos especiales. Código de Procedimientos Civiles para el Distrito Federal, publicado en el Diario Oficial de la Federación, el 26 de mayo de 1928. Última reforma publicada en la Gaceta Oficial del Distrito Federal, el 14 de mayo de 2010.

circunstancia no exime a las autoridades de proteger los datos que administren a través de sistemas de datos personales, sobretodo porque la ley establece que las búsquedas de información, cuando se realizan solicitudes de derechos ARCO, se hacen a través de los sistemas.

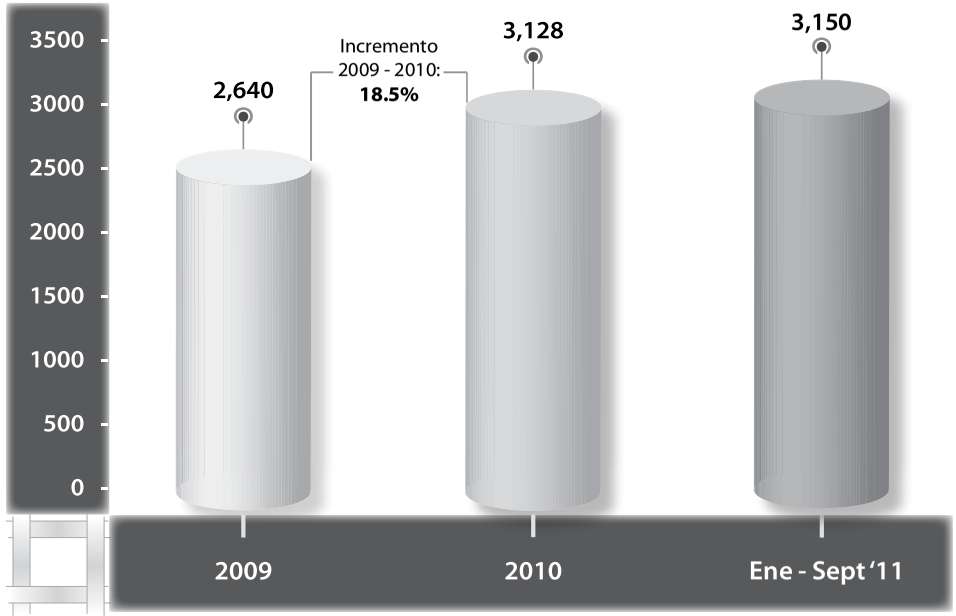
Esta situación conlleva a la necesidad de que los entes obligados atiendan a los principios de la LPDPDF, para actuar en consecuencia.

De igual manera, otra de las áreas de oportunidad detectadas por el órgano garante es que una vez definido el nivel de seguridad del sistema, se debe determinar el tipo de medidas a aplicar, considerando la disparidad presupuestaria, el volumen de información, el tratamiento que se le da y el soporte en el que se encuentra (físico, electrónico o mixto), en tanto que no existen parámetros establecidos que permitan conocer hasta que punto una medida de seguridad garantiza la integridad del sistema.

Por otra parte, la experiencia del órgano garante también da cuenta del avance en el ejercicio de los ciudadanos en sus derechos de acceso, rectificación, oposición y cancelación (ARCO), ha sido el aumento progresivo en el incremento de 18.5% de solicitudes ARCO entre 2009 (2,640 solicitudes) y 2010 (3,128 solicitudes), mientras que el pronóstico de un aumento de 4.2% en las solicitudes de la misma naturaleza que se ubicarán en 4 mil 412 al término de 2011.

La estadística sobre el avance de las solicitudes ARCO de datos personales, se muestra a continuación:

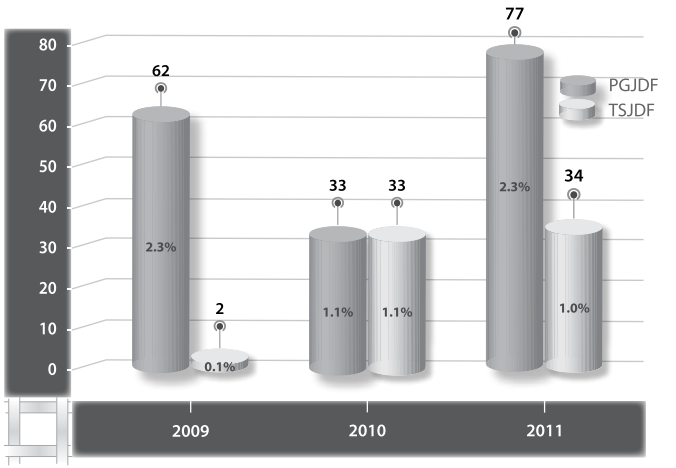
Gráfica 1. Solicitudes ARCO recibidas (2009 - septiembre 2011).



Fuente: InfoDF, Dirección de Evaluación y Estudios.

En especial, esta tendencia se observa en el ejercicio de los derechos ARCO en las instituciones responsables de la procuración e impartición de justicia en el Distrito Federal. Así, se observa que mientras la Procuraduría General de Justicia del Distrito Federal (PGJDF) tuvo un total de 62 solicitudes ARCO en 2009, para octubre de 2011 tenía 77 solicitudes; mientras que el Tribunal Superior de Justicia del Distrito Federal (TSJDF), pasó de 2 solicitudes ARCO en 2009, a 34 antes de terminar el 2011, como se presenta en la gráfica siguiente:

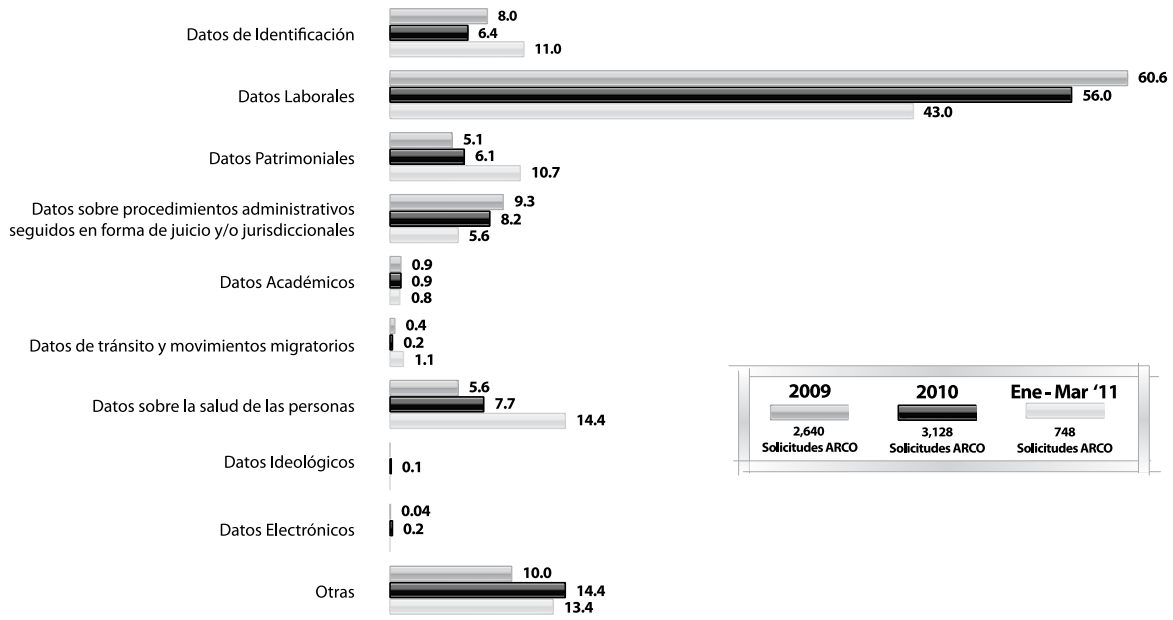
Gráfica 2. Total de solicitudes de datos personales, 2009 - 2011.



Total de solicitudes de datos personales en los Entes Obligados: **2009**: 2,604 **2010**: 3,128 **2011**: 3,292
Fuente: DEE, InfoDF. Información al 11 de octubre de 2011.

Asimismo, de acuerdo con la prevalencia de la categoría en que se clasifican los datos personales, como se mencionó en párrafos anteriores, se tiene que el interés ciudadano para acceder a través de los derechos ARCO, recae principalmente en el acceso a sus datos laborales, como se puede observar en la estadística siguiente:

Gráfica 3. Categoría de datos personales sobre las que recae la solicitud de acceso, rectificación, cancelación u oposición de datos personales, 2009 - primer trimestre de 2011.



Fuente: InfoDF, Dirección de Evaluación y Estudios. Informe estadístico sobre el ejercicio del derecho de acceso, rectificación, cancelación y oposición de datos personales en el Distrito Federal. 2009 - primer trimestre de 2011. Mayo 2011.

Estos datos demuestran también el avance en el proceso de aprendizaje ciudadano e institucional, toda vez que con la aprobación de procedimientos para el ejercicio de derechos ARCO, los solicitantes conocen las vías para la protección de sus datos personales, desde la solicitud de la información hasta la orientación del ente obligado al cual habrán de dirigirla, en medio de un proceso de concientización en el que cada persona se sabe dueña y responsable de sus datos, y tiene información que le permite observar lo que una autoridad puede o no hacer con ellos.

Por su parte, los entes públicos han ido adecuando y eliminando la duplicidad de trámites, a fin de dar respuesta a las solicitudes ciudadanas a través de la expedición de copias certificadas o simples, o para la rectificación de datos personales.

En este proceso de implementación de la LPDPDF, ha sido un proceso complejo, que va más allá de la creación de sistemas y el establecimiento de medidas de seguridad, y que ha implicado también un cambio de visión en torno a su tratamiento, proceso difícil al carecer de una cultura archivística sólida, pues el tratamiento de los datos va desde que su recolección, la cual debe ser en todo momento fundada y motivada, hasta la certeza de su destino final. De esta manera, las instituciones han tenido que modificar formatos y procedimientos, atendiendo con mayor cuidado todos los principios establecidos por la LPDPDF, y procurando el cumplimiento de las medidas de seguridad en su tratamiento. Para ello, los servidores públicos han adquirido los conocimientos sobre el uso de esta información en su quehacer cotidiano, como demuestra el total de 17,839 funcionarios que han sido capacitados en la materia por el órgano garante, de 2009 a noviembre del 2011.[14]

Aunado a lo anterior, la experiencia del órgano garante ofrece áreas de oportunidad con respecto a la interpretación de la ley, en tanto que si bien establece medidas de protección, en algunos casos las excepciones son muy laxas y pueden derivar en incumplimientos a la norma por parte de los entes públicos, o tener criterios interpretativos que implican la discusión entre el derecho de acceso a la información pública y la protección de datos personales, como ocurre por ejemplo,

[14] Fuente: InfoDF, Dirección de Capacitación. *Mimeo.*

en la difusión de datos personales que pudieran resultar de interés público.[15]

El proceso de implementación normativa, plantea así la necesidad de clarificar los conceptos básicos para poder establecer de una manera más clara los alcances de la protección de datos personales dentro de la gestión pública, y de manera específica, en los temas de procuración e impartición de justicia.

En suma, la tarea institucional desde la normatividad que regula los datos personales en la Ciudad de México, persigue el objetivo de que los derechos ARCO sean parte de la política institucional de los entes obligados, que garanticen el establecimiento de sistemas para el tratamiento de la información de esta naturaleza, para evitar su uso con otros fines que pudiesen perseguir el lucro.

Conclusiones

De manera general, existen algunos elementos en torno a los cuales se puede realizar una reflexión para el curso de la procuración e impartición de justicia con apego a estándares más democráticos que consideren el ejercicio ciudadano del derecho a la protección de datos personales, pero también el derecho de acceso a la información pública, ambos competencia del órgano garante a nivel local. Cuestiones tales como la generación de confianza ciudadana en las instituciones judiciales; el diseño para la gestión judicial con profesionales efectivamente capacitados; la armonización normativa para una efectiva rendición de cuentas; y el establecimiento de estándares para la ética pública en la función judicial, constituyen un punto de partida para el fortalecimiento democrático de la procuración e impartición de justicia. [16]

[15] Esta situación se observa desde las excepciones a la protección de datos personales con respecto a cuestiones de procuración de justicia, tal como se encuentra en el artículo 12 de la LPDPDF: "Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones."

[16] Dichos elementos, se encuentran claramente detallados en la ponencia "Elementos

En todo, resulta imperioso contar con diagnósticos integrales que consideren dimensiones cuantitativas y cualitativas, y de cuyo análisis se desprenda un conocimiento efectivo y certero sobre el estado en que se encuentran la procuración e impartición de justicia, de tal modo que sea accesible para la ciudadanía y contribuya a la formación de una cultura de la legalidad.

Asimismo, otro elemento para fundamentar la correcta aplicación de los derechos ARCO, radica en el compromiso institucional para el cumplimiento de la normatividad, atendiendo a la armonización entre las distintas reglamentaciones que pudiesen contribuir conjuntamente a otorgar garantías plenas para el ejercicio de los derechos de las personas. Al respecto, convendría reflexionar sobre la pertinencia de contar con un código de buenas prácticas en torno a la protección de datos personales, que fuese un referente común para todas las instancias, y que en materia de justicia, sea interpretado observando a la unidad del sistema jurídico, y atendiendo a la armonización para evitar antinomias.

Para todo, un elemento central atiende a la ética en la función pública, de tal forma que los responsables de custodiar la información personal que obran en una institución, actúen con apego a la normatividad e impidan la vulnerabilidad de los sistemas de datos.

La protección de esta información desde los ámbitos de procuración e impartición de justicia, se enfrenta a grandes retos en el contexto de una sociedad severamente lastimada por el peso de la violencia, la inseguridad y la corrupción en México.

A nivel institucional, las instituciones públicas se encuentran normadas por leyes que regulan la protección de la vida privada a través de instrumentos nacionales e internacionales implementados por el gobierno mexicano. Sin embargo, existen áreas de oportunidad para el fortalecimiento de la protección de los datos personales en el terreno de la justicia, a partir de los cuales la generación de confianza, el diseño institucional, la armonización normativa y la ética pública

fundamentales para la procuración e impartición de justicia y sus desafíos para la transparencia", presentada por la autora en el contexto del 5º. Seminario Internacional *Transparencia y protección de datos personales en la procuración e impartición de justicia*, el cual tuvo lugar los días 20 y 21 de octubre de 2011 en la Ciudad de México, *Mimeo.*

constituyen elementos importantes para reflexionar sobre el curso de la procuración y administración de la justicia con respecto a la construcción de un país más justo, equitativo y democrático. Esta tarea requiere del esfuerzo conjunto entre sociedad e instituciones públicas, donde la ciudadanía logre participar activamente e incidir en el rumbo de las políticas públicas en materia de procuración e impartición de justicia, y en la demanda y ejercicio responsable de sus derechos.

Referencias

Caballero, José e*l estado de la cuestión.* En: "El acceso a la información judicial en México: una visión comparada." Caballero Juárez, José Antonio, Gregorio G., Carlos, Popkin Margaret, y Villanueva, Ernesto. Instituto de Investigaciones Jurídicas, UNAM, México.

Cano Guadiana, Areli (2011), *Elementos fundamentales para la procuración e impartición de justicia y sus desafíos para la transparencia.* Ponencia presentada en el 5º Seminario internacional *Transparencia y protección de datos personales en la procuración e impartición de justicia*, 20 y 21 de octubre de 2011, Ciudad de México, Distrito Federal. *Mimeo.*

Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación. Última reforma, 13 de octubre de 2011.

Del Peso Navarro, Emilio y Ramos González, Miguel (2002) *La seguridad de los datos de carácter personal*, Díaz de Santos- Informáticos Europeos Expertos, España.

García González, Aristeo (2007), *La protección de datos personales: derecho fundamental del siglo XX. Un estudio comparado.* en: *Boletín Mexicano de Derecho Comparado*, Instituto de Investigaciones Jurídicas, UNAM, número 120, septiembre-diciembre, México.

Human Rights Watch (2011) *Ni Seguridad, Ni Derechos. Ejecuciones, desapariciones y tortura en la guerra contra el narcotráfico de México,* Estados Unidos de América.

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (2011). Dirección de Datos Personales, *Evaluación al Tribunal Superior de Justicia del Distrito Federal.* M*imeo.*

Ley de Protección de Datos Personales del Distrito Federal (2008), Gaceta Oficial del Distrito Federal, 3 de octubre de 2008, México.

Magaloni, Ana Laura (2004) *Escrutinio público de las decisiones judiciales*, en: Islas López, Jorge, "La transparencia en la impartición de justicia: retos y oportunidades", Universidad Nacional Autónoma de México, México.

Organización de las Naciones Unidas, (2002), Comisión de Derechos Humanos, 58ª reunión. *Informe del Relator Especial sobre la independencia de los magistrados y abogados, Sr. Dato'Param Coomaraswamy, presentado de conformidad con la resolución 2001/39 de la Comisión de Derechos Humanos.* Documento E/CN.4/2002/72/Add.1 Información disponible a noviembre de 2011 en la dirección URL http://www.unhchr.ch

Organización de Naciones Unidas (2011). Report of the Special Rapporteur on the independence of judges and lawyers. Mission to Mexico, 18 de abril de 2011. A/HRC/17/30/Add.3

Rodríguez Villafañe, Miguel Julio (2004), *Información sobre la justicia y justicia en la información en Argentina*, en: Islas López, Jorge, "La transparencia en la impartición de justicia: retos y oportunidades", Universidad Nacional Autónoma de México, México.

Serrano Migallón, Fernando (2004) *El Poder Judicial, el Estado de derecho y el desarrollo económico,* en: Islas López, Jorge, "La transparencia en la impartición de justicia: retos y oportunidades", Universidad Nacional Autónoma de México, México.

Suprema Corte de Justicia de la Nación (2006), *Libro Blanco de la Reforma Judicial*, Suprema Corte de Justicia de la Nación, México.

Valencia Carmona, Salvador (2009), *Constitución y nuevo proceso penal*, Revista Mexicana de Justicia, No. 13, IIJ, UNAM, México.

Vázquez González de la Vega, Cuauhtémoc (2010) *Nuevo Sistema de Justicia Penal*. Revista Semestral del Consejo de Coordinación para la Implementación del Sistema de Justicia Penal, Año 1, Noviembre, Número 2, México.

Dilemas conceptuales en torno a la Transparencia y la Protección de Datos Personales en la procuración e impartición de justicia en el Distrito Federal

Miguel Ángel Mancera Espinosa

Miguel Ángel Mancera Espinosa

Procurador de Justicia del Distrito Federal, también se desempeñó como Subprocurador de Procesos y Mandamientos Judiciales en la misma Procuraduría General de Justicia del Distrito Federal. Cuenta con una vasta experiencia en el sector público.

Integrante de la Barra Mexicana de Abogados y Miembro de la Comisión de Derecho Penal de la Barra Mexicana-Colegio de Abogados.

Egresado de la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM), con maestría por la Universidad de Barcelona, España, obtuvo el doctorado con mención honorífica en la Unidad de Posgrado de la Facultad de Derecho de la UNAM. Además es diplomado en Derecho Fiscal, Derecho Penitenciario y Especialista en Derecho Penal por las Universidades de Salamanca y de Castilla - La Mancha, España, así como por la Universidad Panamericana, México.

Cuenta con diversas actividades académicas, especialidades, en universidades del Distrito Federal y de otros estados de la República, así como la autoría y participación en varias publicaciones, entre ellas el “Nuevo Código Penal para el Distrito Federal”.

Introducción

La información es una herramienta fundamental en la toma de decisiones. Quien la posee y tiene acceso a ella, tiene más posibilidades de actuar conscientemente, pero sobre todo, tiene claro como ejercer y exigir sus derechos.

Reflexionar sobre la rendición de cuentas y la transparencia en los asuntos de Estado no es una moda, ni una ocurrencia académica de última hora, como Rodríguez (2004:5) apunta, "la transparencia es un concepto de larga historia intelectual, una profunda raigambre filosófica que halló un lugar centrhal en las construcciones del pensamiento más importantes: desde Platón y Aristóteles, pasando por Kant, Bobbio, Habermas, hasta llegar a John Rawls y muchos otros clásicos contemporáneos".

Hoy la información pública es reconocida como un bien y un derecho de las ciudadanas y los ciudadanos, toda vez que cualquier persona puede y debe tener derecho a ella.[1] Una sociedad mejor informada puede decidir y participar con conocimiento de causa sobre las decisiones gubernamentales que le atañen.

Resulta prioritario que la sociedad conozca la información que está en manos de los entes obligados, con el objeto de que éstos le rindan cuentas. La sociedad debe participar proactivamente en el ejercicio de sus derechos, debe recordar a las y los servidores que tienen una obligación permanente con la sociedad y que sus acciones deben ir encaminadas a ella. Iniciaremos este breve análisis conceptual, con la de rendición de cuentas. En el contexto de la transparencia y la rendición de cuentas, nos encontramos con diversos conceptos que tienen implicaciones particulares en el ámbito de la procuración de justicia, que si bien muchos mencionan en sus ámbitos laborales, pocos son los que realmente conocen su verdadero significado y relevancia. Por tal motivo, en este trabajo se analizarán diversos términos importantes en la intención de abordar con mayor claridad el tema

[1] El derecho de acceso a la información hoy día es considerado como un derecho fundamental. Con la reforma al título primero de la Constitución General de la República de fecha 10 de junio de 2011. De igual manera se le considera en el último párrafo de artículo primero de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

que motiva el presente artículo. Además, se tratará la relevancia social de la función de la Procuraduría de Justicia, así como la importancia de que sus funciones se realicen en armonía con los derechos humanos, particularmente con el derecho a la protección de los datos personales. Posteriormente se analizarán algunos casos de tensión entre el derecho a la protección de los datos personales y los intereses sociales, como el derecho a la seguridad pública, para arribar a un breve ejercicio de reflexión sobre los retos y perspectivas en materia de protección de datos personales en la Procuraduría de Justicia del Distrito Federal.

Análisis Conceptual

En este apartado se abordarán algunos conceptos como el de rendición de cuentas, transparencia, derecho a la información, derecho de acceso a la información, derecho a la intimidad, derecho a la privacidad y derecho de protección de datos personales, los cuales son fundamentales para lograr una mejor comprensión de las tensiones existentes entre el acceso a la información pública y la protección de datos personales, en el contexto de la procuración de justicia en el Distrito Federal.

Rendición de cuentas

En primer lugar se debe señalar que la rendición de cuentas no es otra cosa que la obligación que tiene todo Estado Democrático, de informar a sus ciudadanos respecto de las labores que realiza en representación de ellos. La rendición de cuentas, dice Andreas Schedler "abarca de manera genérica tres maneras diferentes para corregir los abusos de poder: obliga al poder a abrirse a la inspección pública; lo forza a explicar y justificar sus actos, y lo supedita a la amenaza de sanciones" (2006:12).

En términos llanos, la rendición de cuentas se entiende como la obligación que tiene todo servidor público para informar a los gobernados qué hace, con qué lo hace (el presupuesto), para quién lo hace y los resultados obtenidos de su quehacer cotidiano. En otros términos, rendir cuentas es una obligación que tiene cualquier mandatario, con relación a su mandante. Por eso las y los gobernados

de cualquier país que cuentan con gobiernos democráticos pueden exigir de sus gobernantes cuentas claras en el desempeño de sus funciones, esto es, que cualquier ciudadana o ciudadano puede solicitar información relativa a ¿Qué están haciendo sus autoridades?, ¿Por qué lo están haciendo?, ¿Qué cantidad de recursos públicos están utilizando?, ¿A quién están beneficiando?, entre otras.

La rendición de cuentas es un factor fundamental, que contribuye a crear un mejor gobierno, ya que éste nunca aparecerá de manera natural o espontánea, sino que las y los gobernados serán los responsables de inducir a las y los gobernantes a ser cada día más claros y transparentes en su actuar, a través de la rendición de informes periódicos, o bien con algún otro mecanismo de control que puedan ejercer los gobernados[2].

En palabras de Schedler (2006:26,27*),* la rendición de cuentas "...en su dimensión de responsabilidad apunta a la creación de transparencia (aunque siempre relativa nunca absoluta). Su exigencia de información y justificación aspira a iluminar la caja negra de la política. En esto resulta afín a nociones como vigilancia, supervisión y monitoreo."

Transparencia

En nuestros días la transparencia es considerada como un elemento fundamental de cualquier gobierno que se jacte de ser democrático. Una democracia opaca es poco confiable para las y los ciudadanos del país que la sufra, y también para la comunidad internacional, pues ahora nada escapa a la globalización, ni para los organismos internacionales de derechos humanos, los cuales tutelan en todo el mundo el derecho a la información, considerado como un derecho inherente a la naturaleza del ser humano, es decir, un derecho humano. Como el propio Rodríguez (2004:40) señala "La publicidad es la prueba de fuego para el ejercicio del poder, por ello los políticos autoritarios son profundamente recelosos de las exigencias ciudadanas de dar razones, de explicar el porqué de sus decisiones y de transparentar sus documentos y archivos".

[2] La rendición de cuentas, dice Andreas Schedler (2006:12), abarca de manera genérica tres maneras diferentes para corregir los abusos de poder: obliga al poder a abrirse a la inspección pública; lo fuerza a explicar y justificar sus actos, y lo supedita a la amenaza de sanciones.

En términos coloquiales, por transparente se entiende todo "cuerpo que deja atravesar la luz y a través del cual pueden verse de forma clara los objetos". (Larousse, 1604). El que un cuerpo sea transparente, consistirá en dejar al descubierto todo lo que está dentro de sí, es decir, saca a la luz todo aquello que posee, por lo cual no ocultan nada a la vista. Haciendo una analogía al campo del derecho, la transparencia consistirá en que el Estado a través de sus diferentes órganos de gobierno (Ejecutivo, Legislativo y Judicial), deberá otorgar a sus pobladores y ciudadanos una perfecta accesibilidad a la información que mantiene bajo su resguardo. La transparencia, en todo caso, consiste en que el gobierno de cualquier Estado debe poner a la vista de la población y de la ciudadanía en general, sin obstáculo alguno, la información que detenta en sus archivos, para que cualquier persona pueda tener acceso a ella, revisarla, y cuando así lo decida, usarla para los fines que mejor le convengan. La transparencia también implica que el gobierno debe mantener permanentemente la información a disposición de las personas, a fin de que éstas puedan acceder a ella en todo momento. Sin embargo, nunca se logrará que un gobierno sea transparente, si las y los gobernados no son capaces de elevar su nivel de cultura de participación en la cosa pública. Esta cultura deberá crear permanentemente personas que sean capaces de opinar, discutir, evaluar y emitir juicios bien estructurados y fundamentados sobre la actuación de sus gobernantes.

Derecho a la información

El Derecho a la Información en nuestro país tiene su fuente en el texto del artículo sexto Constitucional desde el año de 1977, el cual textualmente decía: "La manifestación de la ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público, el derecho a la información será garantizado por el Estado".[3]

[3] Este derecho fue ampliado o consolidado recientemente con una adición que se dio al texto del artículo citado para quedar como sigue: Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Desde el punto de vista doctrinal se han vertido diversos conceptos respecto del derecho a la información[4]. Sin embargo, en este trabajo se hará alusión solamente a lo expuesto por los Doctores Jorge Carpizo y Ernesto Villanueva, quienes lo definen de acuerdo a lo establecido en el artículo 19 de la Declaración Universal de los Derechos Humanos, estableciéndolo como "…la garantía fundamental que toda persona posee a: atraerse información, a informar y sea informada." (2004:10).

De esta definición se puede apreciar que el derecho a la información comprende tres aspectos o modalidades:

1. El derecho a recabar información. Incluye poder acceder a los archivos, registros y documentos contenidos en los archivos públicos.

2. El derecho a informar. Están incluidas las libertades de expresión y de imprenta y el de constituir empresas informativas.

3. El derecho a ser informado. Este derecho consiste en recibir información objetiva y oportuna.

Derecho de acceso a la información

El Derecho de Acceso a la Información se encuentra circunscrito dentro del derecho a la información, esto es, que éste es el todo y el derecho de Acceso a la Información es parte del mismo. Este derecho es una prerrogativa de toda persona de tener conocimiento de la información en poder del Estado, generada, administrada y en posesión de sus diferentes Instituciones.

Este derecho se elevó a rango constitucional, a través de la adición que se hizo al artículo sexto de la misma, el 20 de julio de 2007[5].

[4] Generalmente se admite que el concepto de acceso a la información se refiere a hechos, datos, noticias, o acontecimientos susceptibles de ser verificados. En este sentido se suele diferenciar de las opiniones o ideas que constituyen la exteriorización del pensamiento de una persona y que implican normalmente, uno o varios juicios de valor. López, (2009:18).

[5] En este día apareció publicada en el Diario Oficial de la Federación, una reforma de gran trascendencia, que se puede calificar como histórica, en el sentido de que a partir de ella habrá un antes y un después en la materia que pretende regular. Crf. Carbonell (2007:2).

Ahora bien, este mismo derecho fue reconocido como fundamental con la reforma de 10 de junio de 2011. "Un derecho fundamental es un ámbito de libertad que la Constitución reconoce a las personas frente al Estado. Esta libertad está protegida por un derecho para que el Estado o sus autoridades no le impidan a una persona hacer aquello para lo que tiene esa libertad" López (2009:17). [6]

Lo anterior debe ser entendido como el derecho de cualquier persona de recabar e investigar información que poseen los diversos entes obligados del Estado, mismo que está protegido por el propio Estado para que nadie impida su libre ejercicio.

La característica más sobresaliente de este derecho es el principio de máxima publicidad, previsto en la fracción primera del artículo sexto constitucional, la cual señala que "Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad".

El términos de la Constitución, el derecho de acceso a la información tiene dos limitaciones señaladas en la fracciones I y II, del segundo párrafo del artículo sexto constitucional y en el artículo 36 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. Es decir, toda la información en posesión de los órganos del estado es pública, y sólo puede restringirse su acceso porque es necesario proteger otros derechos.

De manera específica, la legislación del Distrito Federal prevé que la información en nuestra ciudad será reservada por cierta temporalidad (7 años, inicialmente, pudiéndose prorrogar hasta por otros cinco), cuando encuadre en alguna de la hipótesis establecidas en las 14 fracciones del artículo 37 de la ley referida, y será confidencial

[6] López, nos dice que el objeto de este derecho estriba en: La constitución prevé que: Las personas tienen derecho a conocer los expedientes, reportes, estudios, actas resoluciones, oficios, correspondencia oficial, acuerdos directivas, directrices, circulares, contratos, convenios instructivos, notas, memorándums, estadísticas o cualquier otro registro de la actividad gubernamental sin importar su fuente o fecha de elaboración. Es por esto que en otros países no se habla de derechos a la información, sino de derecho de acceso a documentos administrativos. (2009:27)

cuando reúna los extremos del artículo 38 de la propia ley, así como lo establecido en la Ley de Protección de Datos Personales para el Distrito Federal y los Lineamientos emitidos por el InfoDF.

Derecho a la intimidad

En nuestra sociedad, se puede apreciar con relativa facilidad que existe una contradicción u oposición entre el derecho que tiene una persona a que nadie invada su esfera íntima, y el derecho de la colectividad a mantenerse informados.

De manera cotidiana, comentamos cosas que tienen que ver con la privacidad de algunas personas "públicas", como son los políticos, gente del mundo del espectáculo, deportistas y personas que por sus actividades son sobresalientes en nuestra sociedad. En efecto, hay programas exclusivos de televisión que se dedican a comentar sobre las personas referidas. Ahora bien, existe un dilema entre si la revelación de datos íntimos de una persona por parte de un ente obligado estatal, o una empresa informativa, implican violaciones a la ley.

Sin embargo, se debe apuntar que hay situaciones en la vida íntima de un ser humano que deben ser conocidas por la colectividad, debido a las consecuencias negativas que ésta puede sufrir, por no conocer en detalle algún hecho "privado" de cualquier persona.[7] La intimidad es difícil de definir, puesto que se refiere a lo que cada persona guarda en su interior, en sus pensamientos y deseos. Es lo más importante para la persona, que no quiere compartir con nadie.

Al respecto, Escalante (2010:22) nos dice: "...Tentativamente se podría definir que es íntimo lo que se hace rigurosamente fuera de la mirada de otros, que sólo se manifiesta voluntariamente a unos cuantos."

[7] Ernesto Garzón nos da un ejemplo bastante ilustrativo, al señalar que en 1973, un par de médicos diagnosticaron que Juan Domingo Perón padecía arteriosclerosis y pericarditis y le advirtieron que si asumía el gobierno podría morir en menos de un año. Ambos médicos y la esposa de Perón decidieron guardar la información en secreto, Juan Domingo Perón murió de acuerdo a lo pronosticado y su esposa asumió la presidencia y esto trajo graves consecuencias al pueblo argentino. Cfr. Garzón (2010:13,14).

Derecho a la privacidad

Al entrar al campo del derecho a la privacidad, debemos dejar claro protege dos tipos de situaciones: el derecho a la vida privada y el derecho a la protección de datos personales. Iniciaremos el análisis con el derecho a la vida privada.

De manera cotidiana comentamos sobre la protección a la privacidad y del interés público, como si no existiera problema alguno respecto de su significado. "Lo primero que conviene tener presente es que lo privado es una creación del Estado, mediante la ley. Se configura un acto de autoridad" (Escalante, 2010: 8).

Definir lo que es privado y establecer los medios jurídicos para protegerlo son acciones que cambian dependiendo del tiempo y lugar, ya que depende del tipo de gobierno y el desarrollo tecnológico en cada país.

El espacio de lo privado es muy amplio, abarca un sinnúmero de actividades humanas, muchas de las cuales no son íntimas en estricto sentido, como sería el caso de las comunicaciones, como la correspondencia postal, el teléfono, la correspondencia electrónica. En cambio, el envío de mercancías escapa a este ámbito, pues pueden ser sujetas de revisión por las autoridades aduanales. Otro ejemplo sería el secreto bancario (Escalante, 2010:11,12).

No hay una frontera indudable, de trazo limpio, perfectamente impermeable, porque las actividades de la vida privada se desbordan hacía todos los campos de la vida social. Sin embargo, como Escalante (2010:12) apunta "La actividad no puede abstraerse por completo de lo que la gente hace, en ningún terreno. Tiene el derecho y la obligación de cuidar los intereses colectivos, la seguridad y los derechos de las personas. La dificultad está en saber en qué momento, por qué razón y de qué manera se ven amenazados como para requerir que se ponga un límite a la libertad personal; en mucho se trata de un juicio fáctico: si hay violencia, por ejemplo, está justificado romper la privacidad de un domicilio, si hay sospechas fundadas de actividad delictiva está justificado romper el secreto bancario". En términos generales, se puede afirmar que el Estado puede invadir la privacidad de una persona,

cuando existe un acuerdo social en el que asuntos que causen daños al público generen un interés que justifique irrumpir la privacidad de los individuos.

Dentro de la Declaración Universal de los Derechos Humanos de 1948 no se prevé ninguna limitación específica para el derecho a la vida privada. Sóloen la parte final de la Declaración, en los puntos segundo y tercero del artículo 29, se encuentran reglas que marcan límites generales para el ejercicio de todos los derechos y libertades que enuncia. El artículo referido a la letra dice:

1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.

2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.

3. Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas.

De acuerdo a estas reglas, el ejercicio de los derechos y el disfrute de sus libertades, de toda persona estarán sujetos a las limitaciones establecidas por la ley, con el único fin de asegurar el conocimiento y respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral del orden público y del bienestar general en una sociedad democrática (Novoa, 2008:130).

De lo anterior, se desprende que el interés público tiene prioridad sobre los derechos particulares o individuales, ya que el bienestar colectivo es más importante que el de una sola persona. Novoa (2008) dice que el ámbito más extenso, permanente e importante en que el bien común impone limitaciones a la vida privada, es el de la administración de justicia, en especial en materia penal. Al referirse a la persecución de los delitos, lo hace de la siguiente manera:

> La persecución de los delitos exige que las jurisdicciones correspondientes cuenten con las atribuciones y medios necesarios para investigar los delitos y para determinar a sus responsables, con el fin de que, una vez comprobados suficientemente los hechos y las participaciones, se impongan las medidas penales adecuadas. También deben reconocerse atribuciones y medios a la autoridad para evitar la comisión de delitos y para poner término a los que se están cometiendo.
>
> Para todo ello es necesario, muchas veces penetrar dentro de la esfera privada. Para recoger huellas y pruebas del delito es necesario proceder al registro de moradas y lugares privados, examinar correspondencia y documentación reservada, sostener a los sospechosos a exámenes corporales o psíquicos, fotografiarlos, recoger sus huellas dactilares, tomar sus medidas físicas, etc. (Novoa 2008:133).

Derecho a la protección de datos personales

En este apartado veremos cómo el derecho a la intimidad es muy diferente al de protección de datos personales, en virtud de que la protección de datos[8] involucra a instituciones públicas o privadas que recaban, usan, transmiten y conservan datos de personas físicas, de acuerdo a las atribuciones que tienen las primeras y el objeto social de las segundas.

Los ordenadores de datos representan un peligro inminente para la vida privada de las personas, lo cual ha originado que en países democráticos se hayan creado leyes para regular el manejo de datos personales.[9]

[8] Isabel Davara, los define como: el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. (2007:73).

[9] En el Distrito Federal contamos con la Ley de Protección de Datos personales para el Distrito Federal y los Lineamientos correspondientes emitidos por el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Las normas de protección de datos tienen como fin proteger al individuo frente a un tratamiento ilícito de su información personal. Por tal motivo nos encontramos ante lo que se conoce como derechos Habeas Data, los cuales "Según las particularidades lexicográficas del país de que se trate, puede conceptuársele como una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter persona". (Diccionario de Derecho a la Información, 2006:229)[10]

El estudio de la protección de datos personales —afirma Davara (2007:75)—"…puede estructurarse en un triángulo cuyos tres vértices se denominarían principios, derechos y procedimiento, respectivamente.

Así diríamos que la protección de datos se compone de una serie de principios que, a modo de declaraciones programáticas, establecen los pilares en los que se basa la protección de datos. Los derechos, por su parte, representan la concreción subjetiva del ejercicio de esos principios, es decir, como el titular de los datos de carácter personal pueden ejercer unos derechos que concretan los principios teóricos en los que se basa toda normativa. El procedimiento, finalmente, cerrando este triángulo ficticio, concreta la tutela estatal a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de tales principios".

Más adelante trataremos lo relativo a los principios, derechos y el procedimiento, para hacerlos valer ante los entes obligados y, en su caso, ante el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, a través del recurso de revisión correspondiente.

[10] Estos derechos Habeas Data, los conocemos en México como derechos ARCO, es decir derechos de acceso, rectificación, cancelación y oposición de datos personales, estos derechos están contemplados en la Ley de Protección de Datos personales del Distrito Federal en sus artículo 26 al 30, a través de esos derechos el titular de los datos controla el tratamiento de los mismos, por parte de los entes que los poseen.

Relevancia social de la función de la Procuraduría General de Justicia del Distrito Federal

Después de hacer un breve estudio de los conceptos que pueden causar dilemas en cuanto su interpretación y aplicación en los procedimientos de acceso a la información y protección de datos personales, veremos la relevancia social que tiene la función de la Procuraduría en el Distrito Federal, haciendo hincapié en que la procuración de justicia está a cargo del Ministerio Público.

El Ministerio Público es la institución unitaria y jerárquica dependiente del órgano ejecutivo, que posee funciones esenciales de persecución de delitos y el ejercicio de la acción penal; interviene en otros procedimientos judiciales para la defensa de intereses sociales, de ausentes, menores e incapacitados, y finalmente, asume el papel de consultor y asesor de jueces y tribunales. (Zamudio, 2007:2523)

Inicialmente se debe comentar que, de acuerdo a lo dispuesto en el artículo 21 constitucional, la investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actúan bajo la conducción y mando de aquél en el ejercicio de esta función. El ejercicio de la acción penal ante los tribunales corresponde al Ministerio Público.

De la actividad investigadora se puede afirmar que tiene la calidad de pública, en virtud de que se dirige a la satisfacción de necesidades de carácter social. No debemos olvidar que el delito tiene dos aspectos: uno que obedece a intereses particulares (interés entre el sujeto pasivo y activo), y otro que se vincula con intereses sociales, es decir, el mantenimiento de un orden social para la buena convivencia. En la actividad investigadora siempre se actúa atendiendo los intereses sociales, es decir, atendiendo al orden social establecido. (Rivera, 1982:56).

La procuración de justicia en el Distrito Federal estriba fundamentalmente en investigar los delitos del orden común y perseguir a los probables responsables de los mismos; proteger los derechos e intereses de niñas, niños, adolescentes, ausentes y adultos mayores que se encuentren en situación de riesgo o vulnerabilidad; así como proporcionar atención a los ofendidos y a las víctimas del delito.

No hay que olvidar que el Ministerio Público representa los intereses de la sociedad misma en diferentes ámbitos de la procuración e impartición de justicia. Así, por ejemplo, debe proteger los derechos e intereses superiores de los niños, adolescentes, incapaces, ausentes, personas adultas mayores y otros de carácter individual o social, que por sus características sean vulnerables o se encuentren en situación de riesgo.

En los procesos de lo civil, el Ministerio Público debe intervenir, en su carácter de representante social, ante los juzgados y salas del ramo civil para la protección de los intereses individuales y sociales en general, en los términos que establezcan las leyes; en materia familiar interviene en los juicios relativos a la familia, el estado civil de las personas, sucesiones y todos aquellos del orden familiar en que por disposición legal sea parte o deba darse vista al Ministerio Público, interponiendo los recursos legales que procedan.

En cuanto a las víctimas de delito[11], la Dirección General de encargada de la materia debe proporcionar, establecer y aplicar, lineamientos y políticas victimológicas con enfoques de derechos humanos, perspectiva de género y protección integral a la infancia, para alcanzar el oportuno acceso a la justicia y la restitución de los derechos de los ofendidos y víctimas del delito; así como proporcionar atención jurídica, psicológica, médica y de trabajo social a los ofendidos y víctimas del delito, conforme a los lineamientos que se establezcan en los manuales de normas y procedimientos.

De lo anterior, se pone de manifiesto que, en conjunto, el actuar de la Procuraduría General de Justicia del Distrito Federal es eminentemente de carácter social, la cual debe apegarse ineludiblemente al respeto a los derechos fundamentales de las personas con las que interactúa.

[11]La Procuraduría cuenta con seis centros de Atención a Víctimas de delito: CTA. Centro de terapia de apoyo a víctimas de delitos sexuales; CAVI, Centro de Atención a la violencia intrafamiliar; CARIVA, Centro de Atención a riesgos victimales y adicciones; ADEVI, Centro de apoyo socio jurídico a víctimas de delito violento; CAPEA, Centro de apoyo a personas extraviadas y ausentes y CIVA, Centro de investigación victimológica y de apoyo operativo.

Procuración de Justicia en armonía con los Derechos Humanos

La procuración de justicia comprende aplicar cotidianamente disposiciones y principios contenidos en instrumentos internacionales relativos a derechos humanos, en los que el Estado Mexicano es parte. Esto es de suma importancia porque los derechos humanos[12] son inherentes a cada persona y constituyen herramientas que fomentan el respeto a la dignidad humana. Sin ellos no es posible realizarse plenamente como ser humano. Los derechos humanos universales están contemplados en la ley y son garantizados por ella, a través de los tratados, el derecho internacional consuetudinario, los principios generales y otras fuentes del derecho internacional. En cuanto a los derechos humanos, el derecho internacional establece las obligaciones que tienen los gobiernos de tomar medidas en determinadas situaciones, o de abstenerse de actuar de determinada forma en otras, a fin de promover y proteger los derechos humanos y las libertades fundamentales de los individuos o grupos. Así, recientemente (14 de julio de 2011), en el artículo primero de nuestra Carta Magna quedó establecido , lo siguiente:

> En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece…Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

[12] Generalmente los derechos humanos se incorporan a las constituciones políticas de los diversos países y dentro de ellas se transforman en limitaciones que la carta fundamental pone a las atribuciones de los poderes públicos y en especial del poder legislativo (Novoa , 2008:13).

Por lo anterior, procurar justicia en esta ciudad respetando los derechos humanos es un verdadero reto. En efecto, la sociedad en su conjunto exige a sus autoridades, entre éstas a la Procuraduría capitalina, que combata efectivamente la impunidad y que utilice todos los recursos humanos y materiales que tenga a la mano. La sociedad civil organizada está al tanto de las actividades de esta Procuraduría. Constantemente ejerce su derecho a la información utilizando mecanismos establecidos en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, para conocer sus actividades y resultados, situación que es atendida con diligencia y eficacia.

Tratamiento de los datos personales con apego a los principios establecidos en la Ley de Protección de Datos Personales para el Distrito Federal

El tratamiento de los datos personales se debe hacer con estricto apego a los principios que establece la Ley de datos personales.[13] Al comentar el artículo 5 de la ley, Davara manifiesta:

> A la vista del artículo, podemos especificar que los principios que rigen en el tratamiento de datos de carácter personal son los de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad. Estos principios, que tienen que darse en todo tratamiento de datos, son los que legitiman dicho tratamiento. Si bien el artículo enumera estos principios, consideramos que hay otros como el de información, que posteriormente se incluye y desarrolla en el artículo 9 de la Ley, que también son necesarios con la finalidad de garantizar que el titular de los datos pueda conocer en todo momento dicho tratamiento. (2010:53)

[13] La Ley de Protección de datos personales para el Distrito Federal establece en su artículo 5 los siguientes principios: Licitud; Consentimiento; Calidad de Datos; Confidencialidad; seguridad, disponibilidad y Temporalidad. En el mismo precepto, se establece el concepto legal de dichos principios.

Principio de licitud

El tratamiento de los datos personales abarca desde la forma en que se recaban, usan o migran, es decir, comprende cualquier uso que se les dé. Este principio estriba en que la posesión y tratamiento de sistema obedecerá exclusivamente a las atribuciones legales de cada Ente Obligado y deberán obtenerse a través de los medios previstos en esas disposiciones.

En la Procuraduría General de Justicia del Distrito Federal se recaban y tratan los datos personales, de acuerdo a lo establecido en su Ley Orgánica y su Reglamento, así como el Acuerdo A/010/2002[14] del entonces C. Procurador Bernardo Bátiz. La información se utiliza sólo para los fines para los cuales se recabó.

Principio de Consentimiento

Se refiere a que el interesado otorgue de manera libre, inequívoca, específica e informada, su consentimiento respecto del tratamiento de sus datos personales. En esta Institución siempre se respeta este principio cuando alguna persona solicita algún servicio y, en el caso de la iniciación de averiguaciones previas, se aplica el contenido de lo establecido en el artículo 11 de la Ley de la materia, que a la letra dice:

> Artículo 11.- Los archivos o sistemas creados con fines administrativos por las dependencias, instituciones o cuerpos de seguridad pública, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley.
>
> Los datos de carácter personal obtenidos para fines policiales, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro

[14] Este Acuerdo establece los lineamientos para los agentes del Ministerio Público, en relación a los domicilios de los denunciantes, víctimas u ofendidos testigos de cargo en delitos graves.

real para la seguridad pública o para la prevención o persecución de delitos, debiendo ser almacenados en sistemas específicos, establecidos al efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad.

La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales..." (El resaltado es nuestro)

Principio de calidad de datos

Este principio se refiere a que los datos que se traten deben ser ciertos, adecuados y pertinentes y no excesivos para la finalidad que se recaban. La Procuraduría capitalina sólo recaba los datos estrictamente necesarios para identificar a las personas que solicitan algún servicio, o de las que se ven involucradas en alguna averiguación previa.

Principio de confidencialidad

Este principio fundamentalmente protege el hecho de que sólo el titular de los datos, o su representante legal, deberá tener acceso a ellos o podrá ejercer cualquiera de los derechos de acceso, rectificación, cancelación y oposición (ARCO). En la Procuraduría de esta ciudad se tiene un especial cuidado en el cumplimiento de este principio, ya que cuando existe una petición o una solicitud de información a través de la Oficina de Información Pública, en la que el solicitante sea una persona diferente al titular de los datos, o su representante legal, se les niega el acceso, con fundamento en lo previsto en el segundo párrafo del artículo 32 de la ley de la materia que a la letra dice:

> Artículo 32.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de

datos personales que se formule a los entes públicos se sujetarán al procedimiento establecido en el presente capítulo.
Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al ente público, a través de la oficina de información pública competente, que le permita el acceso, rectificación, cancelación o haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema de datos personales en posesión del ente público". (El resaltado es nuestro)

Principio de seguridad

Consiste en que sólo el responsable de los sistemas de datos o los usuarios puedan efectuar el tratamiento de los datos. La seguridad de los sistemas[15] en la Procuraduría está a cargo exclusivamente por los responsables de los mismos, por tanto queda debidamente garantizada la seguridad de los datos que se administran.

Principio de disponibilidad

Este principio consiste en que los datos deben estar debidamente almacenados de modo que permitan que las personas puedan ejercer los derechos ARCO. Los datos que se recaban y tratan en la Procuraduría están debidamente sistematizados, de tal manera que en cuanto tenemos alguna solicitud de esta naturaleza, se atiende con la diligencia debida.[16]

[15] Actualmente, la Procuraduría capitalina tiene registrados ante el InfoDF un total de 34 sistemas de datos personales.

[16] A partir de la vigencia de la Ley de Protección de Datos Personales de esta ciudad (3 de octubre de 2008), a septiembre de 2011, se han atendido en la PGJDF, oportunamente 170 solicitudes ARCO de datos personales.

Principio de temporalidad

Este principio consiste en que los datos deben ser destruidos cuando dejen de ser necesarios, respecto de la finalidad con la cual fueron recabados. En lo relativo a este principio, en la Procuraduría los datos personales en cada sistema se mantienen el tiempo estrictamente necesario. Cabe señalar que en las averiguaciones previas los datos no se destruyen, pero se bloquean, con el objeto de mantener una estadística y, sobre todo, saber si una persona tiene ya antecedentes en la Institución.

Una vez que se ha expuesto la manera en que se recaban los datos personales y cómo se les trata en la Procuraduría de esta ciudad capital del país, nos abocaremos a explicar los casos en que posiblemente existiera conflicto o tensión entre el derecho de protección de datos personales y el mantenimiento de la seguridad pública.

Tensión entre el derecho a la protección de datos personales y mantenimiento de la seguridad pública

Inicialmente, se debe explicar en forma breve ¿qué es la seguridad pública? Sobre el particular se puede afirmar que es una obligación del Estado, consistente en salvaguardar los intereses de la sociedad, es decir los bienes jurídicos a los cuales tiene cada persona y la sociedad en su conjunto, como lo sería respecto de su persona (integridad física), patrimonio, prevenir y combatir la comisión de delitos. Dicha obligación se cumple por medio de la procuración e impartición de justicia.

Hoy día la seguridad pública, es concebida no sólo como una función que comprende las actividades ejecutivas de prevención, sino también las acciones de investigación y persecución, para que los delincuentes sean enjuiciados y readaptados conforme a las leyes (Plascencia, 2007:3432).

De acuerdo a lo anterior, la seguridad pública contiene actos de prevención y combate a los delitos; esto se da a través de la procuración del Ministerio Público que, como se ha visto, tiene bajo su

encomienda dicha función, de acuerdo a lo establecido en el artículo 21 Constitucional. Por tal motivo dentro de las funciones del Ministerio Público y de todas las unidades administrativas de la Procuraduría, se debe ser muy cuidadoso de compaginar la procuración de justicia con la protección de los datos personales, aunque pueden presentarse casos en los que sea necesario divulgar información específica, con la finalidad de proteger el interés social que la Procuraduría representa.

A continuación se presentan algunos ejemplos que pudieran ejemplificar los dilemas o tensiones existentes entre al derecho a la protección de datos personales y la seguridad pública.

Cuando alguna persona quiere que se le dé información respecto de cuántas averiguaciones previas y por qué delitos, se están tramitando en contra de otra persona "X".

Es obvio que, en este caso, la persona que solicita el dato cree que tiene derecho a contar con dicha información. Sin embargo, una de las características de las averiguaciones previas es la secrecía de las mismas, es decir, no se puede proporcionar información a ninguna persona que nada tiene que ver con el contenido de las indagatorias. Además, de acuerdo a la Ley en materia de transparencia, la información sería de carácter restringido, ya que se trata de una averiguación que está en trámite y, por tanto, es información reservada; en consecuencia la fiscalía que tiene la información requerida debe negar el acceso a ella, fundamentando la negativa en los artículos 37, fracción VII y 42 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y siguiendo el procedimiento establecido en el artículo 50, es decir, debe someter la reserva ante el Comité de Transparencia de la Institución.

Ahora bien, en el caso concreto también se debe restringir la información, en virtud de que si se proporcionara se afectaría la privacidad, el honor y la dignidad de las persona "X", ya que su fama pública se vería afectada, por lo que la información también se niega por ser de carácter confidencial, en los términos de la fracción VII del artículo cuatro de la Ley Transparencia y Acceso a la Información Pública del Distrito Federal, 36, primer párrafo y 38, fracción IV de la misma Ley.

Cuando un probable responsable de algún delito grave o de alto impacto es presentado ante los medios

Hemos visto que la protección de datos personales se rige por diversos principios, sin embargo todos esos principios tienen límites. Así lo afirma Sergio López (2009: 46) "Desde luego que todos los principios arriba descritos admiten excepciones, principalmente cuando los datos hayan sido recabados por un mandato legal o para el cumplimiento de las facultades legales de las entidades gubernamentales."

También ya se ha mencionado que en las averiguaciones previas aplica el artículo 11º de la Ley de Protección de Datos Personales para el Distrito Federal, que permite recabar y tratar los datos de los probables responsables sin su consentimiento. De lo anterior, se concluye que, para el caso que nos ocupa, no es necesario que esta Procuraduría cuente con el consentimiento del probable responsable para recabar sus datos y dar tratamiento a los mismos, ya que es de suma importancia que la sociedad de la capital del país sea informada de la actuación de los Entes encargados de la procuración e impartición de justicia, sobre todo tratándose de casos graves como serían secuestro, robo en casa habitación, homicidio, violación, trata de personas, entre otros.

Hay que resaltar que en este caso existe un aparente conflicto de normas jurídicas, ya que el derecho de protección de datos personales es un derecho fundamental a título propio, distinto del derecho a la intimidad, pero también lo es la procuración e impartición de justicia. Por tanto, el primero es individual y el segundo es para la sociedad en su conjunto.

Con la expresión "conflicto de normas'', los juristas designamos la incompatibilidad de dos (o más) normas del mismo sistema jurídico. Hay que resaltar que en este caso existe un aparente conflicto de normas jurídicas, ya que el derecho de protección de datos personales es un derecho fundamental a título propio, distinto del derecho a la intimidad, pero también lo es la procuración e impartición de justicia, por tanto el primero es para una persona y el segundo es para la colectividad. En efecto, el aparente conflicto de normas de la misma jerarquía se debe resolver atendiendo al interés jurídico que protege,

en el caso de datos personales, el interés jurídicamente tutelado es el interés privado de un particular. En cambio, el interés público consiste en el conjunto de pretensiones relacionadas con las necesidades colectivas de los miembros de una comunidad, protegidas mediante la intervención directa y permanente del Estado; es decir se refiere a la seguridad pública, por lo que la autoridad siempre debe estar atenta a lo que su población hace[17].

Ahora bien, hay que recordar que el fin del Derecho Penal no se reduce sólo al listado de las conductas consideradas como delitos, y de la pena que a cada uno corresponde, sino que, fundamentalmente, su misión es proteger a la sociedad. Esto se logra a través de medidas que, por un lado, llevan a la separación del probable responsable (prisión preventiva) por el tiempo necesario que dura el proceso penal y, en su caso, prisión definitiva cuando el procesado es hallado culpable por el juez de la causa[18].

Por todo lo expuesto, se debe concluir que la presentación ante los medios de un probable responsable, no viola en manera alguna el derecho de protección de datos personales, ya que es más importante el derecho colectivo de procuración e impartición de justicia que se relaciona íntimamente con la seguridad pública, al cual tenemos cada una de las personas que vivimos en el Distrito Federal, que el derecho del probable responsable por los razonamientos referidos.

También se debe hacer patente que es necesario que la sociedad conozca físicamente al o los probables responsables de delitos de alto impacto social con el objeto de que:

---

[17] Tiene el derecho y la obligación de cuidar interés colectivo, la seguridad y los derechos. La dificultad está en saber en qué momento, por qué razón y de qué manera se ven amenazados como para requerir que se ponga un límite a la libertad personal, en mucho se trata de un juicio fáctico: si hay violencia, por ejemplo está justificado romper la privacidad de un domicilio, si hay sospechas fundadas en actividad delictiva está justificado romper el secreto bancario. La evaluación técnica de los hechos lleva implícito un juicio de valor: en concreto, supone la definición de aquellos bienes que la colectividad considera valiosos, fundamentales. indispensables, es decir, de interés público. Escalante (2010:12).

[18] Que el derecho a la vida privada no es absoluto se desprende además, de su clara subordinación a exigencias sociales, permanentes como los son las necesidades de una conveniente administración de justicia en el país. Especialmente en materia penal- pero no en forma exclusiva dentro de este ámbito- instrucción acabada de una investigación requiere que el magistrado pueda averiguar, comprobar y poner en evidencia los hechos que quedan comprendidos dentro de lo que de la intimidad de un ser humano. Novoa (2008:186,187).

> Existen casos en los que resulta necesario para el Ministerio Público, sin prejuzgar respecto a la responsabilidad de un detenido, hacer del conocimiento de la población dicha detención, para dos propósitos fundamentales: cuando se trate de delitos graves y se presuma que el detenido pudo haber cometido delitos en agravio de otras personas, para que dichas víctimas lo identifiquen y pueda robustecerse la sanción que le corresponde; y cuando el alto impacto de la conducta del detenido resulte tal, que sea necesario informar a la población que se logró dicha detención, para la tranquilidad social.[19]

Hay que resaltar que con esta acción no se viola el principio constitucional de presunción de inocencia, ya que jamás en la presentación ante los medios se hace alusión de que fueron hallados culpables de los delitos que se les imputan, sino que son simplemente "probables responsables", ya que la culpabilidad del caso será resuelta por un juez de la materia y quedará conformada o no cuando la resolución de dicho juez cause ejecutoria, esto es, que contra ella ya no se puede interponer recurso alguno. Por estas razones, tampoco se puede afirmar que se etiqueta a las personas presentadas ante los medios como delincuentes.

Retos y Perspectivas

La ciudad de México se ha caracterizado en los últimos años por tener una sociedad participativa. Así lo indican las estadísticas del InfoDF en cuanto al ejercicio de acceso a la información pública y de los derechos ARCO.[20] Esto indica que la población puede tener la información necesaria para participar en la toma de decisiones trascendentales para la vida comunitaria en esta capital, como sería la construcción de una nueva línea del Metro, de una nueva vialidad, de la

[19] Véase el Acuerdo A/004/2005, mediante el cual se emiten los lineamientos en relación con los probables responsables que son presentados ante los medios de comunicación. Este acuerdo se puede consultar en el Portal de Transparencia de la PGJDF, en el artículo 14, fracción I.

[20] Véase quinto informe de actividades y resultados 2010 del InfoDF, en la página 17, se puede apreciar una gráfica en la cual aparece el número de solicitudes de información de los años 2004-2010.

creación de una nueva institución pública. La Procuraduría ha realizado una labor importante para ejercer las funciones que la Constitución le encomienda con respeto a los derechos humanos, particularmente en materia del derecho de acceso a la información y protección de datos personales. Sin embargo, aún queda un vasto camino por recorrer. Entre algunos de los retos se distinguen los siguientes:

1. Es necesario el perfeccionar el marco jurídico de la protección de Datos Personales, sobre todo en el ámbito de Seguridad Pública y Procuración de Justicia, ya que a la fecha no se encuentran contemplados de manera explícita en la Ley de la materia, ni en los Lineamientos expedidos por el InfoDF, disposiciones que resulten aplicables.

2. Se requiere una mayor difusión, entre la población general, acerca de los derechos de información y acceso a la información y en qué consisten. También de los derechos ARCO y cómo se pueden hacer efectivos, para evitar confusiones y aparentes conflictos de normas.

3. Se debe fortalecer la actuación de la Procuraduría General de Justicia en lo que corresponde para asegurar la seguridad pública en la capital del país, respetando los derechos humanos, para lo cual se deberán impartir, cursos, talleres, diplomados a la población del Distrito Federal, de manera presencial o en línea, por alguna institución de educación pública, como podrían ser la UNAM y la UAM.

4. Establecer en los planes de estudio de todas las carreras a nivel licenciatura, la asignatura de Transparencia y Rendición de Cuentas, con el objeto de que los jóvenes estudiantes conozcan en qué consisten los derechos derivados de éstos y la manera en que pueden ejercerlos.

La ciudad de México es actualmente una ciudad de vanguardia. Se ha demostrado que los que la habitamos sabemos resolver nuestros problemas dentro del marco jurídico; por tal motivo, se puede afirmar que los aparentes dilemas o conflictos conceptuales en torno a la transparencia y la protección de datos personales en la procuración e impartición de justicia en el Distrito Federal, serán salvables mediante

el diálogo y la construcción de un entramado jurídico moderno, que esté a la altura de las circunstancias que estamos viviendo en nuestra ciudad.

No hay que pasar por alto que contamos con la mejor Ley de Transparencia y Acceso a la Información Pública en el país. Por tanto, podemos llegar a la excelencia en el contexto de la protección de datos personales y nos seguiremos manteniendo a nivel nacional como la ciudad más transparente.

Referencias

Carbonell, Miguel. (2007) *La reforma en materia de acceso a la información, en Hacía una democracia de contenidos: la reforma constitucional en materia de transparencia*. México, 1ª Ed., UNAM, IFAI, INFODF.

Davara F. Isabel, de Marcos *(*2007) *Breve análisis de la reforma al artículo* 6°, en Hacía una democracia de contenidos: la reforma constitucional en materia de transparencia. México, 1ª Ed., UNAM, IFAI INFODF.

Diccionario de Derecho a la Información, Coord. Ernesto Villanueva 1ª Ed., Porrúa-UNAM, México 2006.

Escalante Gonzalbo, Fernando. *El derecho a la privacidad*. (2010), México, 1ª Ed., IFAI (Cuadernos de Transparencia, vol. 2).

Garzón Valdés, Ernesto. *Lo íntimo, lo privado y lo público*, (2010), México, 1ª Ed., IFAI, (Cuadernos de Transparencia, vol. 06).

Larousse.-Enciclopedia del Nuevo Milenio, (2006), México, T., VI.

Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Ley de Protección de Datos Personales para el Distrito Federal Comentada. Carbonell M. Coordinador, InfoDF, México 2010.

López Ayllón, Sergio (2009). *El acceso a la información como un derecho fundamental: la reforma al artículo* 6° de la constitución mexicana, México, 1ª Ed., IFAI, (Cuadernos de Transparencia), Vol. 17.

Novoa Monreal, Eduardo. (2008), *Derecho a la vida privada y la libertad de información"*, México 7ª, Ed., Siglo XXI.

Plascencia Villanueva, Raúl (2007) *Diccionario Jurídico Mexicano*, México, Vol. P-Z, 1ª Ed., Porrúa-UNAM.

Rivera Silva, Manuel (1982) *El Procedimiento Penal*, México, 12ª ed., Porrúa, México.

Rodríguez Zepeda, Jesús. (2004) *Estado y Transparencia: Un Paseo por la Filosofía Política*, México, IFAI, México.

Schedler, Andreas, (2006) *¿Qué es la Rendición de Cuentas?*, México, 1ª ed., IFAI.

Villanueva, Ernesto (2004) *Temas Selectos de Derecho de la Información*, México, 1ª. Ed., UNAM.

Zamudio, Fix, Héctor (2007) *Diccionario Jurídico Mexicano*, México, Vol. I-O, 1ª Ed., Porrúa-UNAM.

Datos Personales e Información de Interés Público en las Averiguaciones Previas

Darío Ramírez Salazar

Darío Ramírez Salazar

Director de la Oficina para México y Centroamérica de ARTICLE XIX, se desempeñó como Director General Adjunto de la Unidad de Promoción y Defensa de los Derechos Humanos de la Secretaría de Gobernación y realizó trabajo humanitario en la Oficina del Alto Comisionado para Refugiados de las Naciones Unidas (ACNUR), en El Salvador, Honduras, Cuba, Belice, República Democrática del Congo y Angola.

Autor de numerosos artículos con temas de acceso a la información, medios de comunicación, libertad de expresión y derechos humanos. Es columnista invitado de periódicos de circulación nacional como El Universal y Excélsior, así como de El Nuevo Mexicano. Se desempeña como corresponsal de la publicación inglesa INDEX en México. En el radio participa en el programa Radio Trece de Javier Solórzano y es conductor de Zigma en Radio Ibero. También es profesor en la Universidad Iberoamericana.

Es licenciado en Relaciones Internacionales por la Universidad Iberoamericana y Maestro en Derecho Público Internacional por la Universidad de Ámsterdam.

Introducción*

En un Estado Democrático de Derecho se requiere que la actuación de sus instituciones pueda ser sometida al análisis público, por lo que la existencia de previsiones normativas como la del artículo *16 del Código Federal de Procedimientos Penales*[1] (art. 16 CFPP) marcan un retroceso en el respeto y efectividad de los derechos humanos y del escrutinio de la función investigadora de los delitos, ya que al establecer, tanto una estricta reserva en todas las investigaciones de asuntos criminales, así como restricciones para la obtención de copias de la averiguación previa, afecta no sólo a las personas que participan dentro de la indagatoria (víctimas e imputadas), sino que además tiene consecuencias negativas para el derecho a saber de la sociedad y la adecuada rendición de cuentas del órgano encargado de la procuración de justicia (ministerio público).

Asimismo, los casos en que las autoridades encargadas de la procuración de justicia exhiben de forma pública a personas acusadas de ser autoras o partícipes de algún delito, trasciende el tema de publicidad de la actuación estatal relacionada con la investigación de conductas criminales ya que involucran la difusión de datos personales de quienes se encuentran sometidas a un proceso de investigación pudiendo tener un impacto negativo en el ejercicio de derechos como el de la honra, el de presunción de inocencia y debido proceso, que requiere reflexionar sobre la forma en que pueda garantizarse tanto de derecho a la información de la sociedad como los derechos humanos de las personas que han sido acusadas de cometer algún ilícito.

En el presente artículo se analizan dos temas fundamentales en el ámbito de la procuración de justicia: la importancia del acceso a la información de las averiguaciones previas y la protección de los datos personales contenidos en ellas para salvaguardar otros derechos de los involucrados en la averiguación.

*Quiero expresar mi enorme agradecimiento a Iván Báez y Paulina Gutiérrez por el importante apoyo para la elaboración de este texto.

[1] Reforma publicada en el Diario Oficial de la Federación el 23 de enero de 2009

Para ello, el trabajo se estructurará de la siguiente manera: en primer término, se analizarán diversos aspectos que destacan la importancia del acceso a la información de las averiguaciones previas; posteriormente se mostrarán algunas consecuencias respecto el escrutinio social a la procuración de justicia, para, finalmente, realizar algunas reflexiones en torno al tema de la exhibición pública de las personas sujetas a investigación criminal.

La importancia del acceso a la información de las averiguaciones previas

La averiguación previa consiste en el conjunto de diligencias legales que permiten al Ministerio Público determinar la existencia de elementos suficientes para ejercitar la acción penal. Por lo tanto, la publicidad y el acceso a versiones públicas de las averiguaciones previas, son piezas claves para que en la sociedad tengamos el poder de controlar y vigilar el buen desempeño del Ministerio Público como institución fundamental del Estado de Derecho encargada de investigar y perseguir los delitos.

En este orden de ideas, la ausencia de una investigación adecuada y de los medios para verificar dicha situación contradice la idea de un Estado Democrático de Derecho, ya que como lo ha señalado la Corte Interamericana de Derechos Humanos, la obligación de investigar debe cumplirse *"*con seriedad y no como una simple formalidad condenada de antemano a ser infructuosa" por lo que "debe tener un sentido y ser asumida por el [mismo] como un deber jurídico propio y no como una simple gestión de intereses particulares, que dependa de la iniciativa procesal de la víctima o de sus familiares o de la aportación privada de elementos probatorios, sin que la autoridad pública busque efectivamente la verdad*"*.[2] La imposibilidad de acceder a los expedientes de averiguación previa por cualquier persona (incluyendo

[2] Bulacio Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 18 de Septiembre de 2003, párrafos 112 y 114; Comunidad Moiwana Vs. Surinam. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia 15 de junio de 2005 párrafos 146, 148 y 149; 19 Comerciantes Vs. Colombia. Fondo, Reparaciones y Costas. Sentencia de 5 de julio de 2004 párrafos 175, 176 y 184; Juan Humberto Sánchez Vs. Honduras. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 7 de junio de 2003 párrafo 144; Bámaca Velásquez Vs. Guatemala. Fondo. Sentencia de 25 de noviembre de 2000 párrafo 212, entre otros.

periodistas e investigadores/as), evita se realice un escrutinio o evaluación de la función investigadora y persecutora de los delitos (especialmente en aquellos casos donde no se procedió penalmente es decir, no se ejercitó la acción penal) ya que al no existir posibilidad de conocer las acciones realizadas y aquellas que no se pudieron realizar, o sobre si existía una estrategia o metodología para el desempeño de las funciones del ministerio público, se evidencia un amplio margen de discrecionalidad que fácilmente puede convertirse en la actuación arbitraria del órgano de procuración de justicia.

Artículo 16 del Código Federal de Procedimientos Penales

El art. 16 CFPP violenta el derecho a saber, y con ello evita el control y vigilancia sobre el desempeño del Ministerio Público y sus actuaciones, por las siguientes razones:

- Supone la estricta reserva de la averiguación previa y todos los documentos relacionados;

- Sólo permite acceso a la información a versiones públicas de las resoluciones de no ejercicio de la acción penal, cuando haya transcurrido un plazo igual a la prescripción del delito de que se trate (hasta 12 años).

- En ningún caso se podrá hacer referencia a información confidencial relativa a los datos personales del inculpado, víctima u ofendido, así como personas que rinden sus testimonios, agentes estatales o cualquier persona relacionada o mencionada en la indagatoria.

- El Ministerio Público no podrá proporcionar información una vez que se haya ejercitado la acción penal a quien no esté legitimado.

- Permite reservar por el tiempo máximo aquellas investigaciones relacionadas con delitos imprescriptibles –p. ej. los de lesa humanidad y los de guerra- así como los delitos permanentes –como en la desaparición forzada de personas-. Esto último resulta inconcebible cuando en dichos supuestos es donde la transparencia y acceso a la información debiera de prevalecer sin titubeos.

En otras palabras, de acuerdo a este ordenamiento, la información que se proporcionará únicamente es la relativa a "la resolución de no ejercicio de la acción penal", es decir que se limita a una parte de lo contenido en un expediente de averiguación previa sin que necesariamente signifique que se pueda contrastar con todas las diligencias (actuaciones) que se realizaron o se tenían previstas e inclusive fueron solicitadas (por víctimas o por imputadas), así como los/as funcionarias encargadas de las mismas (ministerio público, peritos/as, etc.) y en consecuencia contar con elementos para hacer un auténtico análisis de la eficacia y eficiencia en la procuración de justicia, sea por personas especializadas en el análisis del mismo (investigadores/as), periodistas o cualquier persona.

Datos comparativos nacionales sobre el acceso a expedientes de averiguaciones previas

La situación en el ámbito estatal tampoco es muy esperanzadora: De acuerdo al análisis comparativo en México del acceso a expedientes de averiguaciones previas encontramos lo siguiente:

- En 11 casos se reservan hasta por 12 años: Baja California Sur, Colima, Durango, Guerrero, Hidalgo, Querétaro, Tamaulipas, Tlaxcala, Yucatán, Zacatecas y Federal.

- En 5 entidades se prevé como causal de reserva la de evitar se afecten las labores de seguridad o de una investigación adecuada: Durango, Michoacán, Morelos, San Luís Potosí, Sinaloa.

- En 15 entidades se reserva la información de las averiguaciones previas incluso cuando ya estén concluidas: Aguascalientes, Baja California, Colima, Chiapas, Chihuahua, Guanajuato, Oaxaca, Puebla, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán, Zacatecas.

- Mientras que en 9 entidades la reserva de la información sólo aplica durante el desarrollo de la investigación criminal: Baja California Sur, Coahuila, DF, México, Guerrero, Nayarit, Nuevo León, Querétaro y Sonora.

- En el Estado de Campeche, únicamente se reservan los datos personales confidenciales sin importar el estado procesal de la investigación criminal.

- Por último, en Jalisco se exige que la reserva se ajuste a un aspecto previsto de forma casuística y a su vez esté debidamente fundada y motivada.

Estándares internacionales

De acuerdo a los estándares internacionales, los únicos límites al acceso a la información de un proceso penal, entre las que se encuentran las averiguaciones previas, son los siguientes:

- *Protección a la intimidad* de personas acusadas (Principio 8 relativo a la provisión de información a través de los medios de comunicación, en relación con el proceso penal. Recomendación (2003) 13 del Comité de Ministros del Consejo de Europa)

- *Protección especial* se debe dar a las partes que son *menores de edad u otras personas en situación de vulnerabilidad*, así como a las víctimas, a las personas que rinden testimonio y a familiares de personas acusadas. En todos los casos, deberá tenerse especialmente en cuenta el efecto perjudicial que la divulgación de información que permita su identificación puede tener sobre las personas mencionadas en el presente principio (Principio 8 relativos a la provisión de información a través de los medios de comunicación, en relación con el proceso penal. Recomendación (2003) 13 del Comité de Ministros del Consejo Europeo).[3]

- Respetar *la dignidad, la seguridad* y, a menos que la información es de interés público, el *derecho a la intimidad* de víctimas, demandantes, acusadas y testigos, así como de sus familiares, garantizado por el artículo 8 de la Convención. (Declaración sobre el suministro de información a través de los medios de

[3] Disponible en https://wcd.coe.int/ViewDoc.jsp?id=51365

comunicación en relación con el proceso penal,[4] adoptada por el Comité de Ministros el 10 de julio 2003 en la reunión 848a de los Diputados de los Ministros; Declaración sobre la libertad de expresión e información en los medios de comunicación en el contexto de la lucha contra el terrorismo[5] adoptada por el Comité de Ministros el 2 de marzo de 2005 en la reunión 917a de los Diputados de los Ministros del Consejo Europeo).

- Debido respeto al *principio de la presunción de inocencia y el derecho a la vida privada*. (Declaración sobre la libertad de expresión e información en los medios de comunicación en el contexto de la lucha contra el terrorismo[6] adoptada por el Comité de Ministros el 2 de marzo de 2005 en la reunión 917a de los Diputados de los Ministros del Consejo Europeo).

- Proteger *la seguridad de las víctima*s del terrorismo o de la fuerza pública involucrados en una continua operación antiterrorista, de la investigación o la eficacia de la seguridad o medidas de seguridad, en todos los casos en que las autoridades decidan restringir el acceso, deben explicar las razones de la restricción y su duración debe ser proporcional a las circunstancias y la persona autorizada por las autoridades deberán proporcionar información a los periodistas hasta la restricción ha sido levantada (Declaración sobre la libertad de expresión e información en los medios de comunicación en el contexto de la lucha contra el terrorismo, adoptada por el Comité de Ministros el 2 de marzo de 2005 en la reunión 917a de los Diputados de los Ministros del Consejo Europeo).

La Corte Interamericana de Derechos Humanos[7] ha señalado que si bien es admisible que "en ciertos casos exista reserva de las diligencias adelantadas durante la investigación preliminar en el proceso penal",

[4] https://wcd.coe.int/ViewDoc.jsp?id=51365

[5] http://www.regjeringen.no/upload/KKD/Medier/Declaration%20terrorism.pdf

[6] https://wcd.coe.int/ViewDoc.jsp?id=51355

[7] Cfr. Caso Barreto Leiva vs. Venezuela, sentencia de 17 de noviembre de 2009, serie C 206, párr. 45; Caso Rosendo Radilla vs. México, sentencia de 23 de noviembre de 2009, serie C 209, párrs. 252 y 256.

con el objetivo de "garantizar la eficacia de la administración de justicia", en ningún caso podrá negarse el acceso a la persona investigada, acusada o a las víctimas, por lo que la restricción deberá someterse a la prueba tripartita (legalidad, servir a un propósito legítimo, necesidad y proporcionalidad).[8]

Argumentos del IFAI para dar acceso a averiguaciones previas concluidas

Los argumentos del IFAI para dar acceso a las averiguaciones previas antes de la reforma al artículo 16 del Código antes mencionado, son coincidentes con los estándares internacionales señalados. En ese sentido, y tomando en cuenta el marco jurídico de aquel entonces, había sido reconocido por parte del Instituto Federal de Acceso a la Información el derecho a particulares de acceder a una versión pública de las averiguaciones previas ya concluidas (consignadas o mediante el no ejercicio de la acción penal).

La existencia de una averiguación previa por sí misma, no permite desvirtuar la presunción de inocencia constitucionalmente reconocida, de modo que para que una persona pueda ser considerada culpable del delito que se le imputa debe existir la sentencia de un juez que así lo establezca. En suma, por una parte, la información relativa a la existencia de averiguaciones previas en contra de una persona no puede considerarse un dato personal en términos del artículo 18, fracción II, de la LFTAIPG, y por la otra, la averiguación previa por sí misma no determina la culpabilidad o inocencia del indiciado, por lo que no puede considerarse información confidencial. En este sentido, este Instituto considera improcedente clasificar el nombre de los denunciados, como un dato confidencial en términos del artículo 18, fracción II, de la Ley (Recurso 2389/07).

Inclusive en casos de consulta de información con fines estadísticos (cantidad de averiguaciones previas) se ha utilizado el artículo 16 CFPP para negar el acceso a esa información (amparo 651/2011 ante el 10°

[8] Comité de Derechos Humanos ONU Observación general N° 34 sobre el artículo 19 libertad de opinión y libertad de expresión (CCPR/C/GC/34) traducción en español del 12 de septiembre de 2011, párr. 22; *Caso Usón Rámirez Vs. Venezuela, Excepción preliminar, fondo, reparaciones y costas. Sentencia de 20 de noviembre de 2009. Serie C No. 207, párr.*48

Juzgado de Distrito en materia penal que se mantiene pendiente de sentencia), que se limitó a solicitar:

Folio 0001700170610

Por este medio solicito me informe el número de averiguaciones previas que se han iniciado en contra de los siguientes servidores públicos durante el 2010…

Este ejemplo sirve para evidenciar como al violentarse el principio de máxima publicidad, una persona ha tenido que recurrir a asesoría jurídica especializada (en materia de protección constitucional), a fin de lograr acceder a la información en poder de la PGR, aspecto que de igual forma violenta el derecho a un recurso de revisión expedito.

Consecuencias respecto el escrutinio social a la procuración de justicia

Lo anterior (la falta de acceso a los expedientes vía solicitudes de acceso a la información) es contrario al derecho a la información que a decir de nuestro máximo tribunal (SCJN tesis aislada del pleno P. LXXXIX/96 emitida en junio de 1996) se relaciona con el respeto a *la verdad* y es un derecho básico para el mejoramiento de la conciencia ciudadana y en consecuencia *si las autoridades asumen conductas que permitan atribuirles conductas faltas de ética al entregar información manipulada, incompleta o condicionada a intereses de grupos o personas, incurren en violación grave a los derechos humanos pues conlleva a una cultura de engaño, maquinación y/u ocultación* en lugar de la verdad que permite tomar acciones eficaces y rápidas para llegar a ésta y hacerla del conocimiento de los/as gobernados/as.

Acceso a la Información y perjuicio a las actividades de prevención o persecución de delitos

Al no encontrarse en trámite la averiguación previa no se acredita un perjuicio a las actividades de prevención o persecución de delitos, ni a la actuación que realiza el Ministerio Público durante la etapa en que realiza todas aquellas actuaciones y diligencias necesarias para conocer

la verdad histórica de un hecho posiblemente constitutivo de delito, a efecto de ejercitar o no la acción penal, puesto que la investigación correspondiente ha concluido (Recurso de revisión 114/07).

Al haber concluido las investigaciones a cargo de la autoridad ministerial, la causal de clasificación que prevé el artículo 14, fracción III, de la ley se extinguen, en razón de que concluyeron las actuaciones ministeriales y se recabaron las pruebas necesarias para configurar el cuerpo del delito y la probable responsabilidad del indiciado (Recurso 2319/07).

Aún cuando puedan contener datos personales confidenciales, el expediente de la averiguación previa en sí mismo no puede considerarse como dato personal, sino como información de carácter gubernamental que da constancia de las actuaciones de la autoridad en un asunto específico. El sujeto obligado deberá entregar al recurrente una versión pública del expediente en el que se omitirá exclusivamente los datos personales confidenciales (Recurso de revisión 114/07).

AMICUS CURIAE sobre la acción de inconstitucionalidad 26/2009 de la CNDH

1. Después de esta breve revisión, pongo a su consideración las propuestas que presentamos en el *Amicus Curiae* ante la Suprema Corte de Justicia de la Nación, junto al CIDE: La reforma al artículo 16 del Código Federal de Procedimientos Penales y su contradicción con la Constitución.

2. Debe prevalecer el principio de publicidad y transparencia y el de máxima publicidad en la elaboración del sistema de acceso a la información de las indagatorias ministeriales;

3. Sólo por causas de interés público, debidamente acreditado, se pueden reservar partes de una indagatoria;

4. Toda la información clasificada como reservada, sin excepción, debe estar sujeta a una temporalidad;

5. Por ningún motivo se puede considerar información reservada

aquellas investigaciones que versen sobre violaciones graves a los derechos humanos y sobre crímenes de lesa humanidad;

6. El derecho a la información se debe de hacer extensivo a la averiguación previa, no a una sola resolución final de ésta. Es necesario hacer compatible la regla de sigilo en la investigación criminal con la regla de la máxima publicidad. La primera aparece como una excepción de la segunda. Ello implica que no es absoluta y su procedencia debe ser limitada y debidamente justificada por un interés público superior y legítimo conforme a las obligaciones internacionales;

7. La averiguación previa no puede estar reservada cuando ya se haya determinado el no ejercicio de la acción penal o bien cuando se haya ejercitado acción penal y,

8. La opacidad en la información sobre el desempeño de agentes estatales encargados de realizar una investigación criminal atenta contra el principio elemental que obliga a toda persona que ejerce una función pública a rendir cuentas sobre su labor.

Restricciones para la expedición de copias de la averiguación previa

Respecto las restricciones para la expedición de copias y acceso a la indagatoria para los sujetos que participan dentro de la averiguación previa (acusadas y víctimas), que de acuerdo a la interpretación que se le ha dado al artículo 16 del CFPP (párrafo 2° en relación con el párrafo 7°) ha permitido se impida proporcionar copias del expediente de averiguación previa a las víctimas evitando tengan las condiciones materiales para un adecuado ejercicio del derecho de participación en la investigación criminal, así como para un análisis minucioso sobre la debida actuación del ministerio público.

Ejemplos

En el caso Rosendo Radilla vs México, la Corte Interamericana de Derechos Humanos resolvió que la negativa de expedir copias de un expediente de averiguación previa violaba el derecho humano

a la participación en la investigación y proceso penal (art. 8.1 de la Convención Americana) de las víctimas.

En la experiencia de ARTICLE 19 es necesario el acceso a la información contenida en los expedientes de averiguación previa a fin de que las víctimas puedan evaluar el desempeño de los órganos investigadores, así por ejemplo en el estado de Michoacán se ha limitado por la procuraduría estatal la consulta del expediente ya que, sólo muestran las partes que el agente de ministerio público considera pertinentes de acceso a la víctima, aspecto que notoriamente impide hacer una evaluación exhaustiva de la función ministerial, o en múltiples ocasiones el agente del ministerio público ha solicitado que la consulta del expediente sea en otra fecha por no contar con tiempo o eventualmente ante la ausencia del responsable se ha negado acceso a dicho expediente.

Otro ejemplo es un caso en el estado de Coahuila donde al consultar el expediente de averiguación previa en la Procuraduría estatal, se pusieron a la vista una serie de hojas sueltas y sin numeración, donde fácilmente se podía incluir o quitar alguna información tanto por el órgano ministerial como por cualquier otra persona, y bajo el argumento de la secrecía se impidió fotografiar tal irregularidad.

Efectos de la negativa de copias de los expedientes de averiguaciones previas a las víctimas

La negativa a expedir copias del expediente, limita el ejercicio de los derechos de las víctimas y las obliga -en la mayoría de los casos- a recurrir a asesoría de abogadas/os que eventualmente cobran un cargo adicional por la consulta del expediente en las instalaciones de la procuraduría, asimismo repercute en el análisis exhaustivo del expediente al ser necesario consultarlo en un horario y días que lo permitan las actividades del ministerio público responsable del expediente.

Buenas prácticas

Una alternativa de buenas prácticas realizadas en cuanto el acceso a los expedientes de averiguaciones previas, son los programas del DF (SAP veb 2.0) y de Querétaro (Integr@) puestos en marcha en este año, y están dirigidos inicialmente para que las víctimas del delito puedan conocer vía Internet, el estado de las averiguaciones previas con el objetivo de agilizar y transparentar la consulta de las investigaciones.

Un sistema electrónico de difusión de información similar al del DF y Querétaro puede ser una alternativa viable ya que podrían salvarse aquellos datos considerados sensibles.

Exhibición pública de las personas sujetas a investigación criminal

Con la reciente resolución del pasado 16 de noviembre de 2011 por la que el InfoDF anunció que *"la difusión del nombre y la fotografía de detenidos (sic) por la presunta responsabilidad de la comisión de un delito no constituye una violación a la Ley de protección de Datos Personales del Distrito Federal"* (LPDPDF), se actualiza la discusión sobre si la exhibición pública de personas acusadas de cometer un delito viola o no su derecho a la privacidad, y si en todo caso resulta pertinente para informar a la sociedad de las acciones tomadas por el estado para la procuración de justicia.

El InfoDF[9] argumenta que la exhibición ante los medios de comunicación de las personas acusadas de cometer un delito *"atiende a una causa de interés público vinculada con la prevención del delito, la seguridad y la procuración de justicia"* y se ajusta a los principios de *"licitud, consentimiento y confidencialidad"* por lo que el acuerdo A/004/2005 del Procurador de Justicia del Distrito Federal y la práctica de esa institución se ajustan a derecho.

[9] Boletín disponible en http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1085&Itemid=999

Contrario a lo señalado por el InfoDF, la Comisión de Derechos Humanos del Distrito Federal (CDHDF) precisó desde noviembre de 2011 que emitiría *"una recomendación contra la presentación ante los medios de comunicación de personas detenidas"* [10] ya que debería ser hasta el auto de formal prisión cuando esa práctica podría justificarse, al respecto la CNDH se ha manifestado de forma similar considerando que serían "flagrantes violaciones" a la persona que ha sido exhibida.[11]

Es evidente que los organismos públicos mencionados (InfoDF y CDHDF) tienen una visión diferenciada respecto el tema, no obstante eso no significa que los derechos señalados (libertad de expresión y derecho al honor) se encuentren en un conflicto real. Por el contrario, un análisis realizado desde la perspectiva de ponderación de derechos permite articular los diversos derechos señalados en aparente conflicto y procurar se favorezca a las personas con la protección más amplia.

El tema de exhibición mediática de las personas sometidas a una investigación por su probable participación criminal, aborda varios aspectos, por lo que se desarrollaran brevemente cada uno de ellos iniciando por lo relativo a la publicidad del proceso penal,[12] que tiene la función de evitar que la administración de justicia sea secreta, relacionándose con la necesidad de transparencia e imparcialidad de las decisiones judiciales que sea respetuosa del derecho a la presunción de inocencia.[13]

Bajo el argumento de la publicidad y búsqueda de imparcialidad en el proceso, el estado tiene la obligación de evitar una condena previa y por tal motivo garantizar la presunción de inocencia,[14] el derecho a la intimidad o a la honra y la dignidad de las personas sujetas a una

[10] http://www.eluniversal.com.mx/ciudad/108708.html

[11] http://www.informador.com.mx/mexico/2010/170429/6/presentan-detenidos-ante-los-medios-viola-sus-garantias-derechos-humanos.htm

[12] Caso Palamara, párr. 168

[13] Caso Herrera Ulloa vs Costa Rica, párrafo 153. Caso Cantoral Benavides, párrafo 120.

[14] Segunda Sala SCJN Amparo en revisión 89/2007. 21 de marzo de 2007. Cinco votos. Ponente: Genaro David Góngora Pimentel. Secretario: Marat Paredes Montiel. *"El principio de presunción de inocencia que en materia procesal penal impone la obligación de arrojar la carga de la prueba al acusador…".*

investigación ministerial. En este punto es necesario hacer un paréntesis para señalar que no sólo es una obligación estatal sino un deber correlativo de los medios de comunicación (deontológico) el proteger la dignidad y honra de las personas,[15] además de tener una función social que cumplir respecto a vigilar y divulgar el funcionamiento gubernamental a fin de generar opinión pública,[16] y contribuir al progreso cultural de la sociedad. En cuanto a la decisión del InfoDF en la que señalan que la exhibición en medios se ajusta a los principios de licitud, consentimiento y confidencialidad, debe precisarse que la licitud sólo se satisface si se apoya en ley previa que sea accesible[17] y se justifique como necesaria y proporcional,[18] contemplando un recurso efectivo[19] para inconformarse de su implementación;[20] en cuanto al consentimiento[21] de acuerdo a la ley (art. 11 LPDPDF) se concede la obtención de datos personales no así su divulgación, por lo que la confidencialidad de una persona se encuentra en una posible vulneración que inclusive podría volverse un trato degradante,[22] toda

[15] Opinión consultiva 5/85, párr. 69

[16] Cfr Opinión Consultiva 5/85 párr. 70; caso Herrera Ulloa, párr. 112

[17] Cfr. ONU-CDH Observación general No. 34, párr. 25; CoIDH *La Colegiación Obligatoria de Periodistas* (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85, párr. 40. *Ver también*, *Caso Tristán Donoso*, párr. 77; *Caso Kimel*, párr. 63, y *Caso Claude Reyes y otros Vs. Chile. Fondo, Reparaciones y Costas*. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párr. 89; Caso Usón Ramírez, párr. 55.

[18] Cfr. *La colegiación obligatoria de periodistas*, párr. 46, *Caso Claude Reyes*, párr. 91; Comité de Derechos Humanos, *Aduayom y otros c. Togo* (422/1990, 423/1990 y 424/1990), dictamen de 12 de julio de 1996, párr. 7.4.; European Court of Human Rights, *Case of The Sunday Times v. United Kingdom,* Judgment of 29 March, 1979, Series A no. 30, para. 65; y *Eur. Court H. R., Case of Barthold v. Germany*, Judgment of 25 March, 1985, Series A no. 90, para. 58; African Commission on Human and Peoples' Rights, Media Rigths Agenda and Constitucional Rights Project v. Nigeria, Communication Nos 105/93, 128/94, 130/94 and 152/96, Decision of 31 October, 1998, para 54.

[19] Cfr. *Caso Acosta Calderón*, párr. 93; *Caso de las Hermanas Serrano Cruz*, párr. 75; *Caso Tibi, supra* nota 206, párr. 131; Caso Palamara Iribarne, párr. 184

[20] Cfr. caso Maritza Urrutia, párr. 99 y 103;

[21] A manera de ejemplo el TEDH en el caso Gaskin vs Reino Unido (7 de julio de 1989, serie A no. 160, párr. 37) evidenció la importancia del tema relativo a contar con el consentimiento de las titulares de la información considerada confidencial.

[22] Voto 990-07 Sala Constitucional Costa Rica, respecto la inclusión de fotografías de personas en el "Álbum de Sospechosos del organismo de Investigación Judicial" sin consentimiento, misma que se considera implica una violación al derecho a la intimidad.

vez que con la exhibición pública se hacen de dominio público diversos datos que no necesariamente se relaciona con los fines de *prevención del delito, la seguridad y la procuración de justicia*. Entre los datos difundidos con la exhibición pública (en casos de delitos graves) se encuentran:

- Nombre
- Fotografía
- Alias
- Voz (eventualmente)
- Diversas impresiones fotográficas (vg. caso DDP/006/2011[23])
- Delitos por los que una persona es probable responsable

Lo anterior eventualmente es coincidente o deriva de la información contenida en expedientes de averiguaciones previas. Es evidente que los datos difundidos con la exhibición pública se relacionan más con las características que permiten la individualización de la persona acusada y, por tanto, sus datos personales, que con las formas de realización del delito, las zonas o personas afectadas y posible identificación de otras personas involucradas tanto directamente (participes) como indirectamente (autoridades que por omisión o negligencia influyen en la impunidad).

La exhibición pública y privacidad[24] *de datos personales*

A diferencia de lo señalado por el INFODF la exhibición ante medios se refiere más a un asunto de privacidad que a una política preventiva del delito o de interés público. Así el estándar internacional apuntalado por el Tribunal Europeo de Derechos Humanos respecto la vida privada de una hace evidente *"reitera la importancia fundamental de su protección con el fin de asegurar el desarrollo de la personalidad*

[23] Se refiere a la difusión de un comunicado de prensa de la PGJDF en el que se dan a conocer diferentes impresiones fotográficas, información y delitos relacionados con violencia familiar, secuestro y homicidio, por los que una persona es probable responsable. http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=1085&Itemid=217

[24] El uso de "privacidad" se da en el sentido de "privacy", es decir abarcando no sólo el derecho a la intimidad. Este derecho se encuentra reconocido en los artículos 16 de la Constitución Política de los Estados Unidos Mexicanos, 12 de la Declaración Universal de Derechos Humanos y 11 de la Convención Americana sobre Derechos Humanos, así como en la resolución 45/95 de la Asamblea General de la Organización de naciones Unidas por la que se establecen las directrices de protección de datos.

de cada ser humano. Tal protección se extiende más allá del círculo familiar privado para incluir una dimensión social."[25] De forma similar el Comité de Derechos Humanos de la ONU en su Comentario General No. 16 sobre *"El derecho al respeto a la privacidad, la familia, el hogar y la correspondencia, y protección al honor y la reputación"* estipuló:

> La opinión del Comité es que se requiera que se garantice este derecho contra toda interferencia y ataque, ya sea de las autoridades Estatales o de cualquier persona natural o jurídica. Las obligaciones impuestas por este artículo requieren que el Estado adopte medidas legislativas y de otro tipo para efectuar la prohibición contra tales interferencias y ataques, así como la protección de dicho derecho.[26]

Así, el tema de la exhibición pública de personas ante medios al tratarse de un asunto relacionado con la privacidad de los datos personales requiere que su restricción se base en los mismos requisitos establecidos para la libertad de expresión, como la ha precisado el *Relator Especial de Naciones Unidas en la promoción y protección de los derechos humanos y las libertades fundamentales al contrarrestar el terrorismo*:

> …a pesar de las diferencias en la redacción, el artículo 17 del Pacto debe interpretarse que contiene los elementos de prueba de los límites permisibles. Las restricciones que no están previstas en la ley son "ilegales" en el sentido del artículo 17, y las restricciones que no cumplen lo necesario o no sirven a un objetivo legítimo constituyen una interferencia "arbitraria" con los derechos previstos en el artículo 17. En consecuencia, las limitaciones al derecho a la privacidad u otras dimensiones del artículo 17 están sujetas a una prueba de limitaciones permisibles, según lo establece el Comité de Derechos Humanos en su comentario general No. 27 (1999).[27]

[25] TEDH Biriuk v. Lituania (Solicitud no. 23373/03), 25 de noviembre de 2008

[26] Comité de Derechos Humanos de Naciones Unidas, Comentario General No. 16: El derecho al respeto a la privacidad, familia, hogar y correspondencia y la protección del honor y la reputación (Art. 17): . 08/04/1988.

[27] Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales al contrarrestar el terrorismo, Martin Scheinin, A/H RC/1 3/37, 28 de diciembre 2009.

De esta forma y a fin de evitar que se dé una interferencia "arbitraria" a la privacidad de las personas acusadas de haber cometido algún delito, la autoridad deberá concederles en todo momento los derechos de:

- Informar sobre su tratamiento;
- Acceso,
- Rectificación,
- Cancelación/bloqueo,
- Objeción u oposición,
- Recurso efectivo,
- Reparación

En este punto es indispensable reiterar que el consentimiento para la difusión de los datos personales deberá ser inequívoco.

Exhibición pública, ¿asunto de interés público?

El InfoDF señaló que con la exhibición pública (tal cual se establece en el acuerdo A/004/2005) bajo la premisa del interés público, se busca lograr la colaboración de la sociedad en la persecución criminal (identificación de imputadas, presentación de nuevas denuncia y/o se proporcione mayor información), pero esa situación podría fácilmente cumplirse en otras etapas como cuando se dicte la formal prisión o se condene a la persona, ya que antes de ello opera totalmente la presunción de inocencia no obstante se haya involucrado al poder público en una controversia y en consecuencia se considere relevante para el interés público,[28] aspecto que operará como excepción que deberá estar debidamente justificado para evitar el uso arbitrario.[29]En este sentido, ARTICLE 19 ha propuesto la siguiente definición que:

> …el término "asuntos de interés público" se define en forma extensa para incluir todos los asuntos de legítimo interés público. Esto incluye de manera enunciativa, más no limitativa, los tres poderes del gobierno -y, en

[28] Greenbelt Cooperative vs.Bresler 398 U.S.6 de 1970.

[29] Cfr. caso Maritza Urrutia, párr. 99 y 103;

> especial, los asuntos relacionados con figuras públicas y funcionarios públicos- política, salud pública y seguridad, orden público, asuntos económicos, ejercicio del poder y arte y cultura. Sin embargo, no incluye, por ejemplo, asuntos meramente privados en los que el interés público es sólo obsceno o sensacionalista.[30]

La CoIDH también ha señalado al analizar el artículo 13.2 de la CADH que el interés público se refiere a aquellos asuntos *"en los cuales la sociedad tiene un legítimo interés de mantenerse informada, de conocer lo que incide sobre el funcionamiento del Estado, afecta intereses o derechos generales, o le acarrea consecuencias importantes."*[31]

La exhibición pública puede tener en las personas diversas secuelas negativas que afectan su derecho a la honra, una de ellas deriva de que la información al difundirse en Internet y no obstante sea rectificada y eventualmente se suprima la fuente original, esos datos permanecerán ad infinitum evitando se ejerza el derecho al olvido[32] que todas las personas tienen. Incluso la Corte IDH ha señalado que *las consecuencias del proceso penal en sí mismo, la imposición de la sanción, la inscripción en el registro de antecedentes penales, el riesgo latente de posible pérdida de la libertad personal y el efecto estigmatizador de la condena penal impuesta (…)*[33] en determinados casos no serían proporcionales ya que bajo la idea del derecho penal mínimo se tiene que en "*una sociedad democrática el poder punitivo sólo se ejerce en la medida estrictamente necesaria para proteger los bienes jurídicos fundamentales de los ataques más graves que los dañen o pongan en peligro.*[34]"

[30] ARTICLE 19, Definición de Difamación: Principios de Libertad de Expresión y Protección de la Reputación, julio de 2000.

[31] Cfr. Caso de Ricardo Canese v. Paraguay, párr. 98,

[32] Agencia española de protección de datos: Procedimiento de tutela de derechos TD/266/2007; Corte Suprema de Justicia Argentina, caso Sejean, Juan B. c/ Zaks de Sejean (1986); U.S.A Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931)

[33] *Caso Kimel,* párr. 85

[34] *Cfr. Caso Tristán Donoso, párr. 119; Caso Kimel,* párr. 76.

De igual forma en la etapa de investigaciones criminales se debe salvaguardar el derecho que tiene toda persona acusada a no auto incriminarse y a no expresarse o mantener el silencio como ejercicio del derecho autónomo a la libertad de expresión, ya que esos derechos se ven afectados cuando una persona se ve forzada a mostrarse públicamente.[35] Lo anterior tiene relación estrecha con el derecho de toda persona a la presunción de inocencia, por lo que el estado no deberá condenar informalmente (incluyendo en medios de comunicación) a una persona o emitir un juicio mientras no se acredite su responsabilidad penal por un juzgado.[36]

De esta forma con relación a la exhibición pública de personas acusadas de cometer un delito podría operar como regla general la no exhibición salvo que se justifiquen con gran rigor (cumpliendo las exigencia de la prueba tripartita) las razones por las cuales de forma excepcional deberá mostrarse mediáticamente a dichas personas, o ¿acaso la exhibición pública de las personas sujetas a investigación es una exigencia de un estado democrático y, por tanto, hay interés público de que se difunda esa información para prevenir los delitos y coadyuvar con la procuración de justicia?

* Elaborado con el apoyo de los licenciados Juan Antonio García Villa, Armando Arias Díaz Barriga y Aldé Lovera Ramírez.

Referencias

ARTICLE 19 (2000) *Definición de Difamación: Principios de Libertad de Expresión y Protección de la Reputación*, julio.

Agencia española de protección de datos (1986) *Procedimiento de tutela de derechos TD/266/2007*.

Comité de Derechos Humanos ONU (2009) *Observación general N° 34 sobre el artículo 19 libertad de opinión y libertad de expresión*. (CCPR/C/GC/34) traducción en español del 12 de septiembre de 2011, párr. 22; *Caso Usón Rámirez Vs.*

[35] Cfr. caso Maritza Urrutia, párr. 99 y 103;

[36] Caso Lori Berenson Mejia, párr. 160; Caso Tibi, párr. 182

*Venezuela, Excepción preliminar, fondo, reparaciones y costas. Sentencia de 20 de noviembre de 2009. Serie C No. 207, párr.*48

Comité de Derechos Humanos de Naciones Unidas (1988) *Comentario General No. 16: El derecho al respeto a la privacidad, familia, hogar y correspondencia y la protección del honor y la reputación (Art. 17).* 08/04/1988.

Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales al contrarrestar el terrorismo (2009) *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales al contrarrestar el terrorismo, Caso Martin Scheinin.* A/H RC/1 3/37, 28 de diciembre 2009.

Tensión y dilemas en la protección de los datos personales

Salvador Guerrero Chiprés

Salvador Guerrero Chiprés

A partir de marzo del 2006, es Comisionado Ciudadano del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Es Doctor en Teoría Política Contemporánea, por la Universidad de Essex, Inglaterra, maestro en Comunicación por la Universidad Iberoamericana y Licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México. Además ha asistido a diversos eventos nacionales e internacionales sobre privacidad y protección de datos personales.

Se ha desempeñado como docente e investigador en la Universidad Iberoamericana en el Departamento de Comunicación, en la Escuela de Graduados en Administración Pública y en el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México, donde se encuentra con licencia. Tiene una amplia trayectoria como periodista, por la cual recibió el Premio Nacional de Periodismo en 1997. Actualmente es comentarista en el Instituto Mexicano de la Radio, además, fue comentarista en el programa Para Empezar, en Stereo Rey (hoy Multivisión); articulista en los periódicos unomásuno y La Jornada y reportero en Canal 13. En el 2010 se amparó junto con otros ciudadanos en contra del RENAUT por considerar dudoso su beneficio en el contexto de la ausencia de seguridad de los sistemas de datos personales. Ese recurso únicamente procedió para algunas empresas privadas.

Introducción

La protección de los datos personales y la esfera de la privacidad adquirieron relevancia en México y se fortalecieron en Europa y Norteamérica. Las nuevas tecnologías permiten el flujo acelerado y diversificado de los datos, por lo que aumentan los riesgos para los individuos, quienes también en esa materia se encuentran desprotegidos.

De igual forma, el avance tecnológico facilita que el individuo pueda acceder a la información de manera más rápida, sencilla y económica. Así, mientras el derecho de acceso a la información se ha potencializado, los riesgos que amenazan a los datos personales se han incrementado de manera proporcional, lo que da como resultado una inevitable tensión aparente entre ambos derechos, que para muchos se trata únicamente de establecer y equilibrar el flujo de datos y seguridad protectora.

A aquella tensión, si sumamos los inminentes perjuicios que las personas pueden sufrir por una violación a sus datos personales (sin mencionar los riesgos para la seguridad nacional, ante la probabilidad de una violación generalizada a una base de datos pública o privada de más de 70 millones de cédulas, cómo las del IFE, SEGOB o Telcel) hacen necesaria la redefinición de conceptos y legislaciones, a fin de adecuarlas a los rápidos cambios impuestos por la tecnología.

Los términos asociados a la protección de los datos personales atraviesan por un amplio abanico de disciplinas, en donde el área jurídica representa el espacio para la materialización de la teoría, pero no agota las acepciones de los conceptos.

Tales circunstancias dificultan la posibilidad de construir y compartir, nacional e internacionalmente, un mismo aparato conceptual, pero sobre todo complican la aplicación, con el mismo sentido de urgencia, de un aparato normativo que es casi desconocido y aún muy poco regulado.

A partir de este contexto, en la primera parte se resumirá el debate alrededor de algunas contradicciones normativas y teóricas que implica el derecho de acceso a la información para evidenciar la tensión natural que existe entre los términos asociados a la transparencia y a la protección de datos.

En el segundo apartado, las afirmaciones previas se ejemplificarán con casos prácticos, que reflejan la complejidad de conciliar leyes y

conceptos al momento del ejercicio efectivo del derecho de acceso a la información, donde se incluye a la protección de datos por ser su opuesto más evidente.

Por último, en la tercera parte del artículo se desarrollan algunos puntos relativos al tratamiento internacional que reciben la protección de los datos personales y la privacidad.

Tensiones conceptuales entre el acceso a la información y la protección de datos personales

Los datos personales no existen de forma aislada, sino que deben entenderse como parte del amplio conjunto que constituye el acceso a la información, no sólo en el aspecto jurídico, sino también teórico. Los elementos vinculados a la transparencia y al acceso a la información pública tienden a encadenarse; es decir, la mayoría de los conceptos precedentes y de los surgidos a partir del derecho a la información se complementan unos con otros. Un ejemplo es la trilogía normativa que, en términos generales y según nuestra experiencia, integra el concepto de transparencia: *Acceso a la información – Ley de archivos – Protección de datos personales.*

Como bien decía Saussure en relación al sistema de la lengua: "Los datos del lenguaje no existen sino por sus diferencias, que no valen más que por sus oposiciones. Una palabra, por sí sola, no significa absolutamente nada. Sólo por oposición, por "vecindad" o por diferenciación con otra, un sonido por relación con otro sonido, y así sucesivamente" (Benveniste, 1977: 34).

No es un asunto lingüístico; lo que se pretende es mostrar las tensiones en los conceptos relacionados con el acceso a la información, incluidos los datos personales. Esto se plantea como una característica inherente a toda clase de construcciones teóricas, susceptible de analizarse a partir de la relación que guarda con otros conceptos y cuyo contraste genera sentido mutuo.

Entonces, se tiene que el acceso a la información es una idea multidimensional, porque involucra conceptos e ideas que tensan y delimitan los derechos de acceso a la información y de protección

de datos personales. De esta relación se derivan varios conceptos igualmente opuestos; por lo tanto, las fronteras entre esos elementos muchas veces no son claros. ¿Quién define lo que es intimidad y privacidad? ¿Hasta dónde termina el derecho de acceso a la información y empieza el derecho a la protección de datos? ¿Lo privado puede ser público para otros? ¿Pueden ser opuestos el derecho privado y el público o el primero debe contrastarse con el derecho de acceso a la información (DAI)? La teoría y la legislación sobre transparencia operan a un elevado grado de abstracción, incluso a un nivel procedimental; por tanto, alcanzar las metas sugeridas con la incorporación de la transparencia en los gobiernos requiere del establecimiento de "un contexto específico en donde se defina por unanimidad el concepto, se materialicen esos términos en políticas públicas objetivas y se valore la función costo-beneficio de transparentar la información gubernamental" (Fenster, 2005: 40).

Del mismo modo ocurre con la protección a los datos personales. Al ser un concepto encadenado al de acceso a la información, se define mediante oposiciones abstractas, entre las cuales la más evidente es que "para el derecho de acceso a la información, el principio fundamental lo constituye la publicidad, en cambio, para la protección de los datos personales lo será el consentimiento a la hora de recabar los datos, tratarlos o comunicarlos a terceros" (García González, 2006: 10) y la pretensión de proteger ciertos aspectos del individuo fuera de la esfera pública.

Existen múltiples aproximaciones sobre el significado y alcances del derecho a la protección de los datos personales, pero en todas ellas hay un elemento común: la identificación de un "núcleo esencial" en la vida de las personas, compuesto por "algo" que los individuos perciben como "fuera" o "excluido" de un supuesto ámbito de "lo público". Los conceptos entrecomillados son subjetivos y no es posible entender lo mismo para cada uno de ellos, por lo que puede percibirse cierta ambigüedad, que se acrecienta al insertar cada debate nacional o internacional fuera de los límites que constituyen y separan la vida privada, la privacidad, la intimidad y nociones semejantes. Desde una de las perspectivas, "la vida privada no es una realidad natural que nos venga desde el origen de los tiempos, sino más bien una realidad histórica construida de manera diferente por determinadas sociedades. No hay una vida privada cuyos límites se encuentren definidos de

una vez por todas, sino una distribución cambiante de la actividad humana entre la esfera privada y la pública" (Duby, 2001: 19). También se tiene la visión jurídica, donde la privacidad es "la prerrogativa que tienen los individuos para no ser intervenidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público" (Villanueva, 2003: LXXIV). Además, se habla de que "el derecho a la vida privada o a la intimidad personal debe ser considerado como un derecho humano fundamental, inherente al individuo que no puede ser limitado por la ley" (Mirón Reyes, 2006: 46).

En México, específicamente en el Distrito Federal, los antecedentes se encuentran en la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, el cual señala en los artículos 9 y 10 que la vida privada es aquella que no involucra una actividad pública y que por ende es intrascendente y sin impacto en la sociedad de manera directa. Además, la vida privada excluye, en principio, a terceros, que no deben tener acceso alguno debido a que las actividades desarrolladas no son de su incumbencia, ni les afecta.

El derecho a la vida privada se materializa al momento que se protege del conocimiento ajeno a la familia, domicilio, papeles o posesiones y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público, cuando no son de interés público o no se han difundido por el titular del derecho.

Asimismo, en la citada ley también se establece que el derecho a la intimidad forma parte del derecho a la vida privada, ya que el primero se desarrolla en un ámbito estrictamente privado, el cual no se hace del conocimiento de terceros y no es de interés público, ya que el titular del derecho no lo ha difundido. Puntualiza también que a pesar de que se difunda sin consentimiento del titular de estos derechos, la información no pierde su calidad de íntima o privada. Paralelamente al derecho a la vida privada, en la misma ley se reconoce el derecho al honor, que según el artículo 13, es la valoración que las personas hacen de la personalidad ético-social de un sujeto y comprende las representaciones que la persona tiene en sí misma, que se identifica con la buena reputación y la fama.

Después, en el año 2008, con la publicación de la Ley de Protección de Datos Personales para el Distrito Federal, se establece que el titular de los datos personales tiene el control de sus datos para decidir el motivo y destinatario de su entrega, así como la determinación de quiénes los manejarán; con ello se pretende evitar que sean utilizados por sujetos distintos a los que el titular consintió para su tratamiento.

En esta segunda década del siglo, con la proliferación de gadgets de toda índole –*Smartphones, Tablets*, entre otros– y de redes sociales como *Twitter* y *Facebook*, las nociones de lo privado, esfera privada, privacidad e intimidad comenzaron a unificarse ante la necesidad de traducirlas en leyes y normas; por tanto, fue en el derecho donde se intentó suprimir la tensión entre conceptos.

Warren y Brandeis, en el clásico The Right of Privacy de 1890, dieron el primer salto al trasladar la idea de la privacidad del individuo a la sociedad; sin embargo, "la intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva, resultado del cauce tecnológico" (García González, 2007: 15).

Con el uso de las redes sociales se observa cómo la variable generacional determina la noción de esfera privada y esfera pública, aunque también influyen aspectos culturales como estrato social, región, ingreso, educación y otros factores.[1] Para la mayoría de las personas de entre 40 y 70 años, que precedieron la época de las computadoras e internet, el uso de *Facebook* es una especie de atentado a la privacidad, puesto que no sólo se permite, sino que se fomenta que cualquier persona tenga acceso a detalles privados e incluso íntimos del individuo, incluidas las fotografías y el fenómeno recientemente nombrado como *sex posting*. En cambio, las personas de entre 13 y 39 años ubican a las redes sociales dentro de su esfera privada, ya que en ellas encuentran el espacio perfecto para compartir su privacidad y hasta su intimidad con amigos y conocidos o para ampliar su esfera de interacción. La conclusión de este ejemplo es que resulta relativamente sencillo encontrar las oposiciones que constituyen el concepto general de lo privado, esto a pesar de que

[1] Esta afirmación se presentó y defendió por varios expertos durante la 32a Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que se llevó a cabo bajo el título de *Privacy Generations* en Jerusalén, Israel, del 27 al 29 de octubre de 2010.

factores tan evidentes como la edad o la actitud frente a las nuevas tecnologías modifican las barreras entre lo público y lo privado; no obstante, la idea de transparencia resulta más problemática. Resulta evidente la tensión que existe entre los derechos relacionados con el acceso a la información, ya que en muchas ocasiones no es posible identificar en dónde termina un derecho y comienza el otro. A esta dificultad debe sumársele el factor de las nuevas tecnologías, que a pesar de potencializarlos, también los pone en riesgo.

Prácticas de la protección de datos personales

Más allá de su instrumentalización política, la transparencia es muy difícil de abordar teóricamente. Sus múltiples dimensiones y contradicciones intrínsecas complejizan cualquier intento por agotar el concepto. Lo mismo ocurre con la protección de los datos personales, que se materializa a partir de la correcta puesta en práctica de los llamados derechos ARCO (Acceso, Rectificación, Cancelación, y Oposición). La actual Ley de Protección de Datos Personales del Distrito Federal (LPDPDF) establece los procedimientos y plazos para ejercer este derecho. A partir de ella, el Instituto de Acceso a la Información Pública y Protección de Datos del Distrito Federal (InfoDF) se ha encargado de garantizar la correcta aplicación de dicha ley, por lo que ha resuelto algunos casos que reflejan las tensiones mencionadas.

En el ejercicio de los derechos ARCO se han suscitado conflictos entre la atribución legal de publicar los Boletines Laborales vía internet y el derecho de los particulares a oponerse a que los motores de búsqueda, al indexar el nombre del demandante, remitan directamente a las páginas donde se encuentran dichas publicaciones. Muestra de ello, fue la tramitación ante el Instituto de Acceso a la Información Pública del Distrito Federal del Recurso de Revisión RR. 1490/2010 promovido en contra de la Junta Local de Conciliación y Arbitraje del Distrito Federal, en el que la solicitante requirió al Ente público que se eliminara la información publicada en Internet del expediente laboral del cual es parte actora de los resultados de búsqueda de la Web Google.

En este sentido, el instituto analizó y en discusión plenaria, estableció el límite entre la obligación legal de la publicidad de los Boletines

Laborales y Judiciales y el derecho de oposición a la publicación de dichos Boletines vía Internet para evitar que los nombres de las partes sean indexados y como resultado, se remitan a las páginas de los buscadores.

La justificación que la ciudadana daba para solicitar la oposición de sus datos personales era que la información contenida en los boletines publicados por la Junta Local la habían llevado a sufrir discriminación laboral, ya que a través de ellos sus empleadores se enteraron de que siete años atrás había interpuesto una demanda por despido injustificado contra la empresa en que laboraba en ese entonces.

Ante tal solicitud, la Junta Local se negó a la cancelación de los datos bajo el argumento de que en su sistema de datos personales, a cargo de la Coordinación de Recursos Humanos, no se tenía registro alguno del nombre de la ciudadana. Al recibir esta respuesta, la ciudadana interpuso un recurso de revisión. Sostenía que independientemente de que su nombre no apareciera más en el sistema de datos de la Junta Local, éste ya había sido publicado en los boletines Laborales, los cuales aún estaban disponibles en Internet. Lo que llevaba consigo una supuesta discriminación laboral. En la discusión se pudieron observar los siguientes elementos: al tomarse el nombre como un dato personal y que el titular de los datos personales es el único con capacidad de decidir sobre su difusión, transmisión y tratamiento, en el ejercicio del derecho de oposición a la publicidad de un nombre de una parte que confluye en un juicio, se determinó que no se lesiona al interés público. La finalidad, se dijo, del Boletín o Lista, es la de notificar a las partes de la actividad jurisdiccional —y que puede identificarse con otro elemento como lo es el número de expediente.

Sin embargo, se consideró que a fin de evitar que los nombres de las partes sean indexadas en algún motor de búsqueda y se arroje como resultado el vínculo donde se encuentra la página del Boletín Laboral, la Junta Local de Conciliación y Arbitraje del Distrito Federal, debería de adoptar mecanismos que evitaran la indexación de los vínculos donde se encuentran los Boletines e impedir así se muestren como resultado de dichas búsquedas.

Incluso se comentó que el motor de búsqueda *Google* establece su procedimiento para eliminar una página o un sitio de los resultados

de la búsqueda, dicho procedimiento se encuentra en la página de ayuda de este motor, en la que informa que es necesario que el Webmaster retire la información de Internet para que ésta desaparezca del buscador o indicarle a *Google* que no rastree o indexe la página. Finalmente, el Pleno del InfoDF determinó que la JLCA debía orientar a la ciudadana para que presentara su solicitud de oposición a través de otra petición, pero esta vez no a través del derecho de acceso a la información, sino vía datos personales.

La importancia del asunto radicó en la novedad de la situación, pues nunca se había presentado un recurso de datos personales, al menos a nivel local, con tantas contradicciones legales: por un lado había que proteger los datos personales de la ciudadana, pues su publicación afectaba directamente su situación laboral. No obstante, por disposición legal, la JLCADF debe dar a conocer en su Boletín Laboral electrónico los resultados de los juicios que ahí se procesan, los cuales incluyen los nombres de las empresas y de los trabajadores involucrados. Era evidente la tensión normativa y procedimental entre las obligaciones de transparencia del Ente Público y la LPDPDF.

En otro asunto, los días 20 y 21 de octubre de 2011 se llevó a cabo el 5° Seminario Internacional organizado por el InfoDF. Ahí, Pedro Salazar habló sobre los dilemas conceptuales y jurídicos entre el derecho de acceso a la información pública y el derecho de protección de datos personales.

Estimó que los problemas de aplicación deberán resolverse en cada caso concreto, pues habrían de definirse las circunstancias que obliguen a que la protección de los datos personales ceda frente al interés público.

Además, propuso que en aquellos casos en que el conflicto entre normatividades fuera inevitable, deberá optarse porque prevalezca el derecho de interés público.

En el caso antes expuesto, se identifica ese dilema a partir de la práctica del derecho a la protección de datos personales y se evidencia que, al menos durante su aplicación, las leyes en materia de transparencia y protección de datos personales tienen lagunas que muchas veces son espacios de tensión entre ellas.

También en el marco del 5° Seminario Internacional, Ernesto Villanueva expuso los resultados preliminares de un estudio sobre impartición de justicia, del que concluyó que las instituciones y organismos públicos, sin importar su ámbito de competencia, debían contar con un sólido aparato sancionador, que les permitiera castigar a quienes no acataran sus resoluciones. En el caso de la ciudadanía mencionado, hubiera sido ideal que el InfoDF tuviera el poder de obligar a la empresa a borrar los datos de su buscador.

Otra de las oportunidades que tuvo el InfoDF para aplicar el derecho a la protección de los datos personales ocurrió el 19 de mayo de 2011, cuando el Director de Quejas y Orientación de la CDHDF, después de remitir una queja presentada ante dicha Comisión contra la Procuraduría General de Justicia del Distrito Federal (PGJDF), solicitaba al InfoDF que investigara los hechos y recomendara cómo debía proceder la Comisión para garantizar la correcta protección de los datos de la quejosa. La ciudadana estaba inconforme con la difusión de un boletín de prensa que incluía, sin consentimiento, su nombre y el domicilio donde habitaba al momento de la detención. Tal comunicado aparecía en la página electrónica de la PGJDF, por lo que desde el momento en que la queja fue recibida, el InfoDF ordenó el retiro inmediato del boletín, al menos mientras duraba la investigación y se emitía una respuesta.

El InfoDF consideró como una infracción a la LPDPDF el que en un boletín de prensa la PGJDF consignara el domicilio particular de la persona detenida, ya que se violaba el principio de confidencialidad de los datos, puesto que ese sitio no guardaba relación alguna con el lugar donde se suscitaron los hechos presumibles de delito.

También se dio vista a la Contraloría General Interna de la PGJDF del DF, porque se determinó que la Procuraduría transgredió el principio de temporalidad de la LPDPDF al mantener la información publicada en su portal de internet por un plazo que excedió al necesario para la integración de la averiguación previa, además de que omitió inscribir su Sistema de Averiguaciones Previas en el Registro de Sistemas de Datos Personales del InfoDF, a lo que también está obligado por ley.

Sobre la denuncia, se determinó la licitud de que el sujeto obligado diera a conocer en su comunicado de prensa el nombre, la edad y la

fotografía de la presunta responsable, por tratarse de un delito grave, así tipificado por el Código Penal del Distrito Federal. De nueva cuenta se puede observar la tensión que existe entre el derecho de acceso a la información pública: El Ente Público cumplió con sus obligaciones de transparencia al dar a conocer cierta información socialmente relevante, pero al mismo tiempo esta acción se oponía al derecho de protección de datos personales, ya que esos datos, debido a circunstancias específicas y en apego a la LPDPDF, ya no eran susceptibles de ser divulgados. Si bien es cierto que la protección de datos personales es un derecho de vanguardia y que su ejercicio y difusión apenas comienza, el InfoDF ha sido pionero en México al establecer criterios para resolver asuntos donde se limitan y tensan el derecho de acceso a la información y la protección de datos.

La experiencia internacional en protección de datos

Desde hace varios años se han promulgado leyes para proteger la privacidad en relación a los datos personales. Esta tendencia inició en los países más desarrollados, simultáneamente, entre los más involucrados en asimilar la experiencia autoritaria europea, y paulatinamente se extendió hacia las demás naciones. En Latinoamérica, el reconocimiento de la necesidad de legislar en torno a la privacidad es más reciente y está determinada por la influencia de los países desarrollados; sin embargo, a nivel internacional se comparten más o menos los mismos objetivos: "Prevenir y eliminar violaciones a las garantías individuales con respecto a la privacidad, tales como el almacenamiento y tratamiento ilegal o incorrecto de los datos personales o la transmisión no autorizada de dichos datos; y evitar que estas regulaciones dificulten el flujo de la información, necesaria para el eficiente funcionamiento de los mercados y para el adecuado desarrollo de la economía" (Bello, 2004: 244). Los miembros de la Unión Europea y la OCDE han intentado establecer un marco común para la protección de datos a nivel internacional desde que comenzó a discutirse el tema. Una de las referencias obligadas es el conjunto de las directrices conocidas como *The OECD Privacy Guideliness,* elaboradas entre 1978 y 1980, donde se establecieron las bases para la protección de la privacidad. Su importancia radica en que, a pesar de que fueron los primeros acuerdos internacionales sobre los principios para regular la privacidad (s/a, 2011: 7), se han mantenido

en constante actualización, por lo que siguen vigentes a más de 30 años de su emisión. La OCDE reconoce cuatro tendencias actuales en cuanto al tratamiento internacional de los datos personales: desarrollo tecnológico, flujo global de los datos, cambios en las prácticas organizacionales y cambios en las prácticas individuales.

Como parte del desarrollo tecnológico, la OCDE incorpora al "cuerpo humano como información". Establece que "los descubrimientos en ingeniería genética han resultado en una importante cantidad de información sobre las personas, que es particularmente sensible porque podría generar actos discriminatorios. La información biométrica (incluida la huella digital) cada vez está más protegida, ya que con frecuencia es usada para fines de identificación y autentificación en una gran variedad de contextos." (s/a, 2011: 31).

Justo en relación a este tipo de asuntos, Ann Cavoukian, comisionada de información y privacidad de Ontario, Canadá, presentó un reporte de investigación sobre el reconocimiento facial enfocado a la protección de la privacidad. La investigación se refiere al uso de la encriptación biométrica para que una persona se "autoexcluya" (del inglés *self-exclusion*) de situaciones que podrían serle perjudiciales; en este caso, los voluntarios del programa deseaban que se les impidiera la entrada, a partir del reconocimiento de sus rasgos faciales, a cualquier casa de juego y apuestas.

Ann Cavoukian considera que "el rápido y acertado reconocimiento de los individuos se ha vuelto un reto para la mayoría de los sectores y jurisdicciones que pretenden proteger la privacidad, ya que los modelos actuales de seguridad funcionan bajo tres formas de autentificación: *algo que sabes* (códigos y claves secretas), *algo que tienes* (una tarjeta o credencial) y *algo que eres* (información biométrica). El tercer tipo ha tenido un rápido desarrollo, de tal forma que ahora es la tendencia en los nuevos modelos de seguridad, que son implementados con mayor frecuencia por las agencias privadas y públicas." (Cavoukian, 2010: 1). Esta investigación es un ejemplo del modelo llamado "Privacidad por Diseño" (del inglés *Privacy by Design*),[2] que tenía como objetivo crear un concepto que incluyera los efectos siempre cambiantes de las

[2] También propuesto por la comisionada canadiense alrededor de la década de los 90 y aprobado como directriz conceptual defendida en la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, realizada en Jerusalén, Israel.

nuevas tecnologías y de los sistemas de datos en red a gran escala; sin embargo, no se trataba sólo de un objetivo teórico, sino que perseguía el fin práctico de implementar la protección de la privacidad en el modo de operación predeterminado de cualquier organización, es decir, lograr cambios desde su interior.

Actualmente, se intenta que la "Privacidad por Diseño" se transforme en "Privacidad por Re-Diseño", que ya no esté enfocada a la creación de modelos para proteger la privacidad a partir de problemas específicos, sino a modificar los existentes.

Las resoluciones internacionales se han firmado en foros y conferencias que reúnen a expertos y autoridades en la materia. Un ejemplo es la *International Conference of Data Protection and Privacy Commissioners*, que en el 2011, en su edición 33, tuvo como cede a México, esta vez organizada por el IFAI y bajo el título de "Privacidad en la Era Global".

Al igual que en años anteriores, en esta ocasión se discutieron los aspectos más novedosos respecto a la creación de herramientas jurídicas, diplomáticas, culturales y en general de todos los ámbitos para garantizar la protección de los datos personales. Como ejemplo están las temáticas de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad, ya que constituyen una prueba anual de cómo ha evolucionado el abordaje de los temas relacionados con los datos personales, desde su definición hasta la toma de acuerdos internacionales para protegerlos. A continuación se presenta un breve recuento de las últimas cinco conferencias, puesto que a partir de ahí es posible identificar las transformaciones que ha sufrido el tema año con año.

En Londres, Inglaterra, se llevó a cabo la 28ª Conferencia con el tema de los datos personales a partir del riesgo que implica su protección. El objetivo era discutir si al garantizar ese derecho se fomentaba la creación de una "sociedad de vigilancia", con sus respectivas consecuencias para la libertad de expresión del individuo y con una cierta tendencia a la paranoia normativa, que involucraba la sensación de ser acosado por un exceso de control y de pérdida de la privacidad.

Para el 2007, la Conferencia se realizó en Montreal, Canadá. En contraste con el año anterior, el problema no era la aparente rigidez

en la normatividad para proteger la privacidad, sino el reconocimiento de la falta de límites claros en los conceptos e ideas básicas para la práctica cotidiana de la protección de datos; de ahí que el título fuera "Horizontes de la Privacidad: Tierra Incógnita".

Las dudas iniciaron desde el nombre mismo de la conferencia, ya que aún hoy no es definitiva la frontera que divide en dónde empieza y hasta dónde llega la privacidad, ni tampoco se ha podido dibujar un límite claro entre el acceso a la información y el derecho a proteger los datos de las personas. Desde la conferencia en Canadá, ya no fue prioritario flexibilizar la normatividad, sino más bien acotar, desde sus raíces, el concepto de privacidad (incluido también el rubro de protección de datos personales).

En el 2008, en Estrasburgo, Francia, se conversó acerca de las dificultades que implicaba la protección de la privacidad en un mundo sin fronteras, por lo que la cuestión se trasladó del concepto de privacidad hacia el de globalización.

A partir de ese momento ya no era necesario definir la privacidad como una construcción teórica, de lo que se trataba era de insertar esa práctica en el contexto global. Si bien es cierto que la privacidad seguía sin tener límites identificables, era más relevante que el mundo, en todos los aspectos posibles, hubiera "borrado" sus fronteras. Cuando en el 2009 llegó el turno a Madrid para celebrar la Conferencia, comenzó el debate sobre la actualidad de las temáticas de privacidad. Bajo la premisa de que "Hoy es mañana" se introdujo el panorama cambiante del uso de las nuevas tecnologías; además fue la primera vez en que se trató el uso generalizado de las redes sociales como un peligro latente para los datos personales por la facilidad de su publicación, la supuesta falta de control y la dificultad para rastrearlos.

En la Conferencia del 2010, ocurrida en Jerusalén, se analizaron los retos para la creación de políticas en materia de protección de datos a partir del actual contexto tecnológico. También se dialogó sobre la forma en que las tecnologías determinan lo que las nuevas generaciones entienden por privacidad, intimidad, confidencialidad y otros conceptos. Fundamentalmente, se adoptó la propuesta de Ann Cavoukian y su enfoque de *Privacy by Design* como base teórica. Además de actualizar las discusiones, en estas conferencias anuales se

renueva el sentido atribuido a los conceptos utilizados cotidianamente en esta comunidad internacional del Derecho de Acceso a la Información y Protección de Datos Personales. Asimismo, constituyen una oportunidad para actualizar el ejercicio de este derecho a la privacidad en cuanto al uso de Internet y de las redes globales, en donde la información se intercambia en cantidades tan grandes y a un ritmo tan vertiginoso, que tiende a desafiar la autonomía individual y a debilitar el control que las personas tienen de sus propios datos, lo cual pone en riesgo su privacidad. Cabe destacar que también arriesga la efectividad y credibilidad del Estado, que por norma deben proteger los sistemas de datos personales.

Los eventos internacionales exhiben los límites del Estado para resguardar la seguridad de las personas, especialmente en países "emergentes", donde la discusión sobre los datos personales se aleja del entorno europeo. Mientras en los países desarrollados el tema de la privacidad se desarrolla desde un punto de vista globalizado y mercantil, en los países "en desarrollo" el tema se extiende a lo que sería la protección de la vida en su conjunto.

Conclusiones

Es inevitable el flujo constante de datos en cantidades inconmensurables. Ello es beneficioso: la reducción de costos, mayor automatización y diversificación de los servicios. No obstante, también ha complejizado el desafío de proteger la privacidad. La evolución tecnológica ha generado un ambiente de vulnerabilidad del individuo, no sólo en cuanto a la protección de sus datos personales, sino en todo lo relacionado con el espacio constitutivo de su privacidad. En México, la propia vida del individuo está en riesgo por estar inserto en un entorno percibido como altamente delincuencial.

Debido a que la protección de datos personales en la era de la hiper información y la comunicación trasciende los límites geográficos, todas las autoridades vinculadas con la garantía de este derecho deben compartir una visión similar en cuanto al establecimiento de normas, estándares y metodologías que sean adoptadas a nivel internacional, que permitan la unificación de criterios y que en consecuencia fomenten una mayor y mejor regulación de los datos de las personas.

No hay conclusiones definitivas respecto al amplio tema de la privacidad y la protección de datos. Menos aun cuando no hay fronteras claras entre los conceptos (situación agravada por la expansión de internet, el auge de las redes sociales, las transformaciones sociopolíticas y una convergencia de contextos contradictorios: países emergentes y desarrollados con graves divergencias en capacidades de hacer efectivo el estado de derecho) y cuando es necesario recurrir a una infinidad de disciplinas para esbozar tan sólo un aspecto mínimo de la problemática.

Uno de los mayores desafíos es que más personas conozcan y ejerzan los derechos de acceso a la información y protección de datos personales. En México la potencialización y socialización de este derecho es minúscula. La tensión que existe entre el derecho de acceso a la información y la protección de datos personales, es un tema que sólo con el avance en el conocimiento y práctica de ambos derechos, por parte de la ciudadanía, y la emisión de resoluciones y el consecuente cumplimiento por parte de las autoridades competentes, podrá avanzar y consolidarse con una serie de criterios claros, que auxilien la resolución de asuntos en donde uno de los dos derechos, presiona, se entrelaza, limita o tensa al otro.

Idealmente el equilibrio no debe ocurrir entre la protección de los datos personales y el flujo de mercancías como enfatizan los países desarrollados sino eventualmente, entre la adquisición de derechos que reposicionan al individuo como centro de la atención del Estado y la supervisión que la persona realiza acerca de las actividades del Estado, entre ellas la que debería garantizar su derecho básico a la vida y a otros derechos fundamentales.

Referencias

s/a (2011). *Thirthy years after the OECD Privacy Guideliness*. OECD. 111pp.

Bello Martínez, Gustavo Adolfo (2004). *Principios generales a considerar en la elaboración de una Ley de Protección de Datos Personales.* En CONCHA CANTÚ, Hugo A., López Ayllón, Sergio y Tacher Epelstein, Lucy (Coordinadores). "Transparentar al Estado: La experiencia mexicana de acceso a la información". IIJ-UNAM. México.

Benveniste, Émile (1977). *Problemas de Lingüística General II*. Ed. Siglo XXI. México. 289pp.

Cavoukian, Ann (2010). *Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept*. Privacy by Design. Ontario, Canada.16pp.

Duby, George (2001). *Historia de la vida privada. Del imperio romano al año mil.* Vol. V. Ed. Taurus. España.

Fenster, Mark (2005). *The Opacity of Transparency*. En *The Berkeley Electronic Press*. Legal Series. No. 520. 47pp.

García González, Aristeo (2006). L*a protección de datos personales dentro del ámbito judicial en México*. En "AR: Revista de Derecho Informático". No. 101. Diciembre.

—— (2007). *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.* En "Boletín Mexicano de Derecho Comparado". No. 120. Septiembre-Diciembre.

Villanueva, Ernesto (2003). Derecho de acceso a la información pública en Latinamérica. México. UNAM.

Instituto de Acceso a la Información Pública y
Protección de Datos Personales del Distrito Federal
Retos de la Protección de Datos Personales en el Sector Público
Se terminó de imprimir en Servicio Editorial Gráfico, en la Ciudad de México
durante el mes de diciembre de 2011.
El tiraje consta de 1,000 ejemplares impresos.
La edición estuvo al cuidado del Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal.