Protección de Datos

Protección de las Personas

La Agencia de Protección de Datos de la Comunidad de Madrid
se encarga de que se respeten sus derechos
y se cumplan los principios de protección de datos
en las Administraciones Públicas en el ámbito de la Comunidad de Madrid

Para contactar con la APDCM:
e-mail: apdcm@madrid.org
www.apdcm.es
Teléfonos: 91 580 28 74 - 91 580 28 75
Fax: 91 580 28 76
C/ Cardenal Marcelo Spínola, 14
28016 Madrid

Agencia de Protección de Datos de la Comunidad de Madrid

Vía TRANSPARENTE

Año 3 Número 3 Enero 2008

El Reto de la Protección de los Datos de Carácter Personal

La Protección de Datos Personales: El Desafío de la Inteligencia

Vida Privada y Datos Personales

Avances de la Legislación Federal en Materia de Datos Personales

Firma ICAI convenio de trabajo con la Agencia de Protección de Datos de la Comunidad de Madrid

Con el fin de coadyuvar en materia de protección de datos personales, el Instituto Coahuilense de Acceso a la Información y la Agencia de Protección de Datos de la Comunidad de Madrid firmaron un convenio de trabajo y colaboración el 13 de agosto de 2008.

La capital española fue sede del convenio que permite iniciar una etapa de cooperación con la finalidad de promover la difusión y la implantación efectiva de las garantías derivadas de la legislación reguladora del derecho a la protección de los datos personales.

En punto de las 13:00 horas, tiempo local de la ciudad de Madrid, los consejeros propietarios del ICAI, Manuel Gil y Alfonso Villarreal, en representación del Instituto Coahuilense de Acceso a la Información, acordaron participar en conjunto con la Agencia de Protección de Datos de Madrid en el inicio de una etapa de cooperación y colaboración institucional para promover la difusión de las garantías del derecho a la protección de datos personales.

A su vez se desarrollarán e implementarán acciones para formar a los ciudadanos en el conocimiento de la protección a los datos personales y los derechos que les atribuyen.

La Agencia de Protección de Datos de la Comunidad de Madrid tiene como finalidad garantizar y proteger los derechos fundamentales de las personas físicas respecto al honor e intimidad familiar y personal, en lo relativo al tratamiento de sus datos personales.

La retroalimentación que dejará dicho convenio de colaboración reditúa en la realización de investigaciones, estudios, análisis e informes en el campo de la protección de datos personales, apartado de la Nueva Ley de Transparencia, mismo que entrará en vigor en diciembre del 2009.

APDCM
Agencia de Protección de Datos de la Comunidad de Madrid

icai
Instituto Coahuilense de Acceso a la Información Pública

El día 20 de julio del año dos mil siete se publicó en el Diario Oficial de la Federación la reforma al Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. La reforma buscó homologar el derecho de acceso a la información pública gubernamental en cualquier parte del país. La aludida reforma, además de establecer nuevos horizontes en materia de acceso a la información pública y transparencia añadió, en la fracción II, un reconocimiento al derecho a la protección de datos personales.

Derivado de lo anterior el presente número de *Vía Transparente* se encuentra dedicado a la protección de los datos personales, con una perspectiva global, ya que en el mismo se podrá encontrar artículos de opinión no sólo de distinguidas personalidades del país, sino también del extranjero. Ambos tipos de participaciones destacan por sus aportes al tema que, dicho sea de paso empieza a ser fértil en todo el territorio mexicano, encontrándose ya en camino de ser considerado un derecho fundamental.

Esto último, derivado de que en el Senado de la República, las comisiones unidas de Puntos Constitucionales y de Estudios Legislativos, recientemente han propuesto una modificación constitucional, con el objetivo de incluir la protección de los datos personales como un nuevo derecho fundamental dentro del catálogo de garantías.

El contenido de la revista tiene una intención importante, que es: dar a conocer qué es la protección de datos personales, con la intención de que cualquier ciudadano que la lea se adentre en el tema, sin requerir para ello de conocimientos especiales, ya que una sociedad no se mide por los derechos que en todo caso contempla su ley máxima, sino del conocimiento que tienen los ciudadanos de sus derechos.

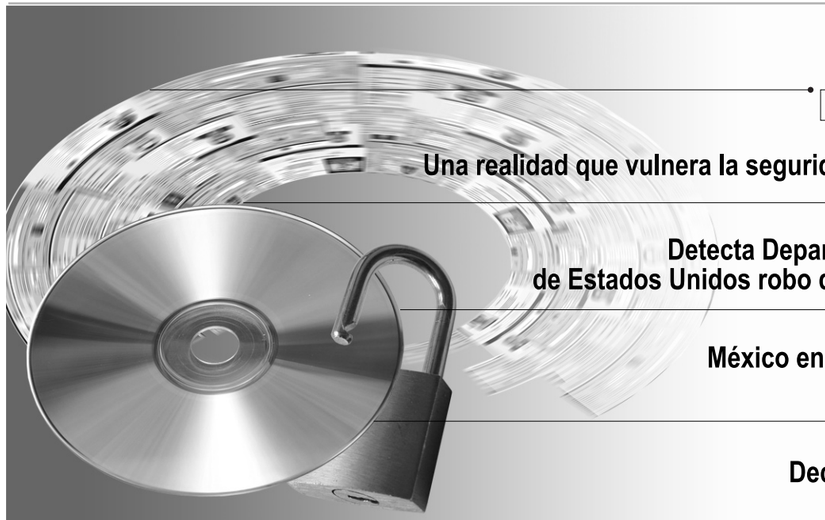
La *Vía Transparente* que hoy está en sus manos, es un producto editorial que pretende ser por el momento, único en su contenido y detonador del tema en el lugar al que llegue, ya que no debe de existir necesidad de que se vulneren los datos personales para regular su protección. En todo caso, debe de ser a la inversa. Es decir, regular para no vulnerar.

Por último, sólo resta agradecer a todas las personas que colaboraron para la realización de la revista, dado que su participación desinteresada contribuye a enriquecer el tema.

El Instituto Coahuilense de Acceso a la Información Pública (ICAI) es un organismo autónomo, apartidista, independiente en sus decisiones y funcionamiento, y profesional en su desempeño; dotado de su personalidad jurídica y patrimonio propios. www.icai.org.mx / 01 800 TELICAI, email de la revista: viatransparente@icai.org.mx
Esta revista fue pagada con recursos públicos del ICAI y no obedece a ninguna campaña política o partidista.
Consta de 2000 ejemplares y tuvo un costo de $ 64,340.00 . Impresión: Primercuadro Grupo Editorial.

ÍNDICE

REPORTAJES



P6 **Tráfico de Datos: Una realidad que vulnera la seguridad de las personas.**

P11 **Detecta Departamento de Justicia de Estados Unidos robo de identidad masiva.**

P13 **México en la encrucijada de la transparencia.**

P15 **Declaración de Atlanta.**

EDITORIALES

P17 **Alfonso Raúl Villarreal Barrera.**
Vida Privada y Datos Personales

P21 **Juan Antonio Travieso.**
La Protección de los Datos Personales: El desafío de la inteligencia

P24 **Lina Gabriela Ornelas Nuñez.**
Las Obligaciones del Estado en materia de Privacidad y Protección de los Datos Personales: El caso mexicano

P28 **Antonio Troncoso Reigada.**
Las Autoridades de Protección de Datos; Ante el reto de la Protección de Datos de Carácter Personal

P31 **Luis Gustavo Parra Noriega.**
La Protección de Datos Personales en México: Avances en la Legislación Federal

P35 **Sandrino Saucedo Contreras.**
Jurisprudencia relevante sobre el Derecho a la Información, caso Coahuila

P41 **Lourdes Hernández Crespo.**
El Derecho Fundamental a la Protección de Datos Personales. Pasado, Presente y Futuro

P44 **Javier Rodríguez Suárez.**
Protección de la Información Médica

P47 **José Manuel Gil Navarro.**
La Vida de los Otros

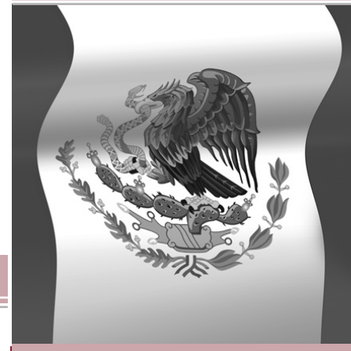
P51 **Ricard Martínez Martínez.**
Seguridad y Protección de Datos en la Legislación Española

P55 **Ricardo Cantú Aguillén.**
Protección de Datos Personales en los Poderes Judiciales de México (Información Pública, Confidencial y Reservada)

ESTADÍSTICAS

P65 **La Protección de Datos Personales en los Estados de la República Mexicana**

SECCIONES

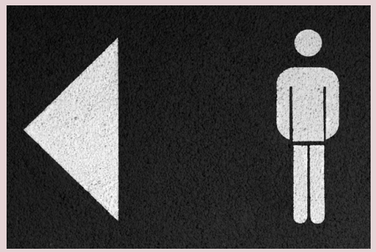


P66 **Entorno Mundial**

P68 **Entorno Nacional**

BUENAS PRÁCTICAS DE PRIVACIDAD

P70 **Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público.**



TECNOLOGÍA

P72 **Los Datos Personales y las Tecnologías de Información**

Tráfico de datos:

Una realidad que vulnera la seguridad de las personas

Por: Heriberto Medina.

¿Dónde obtienen información de sus víctimas los secuestradores y quiénes se dedican a extorsionar personas mediante llamadas telefónicas?; ¿dónde consiguen datos quienes defraudan a los bancos y a sus clientes a través de Internet? La respuesta podría estar en el tráfico de datos personales.

Por Heriberto Medina.

Se identifica como Muuk y es originario de San Luis Potosí. Es la única información disponible acerca del vendedor de una base de datos con más de 500 mil registros.

Cualquiera puede saber dónde vives, cuál es tu número telefónico, tu correo electrónico, dónde trabajas e incluso tu nivel de ingreso. Sólo tiene que pagar cantidades que van de los 750 pesos hasta los 450 mil pesos y tendrá a su disposición archivos electrónicos que agrupan la información de miles de individuos. El tráfico de datos personales es hoy una realidad en México. El fin con el que se acceda a esa información no importa, el vendedor, en la mayoría de los casos protegido por el anonimato, no pregunta para qué serán usados los registros. Su objetivo es lucrar.

Tampoco parece importar el origen de los datos, o si para obtenerlos se vulneró alguna disposición legal, o se cometió un delito.

Se identifica como *Muuk* y es originario de San Luis Potosí. Es la única información disponible acerca del vendedor de una base de datos con más de 500 mil registros.

El origen de esos registros está en las entidades públicas de San Luis Potosí. Al menos así lo destaca *Muuk* en el anuncio de venta que publicó en el portal de internet: *Mercado Libre*.

"Base de datos para telemarketing o usos similares, de el estado de San Luis Potosí y sus municipios de diversas dependencias"(SIC), indica el vendedor en su anuncio, y destaca otros aspectos de su producto: "en formato excel y access, hacer cualquier pregunta al respecto, son más de 500,000 registros y se pueden cotejar para crear una base de datos aun más grande"(SIC).

El precio es de 49 mil pesos. El comprador puede mantener el anonimato al igual que el vendedor y, además, tiene facilidades de pago. Puede cubrir el costo con diversas tarjetas de crédito como Visa, Mastercard, American Express, Bancomer, Banamex, Serfín y Banorte. Además tiene un plazo de hasta 12 meses sin intereses.

Al tratar de saber más sobre *Muuk*, el propio portal indica que es un vendedor con una reputación de 92 por ciento, con 4 referencias negativas y más de 40 positivas.

A diferencia del vendedor, quien no muestra preocupación alguna por los datos de las 500 mil personas que aparecen en su producto, el portal sí protege los datos personales tanto del vendedor como de quien realice la compra del producto. No hay forma de saber quién es *Muuk*, su dirección o su teléfono.

El anuncio se publicó antes del 15 de agosto y expiró el día 28 de ese mismo mes. Aparentemente nadie adquirió la base de datos.

El anuncio de *Muuk* no es el único en *Mercado Libre*. *Skullbeing, tuscontactos, Mr. Solís, Sharitocm*, ofrecen productos similares. Algunos de ellos son más específicos en cuanto a la información que incluyen las bases de datos.

De entre ellos destaca *Mr Solís*. Él ofrece una base de datos de correos electrónicos, con datos muy específicos.

"...más de 8.5 millones de mails de todo México seleccionada por estados, giros, cuenta habientes bancarios, empresas, profesionistas, universitarios, edades etc. la verdad esta completísima... actualizada 2008"(SIC), se indica en el anuncio.

Mr. Solís, dice localizarse en Guadalajara, Jalisco. Vende la base de datos en mil 800 pesos y ofrece, incluso, enviarla a otros países.

Skullbeing, también localizado en Jalisco, va más allá. Ofrece los datos de 200 mil empleados que incluyen: el nombre, el número de seguridad social, el sueldo base integrado, además de los datos de la empresa, razón social y dirección, entre otros. Esa base de datos cuesta 750 pesos. Otras bases de datos de *Mercado Libre* ofrecen direcciones y correos electrónicos.

Pero no sólo en *Mercado Libre* se pueden comprar archivos electrónicos. En la página http://www.idea2.com.mx/infoclean/proceso.htm, se puede adquirir una variedad de datos de empresas y personas.

Los datos que ofrece *infoclean* van desde los nombres de directores y gerentes de miles de empresas a nivel nacional y del D.F., hasta los nombres y formas de localizar a más de 400 mil tarjetahabientes en el Distrito Federal y en todo el país. *Infoclean* vende a 2.20 pesos cada uno de los 12 mil registros de empresas en el Distrito Federal; lo que da un total de 26 mil 400 pesos. Mientras que el registro de cada persona tiene un precio de 1.80 pesos, al ser 250 mil registros el precio total puede llegar a los 450 mil pesos.

Infoclean no proporciona en su página de Internet una dirección fija. Para contactarlos da un correo electrónico y dos números telefónicos en el Distrito Federal.

En el sitio http://efuturnet.com

/ctent/view/126/39/se comercializan los correos electrónicos de personas de altos ingresos en el país. Los propios anunciantes aseguran que los datos son de altos funcionarios del gobierno, empresarios e industriales. También ofrecen los correos electrónicos de miles de tarjeta-habientes bancarios, así como de los comensales frecuentes de los principales restaurantes de la Ciudad de México.

La base de datos de e*futurnet.com* cuenta con más de 7 millones de registros, según los vendedores, y tiene un precio de 3 mil pesos. "En la compra de esta base se incluyen 833,000 emails adicionales de México (Base reciente) y como bono adicional base de 65,000 universitarios", se menciona en la citada página de Internet.

Frente al tráfico de datos personales, la legislación mexicana en la materia y las acciones de las entidades públicas resultan insuficientes.

A finales de 2007, tanto la Procuraduría Federal del Consumidor, (Profeco), como la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, (Condusef), abrieron espacios para registrar a las personas que no desearan recibir publicidad. Ambas instancias del Gobierno cobran a las empresas por acceder a esos registros y tomar nota de las personas a las que no deben llamar o enviar publicidad. La Profeco tiene tarifas que van de los 540 a los 16 mil 100 pesos, mientras que la Condusef cobra 60 mil pesos.

Mientras en Internet se venden cientos de miles e incluso millones de datos, en los registros abiertos por la Profeco y la Condusef el número de usuarios registrados hasta mediados del presente año no pasaba de los 150 mil.

La Profeco y la Condusef pueden sancionar a las empresas que molesten a las personas registradas. La multa que aplica la Procuraduría puede llegar hasta un millón 64 mil 44 pesos; la Comisión, en el caso más grave, puede aplicar una sanción de aproximadamente 100 mil pesos. En el Registro de Usuarios de la Condusef, hasta el 31 de marzo del presente año, se habían inscrito 48 mil 205 personas. A esa fecha la Comisión aún no iniciaba los procedimientos en contra de las empresas infractoras.

En el Registro Público del Consumidor de la Profeco se habían registrado, hasta el 7 de abril de 2008, 97 mil 308 personas.

VT

Detecta Departamento de Justicia de Estados Unidos **robo de identidad** masiva

Redacción: Vía TRANSPARENTE

Los presuntos delincuentes habrían obtenido 40 millones de números de tarjetas de crédito y débito utilizando la suplantación de identidades y mediante la instalación de programas *sniffer*, para rastrear tráfico, en las redes de nueve cadenas de distribución, restaurantes y librerías.

Después de recopilar los datos, los acusados supuestamente los ocultaban en servidores encriptados que controlaban desde Europa del Este y Estados Unidos.

La banda habría vendido algunos de esos números de tarjetas a otros delincuentes a través de Internet. Posteriormente los codificaban en otras tarjetas en blanco con las que habrían retirado miles de dólares de los cajeros. El Departamento de Justicia no ha dado a conocer la suma a la que asciende la pérdida de dinero robado por estos supuestos delincuentes, aunque sí ha dado el caso concreto de un restaurante en el que el *software* espía habría capturado datos de aproximadamente 5 mil tarjetas de crédito y débito, causando pérdidas de, al menos, 600 mil dólares a las entidades financieras propietarias de las tarjetas.

"Este caso denota nuestra creciente vulnerabilidad ante el robo de información personal", reconoció el Abogado General del Estado Michael Mukasey. "Las redes informáticas e Internet son una parte indispensable de la economía mundial. Pero incluso, aunque proporcionen oportunidades extraordinarias para el comercio y las comunicaciones, también son una oportunidad extraordinaria para los delincuentes. Allí donde son capaces de interceptar los sistemas de seguridad informática, como ha sucedido en este caso, tienen una gran posibilidad de causar daño".

Tres de los miembros de esta red son ciudadanos estadounidenses, otro procede de Estonia, tres de Ucrania, dos de China y uno de Bielorrusia. Al último individuo sólo se le conoce por su alias en Internet: *Delpiero*, y se desconoce su lugar de origen.

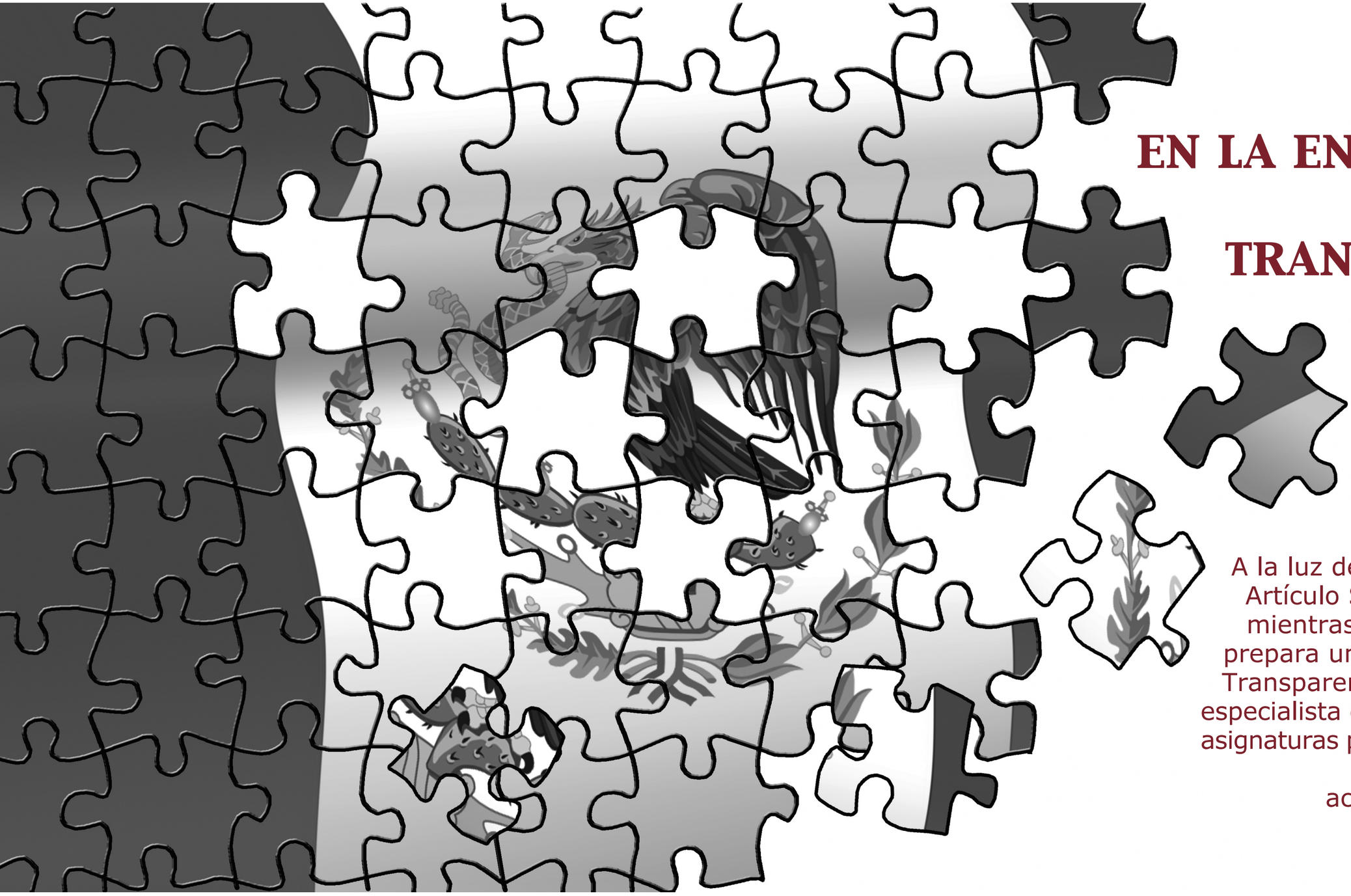
Las autoridades han identificado a Albert *Segvec* González, de Miami, como uno de los cabecillas, y ahora mismo está encarcelado en Nueva York acusado de fraude informático, acceso fraudulento a dispositivos, robo de identidad y conspiración, entre otros, y podría pasar el resto de su vida en la cárcel si finalmente progresan todos los cargos. González ya había sido arrestado por el Servicio Secreto en 2003 por acceso fraudulento a dispositivos. Durante esa investigación, la organización descubrió que González, que

estaba trabajando como confidente de la agencia, estaba involucrado en el caso.

Los arrestos son producto de tres años de investigación llevada a cabo por el Servicio Secreto estadounidense y distintas agencias, y en el proceso también han participado las policías de Turquía y Alemania, países donde se detuvo a dos de los imputados.

La Comisión Federal del Comercio de Estados Unidos ha impuesto sanciones contra las cadenas TJX, DSW y BJ´s por no haber tomado las medidas de seguridad apropiadas para proteger la información de sus clientes. Estas entidades ya habían reportado brechas de seguridad entre 2004 y 2007.

VT



MÉXICO EN LA ENCRUCIJADA DE LA TRANSPARENCIA

Redacción: Vía TRANSPARENTE

A la luz de las modificaciones al Artículo Sexto Constitucional y mientras el Legislativo Federal prepara una reforma a la Ley de Transparencia, ***Laura Neuman***, especialista en el tema, delineó las asignaturas pendientes para México en materia de acceso a la información.

Laura Neuman enumera los retos del país en materia de *acceso a la información*

La abogada estadounidense graduada en la Universidad de Wisconsin, estuvo en la Ciudad de México a mediados del presente año para participar en el foro de análisis sobre las oportunidades y riesgos de las reformas a las leyes de transparencia y acceso a la información, organizado por el Centro de Investigación y Análisis FUNDAR y la UNAM.

Como parte del foro, Neuman presentó la ponencia: "El consenso internacional sobre mejores prácticas en materia de acceso a la información", y explicó lo que, desde su punto de vista, son las diferentes generaciones de leyes en materia de acceso a la información en el mundo.

"La primera generación se refiere a las leyes más antiguas del mundo", indicó. "Una segunda generación podría ser la de las leyes que se aprobaron en México y en Sudáfrica. Finalmente, la tercera generación de leyes es aquella en la que se dan las condiciones para avanzar más respecto a lo alcanzado en la generación anterior, aunque también se corre el riesgo de retroceder".

En el caso particular de México, reconoció los avances logrados y destacó que, de cara a la presente reforma, hay aspectos que se deben cuidar.

"México cumple con todas las normas de acceso a la información. También tiene cualidades únicas que deben ser protegidas durante la reforma", dijo.

Neuman, quien actualmente coordina el proyecto sobre acceso a la información del Centro Carter - una organización internacional en pro de los derechos humanos fundada por el ex presidente de los Estados Unidos Jimmy Carter - enumeró 8 retos que se le presentan a México, tomando en cuenta su realidad particular.

"México debe buscar la forma de garantizar la independencia de las instituciones de transparencia;" precisó, "determinar cuál va a ser el papel de estas instituciones para promover y proteger el derecho a la información".

Estimó que México debe extender a los estados y municipios el acceso a la información que actualmente se da a nivel nacional. Además, continuar con la capacitación de los servidores públicos y mantener a la sociedad civil vinculada y comprometida con la transparencia.

Consideró que se deben sumar otros sectores en el impulso a la transparencia, uno de los cuales podría ser el sector privado, y destacó la conveniencia de desarrollar instrumentos para evitar que las nuevas tecnologías sean un obstáculo para el acceso a la información.

La abogada estadounidense, quien ha editado al menos seis guías en donde se explica cómo la transparencia es un factor preventivo para la corrupción, resaltó la diferencia entre: contar con una ley de acceso, e implementarla realmente.

"De los 70 países que cuentan con leyes de acceso a la información en todo el mundo, solamente cinco la han podido implementar", comentó.

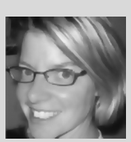
Entrevistada por *Vía Transparente* durante el foro, Neuman reconoció lo difícil que resulta lograr un cambio cultural en materia de transparencia. "Cambiar una cultura del secreto a uno de apertura es una tarea difícil que puede tomar generaciones", señaló. Y, en sus propias palabras, añadió: "However, a first step is to raise the community's awareness of their right to information", (sin embargo un primer paso es aumentar el nivel de concienciación de la comunidad sobre su derecho a la información).

Manifestó que tanto para los ciudadanos como para los gobiernos resulta benéfico el acceso a la información.

"Muchos gobiernos se enfrentan a la urgente necesidad de mejorar su economía, la reforma de su Constitución, fortalecer las instituciones, modernizar la administración pública, luchar contra la corrupción, y controlar disturbios civiles. Y precisó: *"For these governments, access to information can be used to achieve all of these objectives".* ("Para estos gobiernos, el acceso a la información puede ser utilizado para lograr todos estos objetivos").

"El acceso a la información sirve como un instrumento crítico para la lucha contra la corrupción, permitiendo a los ciudadanos participar más plenamente en la vida pública", indicó, "Les permite participar en la fijación de prioridades y la toma de decisiones y les permite asegurar la igualdad de trato y de justicia".

¿Quién es **Laura Neuman**?



* Graduada de la Escuela de Derecho de la Universidad de Wisconsin.
* Gerente de Proyectos sobre Acceso a la Información de el Centro Carter.
* Ha editado seis guías de amplia distribución en el fomento de la transparencia y la prevención de la corrupción.
* Es autora del artículo "Acceso a la información: un elemento clave para la Democracia".
* Coautora del estudio "La Ley. Hacer el trabajo. Los desafíos de la ejecución y divulgación de las contribuciones de campaña a través de las leyes de acceso a la información: la experiencia sudafricana y su pertinencia para las Américas".
* Ha dirigido y participado en las misiones de supervisión de elecciones en todo el hemisferio occidental.

Declaración de Atlanta

En febrero de 2008 representantes de diversos países y expertos en transparencia y acceso a la información se reunieron en Atlanta, Georgia EUA, para abordar el tema. Después de una serie de deliberaciones elaboraron un documento denominado "Declaración de Atlanta". A continuación transcribimos una parte de la misma, denominada "Hallazgos".

Hallazgos

1. El derecho fundamental de acceso a la información es inherente a todas las culturas y sistemas de gobierno.

2. La falta de acceso a la información afecta desmedidamente a los pobres, las mujeres, los grupos vulnerables y marginalizados, cuando el derecho, como tal, debería estar garantizado para todos los sectores de la sociedad.

3. El derecho de acceso a la información es fundamental para la dignidad humana, la equidad, y la paz con justicia.

4. La transparencia es un instrumento necesario y muy efectivo para promover la seguridad humana y la del Estado.

5. Las nuevas tecnologías presentan un gran potencial para facilitar el acceso a la información. No obstante, ciertos factores que limitan el acceso a la tecnología y las prácticas de manejo de datos, han impedido que muchas personas obtengan el máximo provecho de dicho potencial.

6. La promulgación de una ley integral es esencial, aunque no es suficiente para establecer y mantener el derecho de acceso a la información.

7. La creación de un marco institucional apropiado y el desarrollo de la capacidad en la administración pública para gestionar y suministrar información, son de igual importancia.

8. Es además indispensable elevar la conciencia pública sobre el derecho de acceso a la información, asegurar la capacidad de su ejercicio, incluyendo la educación pública, y fomentar el apoyo a la transparencia entre todos los sectores de la sociedad.

9. La prensa libre e independiente es un componente fundamental del establecimiento y pleno goce del derecho de acceso a la información.

Vida **Privada** y Datos **Personales**

Alfonso Raúl Villarreal Barrera*

Las personas tienen la libertad de dejar al margen de los demás parte de su vida. El conocimiento y asociación de sus datos personales por otros, limita esta posibilidad. Los particulares tienen en la vida varias esferas o áreas en donde se desenvuelven. Una de éstas es el espacio público: es decir, la parte de la vida que queda a merced del conocimiento y consideración de los demás, que se ventila abiertamente, en el trabajo, en reuniones sociales, con amigos, o en contacto con conocidos. Donde los otros individuos tienen acceso a conocer de determinada persona, qué es lo que hace y cómo lo hace, lo público es visible. Queda de manifiesto así, la parte pública del desarrollo individual del particular.

¿Son todas las conductas y actividades de los particulares públicas? Por supuesto que no. Existe parte del desarrollo de la persona que permite hacer uso de la libertad, en la que no se consienten intromisiones, se resguardan los actos y actividades de injerencias ajenas. Esta parte de la existencia, es la vida privada, que tiene soporte jurídico, y se acredita como un derecho que protege la vida de las personas de asomos e intrusiones de los demás y de las propias autoridades.

La vida privada es: *"la esfera personal exclusiva jurídicamente reconocida y garantizada como derecho a todo ser humano, a fin de permitirle conducir una parte de su propia existencia de manera autónoma, independiente, y libre de injerencias externas indebidas, en relación con algunas de sus convicciones, decisiones, o actividades intimas, o con sus relaciones o comunicaciones particulares, atributos personales, vida familiar, reserva domiciliaria, etc."*[1]

Con fundamento en la Constitución General de la República, la vida privada es garantizada y reconocida como el derecho a la vida privada, que es parte de los derechos subjetivos de la persona, y a la vez forma parte de los derechos de la personalidad.

De igual forma, el derecho a la vida privada, *"es el derecho fundamental que consiste en no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del cono-*

* • Consejero del Instituto Coahuilense de Acceso a la Información Pública.
• Es Licenciado en Derecho por la UANL.
• Maestría en Administración Pública por el INAP.

¿Son todas las conductas y actividades de los particulares públicas?, por supuesto que no, existe parte del desarrollo de la persona que permite hacer uso de la libertad, en la que no se consienten intromisiones, se resguardan los actos y actividades de injerencias ajenas.

cimiento público. El bien jurídico protegido por este derecho, está constituido por la necesidad social de asegurar la tranquilidad y la dignidad para el libre desarrollo del ser humano, a fin de que cada quien pueda llevar a cabo su proyecto vital."[2]

Podemos advertir que, en la vida privada, decides libremente si compartes o no tus pensamientos, ideas, sentimientos, creencias y demás actos, datos o hechos que forman parte de tu intimidad.

El Artículo 16 de la Constitución Mexicana, establece la posibilidad de que los particulares realicen parte de su vida con autonomía, sin injerencia, censura o critica de sus actos privados, que dichos actos estén libres de injerencias indebidas o incluso ilegales.

Dicho Artículo constitucional establece: *"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..."*[3]

Se interpreta esta parte del Artículo 16, en el sentido que los individuos no deben sufrir perturbaciones, ni molestias en el ámbito de su vida privada, desarrollada en gran parte en su domicilio.

Avanzando en el cuerpo del artículo, en párrafos subsecuentes se puntualiza que las comunicaciones privadas son inviolables. Sólo la autoridad facultada podrá intervenirlas siguiendo el procedimiento adecuado, acatando la forma y fondo señalado en la propia Constitución. Esto también como un reconocimiento a ese espacio de privacidad del que no debe de participar nadie si, previamente, no se le ha otorgado el consentimiento.

Otras disposiciones constitucionales establecen en función de otros supuestos y derechos la protección de que goza la vida privada. El Artículo 7 Constitucional en función del derecho a la libre expresión, funda que debe de existir respeto a la vida privada. Asimismo, la Ley de Delitos de Imprenta en su Artículo 1 asienta los actos que constituyen ataques a la misma.

El peligro de que se vea quebrantada la vida privada, no proviene únicamente de las personas que nos rodean y de las autoridades. También puede presentarse una invasión a la privacidad por los medios de comunicación masiva. Estos representan un reto porque hacen del dominio público, de manera instantánea, aspectos de la vida privada de las personas que solamente deberían de conocer los más allegados.

"También se entiende que la amenaza proviene no sólo de la autoridad, sino de los medios de comunicación masiva. Se vulnera nuestra intimidad cuando se hace del conocimiento público, mediante la prensa, la radio, la televisión.(...) Los medios representan una amenaza para la intimidad porque hacen del dominio público, inmediatamente, masivamente, cosas que sólo correspondería saber a unos cuantos."[4]

Cabe hacer mención que el autor Gonzalbo Escalante se está refiriendo en su escrito, a que la intimidad forma parte de la privacidad, y establece que la definición de lo privado es objetiva, mientras que la definición de lo íntimo es relativa. En relación a este aspecto la Suprema Corte de Justicia de la Nación, establece claramente que lo íntimo forma parte de la vida privada. A la letra dice lo siguiente:

"VIDA PRIVADA E INTIMIDAD. SI BIEN SON DERECHOS DISTINTOS, ÉSTA FORMA PARTE DE AQUÉLLA."

"La vida privada se constituye por el ámbito privado reservado para cada persona y del que quedan excluidos los demás, mientras que la intimidad se integra con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento se reserva para los integrantes de la unidad familiar. Así, el concepto de vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona. Esto es, la vida privada es lo genéricamente reservado, y la intimidad -como parte de aquélla- lo radicalmente vedado, lo más personal. De ahí que si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada."[5].

En adición el Artículo 6º Constitucional, recientemente se reformó y en la fracción II garantiza que la vida privada debe de gozar de resguardo, y contempla en esta protección un elemento determinante para salvaguardar la vida privada, que son los datos personales.

El Artículo 6º. Constitucional establece:

En adición el artículo 6º Constitucional, recientemente se reformo y en la fracción II garantiza que la vida privada debe de gozar de resguardo y contempla en esta protección un elemento determinante para salvaguardar la vida privada, que son los datos personales.

"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. ...

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."*[6]

La vida privada es un derecho que deriva de la persona misma, ya que mantener parte de nuestra vida al margen de los demás, propicia un libre desarrollo de la personalidad, y ésta a su vez es generadora de un adecuado desenvolvimiento de las personas en libertad.

Se entiende que la libertad implica el libre movimiento, pero no solamente físico, sino como una propiedad de la voluntad, que en cuanto su naturaleza racional, le da la posibilidad al hombre de ejercitar libremente su voluntad, sin trabas ni amagues, sin obstáculos que impidan su desenvolvimiento, buscando siempre la posibilidad de elegir, de acuerdo a su razón, lo mejor en la propia búsqueda de la felicidad y su existencia.

El conocimiento y control de los datos e información de cualquier persona, da la posibilidad de conocer de ésta, aspectos relacionados con su vida privada.

De ahí la importancia de conocer cuáles son los datos que se tienen que proteger para garantizar el respeto a la vida privada, del titular de los mismos.

El Artículo 3º de la Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila define a los Datos Personales como:

"La información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a una persona, identificada o identificable: el nombre asociado al origen étnico o racial, o las características físicas, morales o emocionales, a la vida afectiva y familiar; el domicilio, número de teléfono, cuenta personal de correo electrónico, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, los estados de salud físicos, o mentales, las preferencias sexuales, la huella dactilar, el ADN, la fotografía y el número de seguridad social."[7]

Los datos personales pueden representar pensamientos, creencias, ideas, ideologías, emociones, sensaciones, preferencias y convicciones acerca de diversos temas, tópicos, fondos y contenidos.

Al ser del conocimiento de los demás estos datos, se presenta la posibilidad de asociarlos con el titular. Existe la eventualidad de que se presenten discrepancias entre apreciaciones, y en determinado momento diferentes posiciones, que puedan desembocar en acciones o conductas de intimidación, segregación, coacción, discriminación, imposición, exigencia de ciertas actividades, conductas o comportamientos.

Lo anterior vendría a limitar la posibilidad de las personas de moverse con libertad y de acuerdo a sus convicciones y su verdad. Poniendo en riesgo la dignidad humana, entendida ésta, como un valor en donde se tiene dominio pleno ejercido por y para el hombre sobre su propia vida.[8]

En los siguientes párrafos trato de ejemplificar que cuando los datos personales caen en poder de personas que no son los titulares, aquellas pueden tener injerencia en la vida privada de éstos, causando molestia a su privacidad e intimidad.

Respecto al número telefónico, aunque algunos autores no lo consideran como dato personal desde el punto de vista de la teoría de los valores, sabemos que la tranquilidad personal y familiar se ve alterada cuando se establece la relación de un número telefónico con el nombre de la persona física titular de la mencionada línea, identificándola y reconociéndola. Se establece la posibilidad con esta relación, al existir una mala intención o mala fe del poseedor de los datos cuyo titular es otra persona, de perturbar la tranquilidad y armonía personal y/o

familiar.

Las opiniones políticas como un juicio o concepto de las cosas del gobierno, de los partidos políticos, y/o de los asuntos del Estado, surgen y se derivan de un determinado conocimiento de la propia realidad. En ellas se materializa la apreciación, pensamiento, creencia, emoción y/o sensación acerca de las cosas, actividades, acciones o ideologías, de la actividad gubernamental y los entes del Estado.

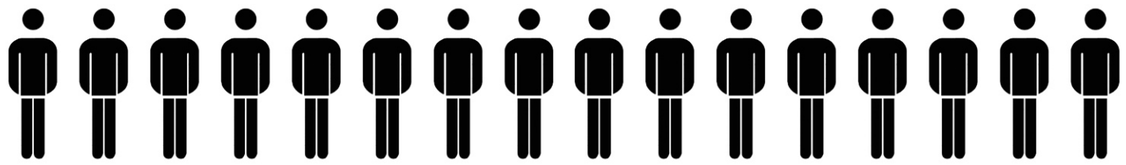
La protección de las opiniones políticas, tutela la igualdad de las personas, evita procesos discriminatorios, que pueden presentarse al conocerse dichas opiniones sino no se coincide con estas. O bien, al relacionarlas con gobiernos establecidos, partidos políticos, asociaciones políticas u otras organizaciones pertenecientes al Estado a los cuales no les convinieren dichas expresiones.

La protección de el estado de salud física o mental de las personas, está relacionado con el resguardo de su libre decisión, autonomía e independencia y no injerencia en algo tan privado y tan íntimo como es la condición humana, física y psíquica, rodeada en un entorno social.

El conocimiento de los datos personales por no titulares, puede revelar la existencia de condiciones de salud no libres de enfermedad, o bien el conocimiento por otras personas de los tratamientos médicos, métodos, sistemas o medicamentos que le suministran al paciente. Al relacionarlos con la persona misma y, para qué tipo de enfermedades se utilizan, se puede establecer con cierta aproximación el estado de salud física o mental del individuo. El estar enfermo, puede dar origen a actitudes discriminatorias por temor a contagios, contaminación o infección. Dichas actitudes o conductas atentan contra la igualdad de las personas que debe de prevalecer en un sistema democrático.

Las personas, pueden dejar parte de su vida al margen del conocimiento de los demás, constituyendo su derecho a la vida privada. Esto le permite al individuo hacer uso de su voluntad para determinar de una manera libre su propio desarrollo. El hecho de que conozcan los demás los datos personales de un individuo, da la posibilidad de injerencias en la vida privada de éste, afectando sus derechos fundamentales como la igualdad y libertad.

La protección del estado de salud física o mental de las personas, está relacionado con el resguardo de su libre decisión, autonomía e independencia y no injerencia en algo tan privado y tan íntimo como es la condición humana, física y psíquica, rodeada en un entorno social.



[1] Editorial Porrúa. *Diccionario Jurídico Mexicano*. Instituto de Investigaciones Jurídicas. UNAM. pp.3883.

[2] Villanueva, Ernesto. *El derecho de la información frente a los derechos de la personalidad*. [En línea] México, Instituto de Investigaciones Jurídicas, 2008, [16/10/2008], *Derecho Comparado de Información*, (Número 11) Formato pdf, Disponible en: http://www.juridicas.unam.mx/publica/rev/indice.htm?r=decoin&n=3 ISSN 1870-0594.

[3] Constitución Política de los Estados Unidos Mexicanos. (CPEUM)

[4] *El Derecho a la Privacidad*. Escalante Gonzalbo, Fernando. 02. Cuadernos de Transparencia. IFAI.

[5] Amparo directo en revisión 402/2007. 23 de mayo de 2007. Mayoría de tres votos. Ausente: José de Jesús Gudiño Pelayo. Disidente: José Ramón Cossío Díaz. Ponente: Olga Sánchez Cordero de García Villegas. Secretaria: Ana Carolina Cienfuegos Posada.

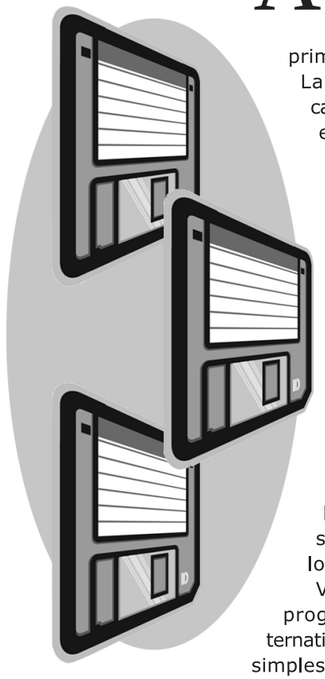
[6] CPEUM.

[7] *Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila*. Publicada en el *Periódico Oficial del Gobierno del Estado* el día 2 de septiembre de 2008. Las disposiciones en materia de protección de datos personales entrarán en vigor el 1 de diciembre de 2009.

[8] Citado por Nájera Montiel, Javier. *El aspecto axiológico de los datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. IIJ-UNAM. Biblioteca Jurídica Virtual. Pág.99.

La Protección de los Datos Personales:
el desafío de la inteligencia

Juan Antonio Travieso*



Así como hay día y noche, siempre hay dos formas de encarar los problemas. Una forma es la directa, con lo primero que salta a la vista. La otra consiste en un camino indirecto, que tiene el poder de lo obvio y que denominamos el camino de las soluciones alternativas a las que tan acostumbrados estamos los latinoamericanos y que provoca una y sólo una exclamación: ¡Cómo no se me ocurrió!. Se trata de esas soluciones simples, que suplantan la más sofisticada computadora por una solución que pone en acción el paradigma que la sabiduría popular ha sintetizado con una frase: lo atamos con alambre. Verdaderamente el mundo progresa con soluciones alternativas. Se trata de soluciones simples, que son de una lógica total, pero por ser tan obvias no las vemos. Es el árbol que tapa el bosque, o éste que tapa el árbol. De una u otra manera no los vemos a ambos.

Dejemos el bosque, los árboles y la naturaleza por ahora. Hay cuestiones urgentes que resolver. Más allá de las soluciones alternativas que debemos formular, se hallan los peligros. Existe la sensación de que estamos rigurosamente vigilados. Como cuando hablamos de un Gran Hermano que todo lo observa y nos remontamos a los libros de Orwell. Ahora, eso nos conduce a los *reality shows*.

Hace un tiempo los medios periodísticos informaron una noticia que se extendió como un reguero de pólvora. El hecho es que aparentemente nos estaban vigilando a través de nuestros datos personales. La noticia era que había peligro porque una compañía norteamericana estaba vendiendo nuestros datos.

No se trataba de una cuestión menor, porque en el sitio de Internet www.epic.org estaba el contrato, donde al mejor estilo de la época de los cazadores de cabezas, se ofrecía al mejor postor nuestras cabezas o, mejor dicho, los datos de los cuales dependemos, esto es: inmuebles,

* • Director Nacional de Protección de Datos Personales, de Argentina; cargo en el que fue designado por concurso.
• Es Abogado y Doctor en Derecho y Ciencias Sociales de la Universidad de Buenos Aires.
• Tiene premios nacionales e internacionales como el Premio UNESCO.

Hace un tiempo los medios periodísticos informaron una noticia que se extendió como un reguero de pólvora. El hecho es que aparentemente nos estaban vigilando a través de nuestros datos personales. La noticia era que había peligro porque una compañía norteamericana estaba vendiendo nuestros datos.

autos, archivos judiciales, préstamos, información médica, etc. Pocos rubros se hallaban fuera del contrato, en el que la contraparte de la empresa privada sería nada menos que el Departamento de Justicia de los Estados Unidos de América. En México esta cuestión tuvo una amplia repercusión.

Esto que parece producto de una mente afiebrada es tan cierto que incluso (nos da vergüenza decirlo) se valuaban los datos de los "*agentine citizen*" en u$s 30 y una gama variada cuyos precios oscilan desde ese precio hasta los us$ 40.

Toda esta situación denunciada enérgicamente en varios Estados latinoamericanos y también en Argentina, pone en descubierto que estamos en peligro.

La informática es un progreso y también una amenaza. Eso no quiere decir que las computadoras, mismas sean peligrosas. Eso sería como decir que la culpa es del mensajero y no del mensaje.

Desde hace un tiempo se estaba planteando académicamente la posibilidad de estas intromisiones pero como de costumbre, se pensó que no sucedería. Sin embargo en Europa se encendieron las luces de alarma roja y se pusieron de acuerdo en la Red Echelon para defenderse de esas injerencias no autorizadas. Asimismo, fue noticia la desaparición de datos en el Reino Unido y en otros países del mundo.

Pero el tema tiene ribetes internacionales porque en el fondo se halla en juego un viejo principio que parece haber desaparecido del derecho internacional. Parece que el peligro del terrorismo es como el de ese cuento que para luchar contra los caníbales el mejor remedio es comerlos. Entonces, en este tema, el mejor remedio para obtener información no es el de recurrir a la colaboración internacional de Estado a Estado y proceder a un intercambio de información que asegure el cumplimiento de los requisitos de la legislación nacional e internacional en vigencia.

Ahora es el momento de protegerse

En la Argentina, hay una pared de fuego que protege a la gente en cuanto a la utilización incorrecta de los datos personales: la *Constitución Argentina* (art. 43), la *Ley Nº 25.326* y el *Decreto Reglamentario* (Nº1558/2001).

Ahora existe la Dirección Nacional de Protección de Datos Personales que constituye el primer escalón en la protección de los datos personales, ya que está diseñada para recibir denuncias y reclamos de quienes hubieran sufrido alguna de las situaciones como las que explicamos.

Hay un segundo escalón: la justicia. Los jueces están interpretando el derecho a la protección de los datos personales de manera dinámica y creativa a través de sus fallos que reiteran el contenido del clásico derecho a la intimidad del Art. 19 de la Constitución de 1853, reactualizado con la Reforma Constitucional de 1994.

La *Constitución Argentina* reformada en 1994 ha caracterizado la autodeterminación informativa que podría expresarse con la siguiente expresión: «Soy dueño de mis datos y nadie puede disponer de ellos sin mi consentimiento , salvo que sean datos públicos de libre acceso. Los datos integran los derechos humanos e incluso se ha establecido un recurso judicial para rectificación, supresión de datos, actualización llamado *habeas data*.»

A partir del año 2000 se sancionó la Ley Nº 25.326 que reglamentó esa norma y la puso en marcha, completándose posteriormente en el año 2001 con el establecimiento de la autoridad de control, la Dirección Nacional de Datos Personales y procediéndose a la designación por concurso de su titular en 2002. Así entonces, nuestros datos se hallan en bases de datos públicas y privadas. Algunas de las bases de datos son de libre acceso e incluso proveen informes. Por ejemplo la base de datos electorales, donde con sólo digitar nuestro número de DNI, se puede saber la mesa y el lugar donde votar. Eso permite incluso controlar los propios datos.

Lo mismo sucede con el *Boletín Oficial*, que en su apertura consagra el principio republicano de la publicidad de los actos de gobierno. Esas acciones son legítimas y autorizadas por la ley porque, como dijimos, soy dueño de mis datos. Lo que no se puede hacer es la cesión masiva de todos los datos de todos los ciudadanos, o habitantes o dueños de autos, etc., salvo que medie interés general. Los responsables de los Registros públicos, donde se hallan nuestros datos personales, son los que pueden dar esa autorización, por supuesto cumpliendo con la *Ley de Protección de los Datos Personales* Nº25.326.

Sin dudas, la información generalizada y abierta produce el progreso de la ciencia y la tecnología, pero al mismo tiempo abre un frágil espacio para superar los ámbitos privados de la confidencialidad. El problema es que la mayoría de los que usan la computadora e Internet no saben que mientras navegan son rigurosamente vigilados por una especie de Gran Hermano que verifica todos los sitios que el desprevenido usuario utiliza mientras navega, que dan como resultado un verdadero perfil de sus creencias, intereses, preferencias, etc.

Pero siempre el damnificado es el último en enterarse. En una reciente encuesta elaborada entre los países de la Unión Europea se llegó a la conclusión correcta: la mitad de las personas encuestadas, entendieron que hay un mínimo nivel de protección de los datos personales y sólo un pequeño porcentaje cree que hay un alto nivel. La gente tiene miedo de que sus datos sean usados incorrectamente, violando no sólo su bolsillo sino también su privacidad. Una consecuencia de todos esos resultados es la conclusión de que la falta de consentimiento de las personas para la utilización de sus datos es habitual, salvo los casos expresamente exceptuados por la Ley 25326 como, por ejemplo, los informes crediticios.

Volvamos a los planteos simples para resolver dilemas.

Por eso, pues, planteamos las soluciones directas y las alternativas indirectas. La computadora ya no es el punto de atención y la clave se halla en los datos y su tratamiento. Tengamos en cuenta que en este momento en cualquier lugar del mundo, nuestros datos están siendo objeto de tratamiento con diversas finalidades y sin nuestro consentimiento. De allí entonces el otro enfoque alternativo que tiene que ver con la nueva sociedad del Siglo XXI calificada como de la comunicación y de la información, y con ecología informática. Eso significa que ahora sería absurdo protestar y hablar de la maldita informática y la maldita información.

Pero la vida es siempre mezcla de peligros y desafíos. El desafío aquí representa importantes recursos para la economía. La transferencia de datos con protección adecuada para las personas es un plus que coloca a los Estados que se hallan en ese nivel en condiciones competitivas. Eso es lo que ha obtenido la Argentina en el marco de la UE y se halla entre los primeros Estados fuera de la mencionada UE que ha pasado el examen de compatibilidad. Generalizando, Argentina tiene normas de protección de datos personales a nivel del Reino Unido y de Francia. Es el primero de Latinoamérica y del hemisferio sur. Esperemos que pronto alguien más de la región nos acompañe.

En consecuencia la solución alternativa, lo nuevo, es incentivar el flujo de datos y la información, pero al mismo tiempo concientizar acerca de la protección de nuestros datos personales. De esta manera, los banqueros, economistas, abogados, contadores y todos aquellos que trabajen con datos personales deben ser custodios de éstos. En resumen: protejo los datos de los demás y me protejo a mi mismo.

Esa es una alternativa para dilucidar dos problemas con una sola solución: desarrollar los datos y el flujo de información junto con la adecuada protección a las personas. En eso consiste el desarrollo económico contemporáneo y está a medida de Latinoamérica, que no tiene tiempo para perder.

La transferencia de datos con protección adecuada para las personas es un plus que coloca a los estados que se hallan en ese nivel en condiciones competitivas.

Esos son los razonamientos alternativos que necesitamos ahora. Ese es el "pensamiento lateral" en tiempos de crisis, en que aspectos como la protección de datos pueden perderse en el bosque de las tribulaciones diarias, pero que de manejarse en modo correcto pueden conducir - tanto a nivel estatal como en las organizaciones privadas - a mejorar los procedimientos, el tratamiento de la información más sensible, y a nivel mundial, cumplir con estándares que ayudarán al comercio y a los servicios internacionales a posicionarse en modo más competitivo, lejos de los fríos *icebergs* del aislamiento, a favor de las personas.

Éste es el desafío de la inteligencia.

Las Obligaciones del Estado en Materia de Privacidad y Protección de los Datos Personales: **El Caso Mexicano**

Lina Ornelas*

1. Introducción

La protección de la persona y bienes del individuo es un principio tan viejo como el *common law*. Sin embargo, en muchas ocasiones se da por sentada la naturaleza y extensión de esta protección. Los cambios sociales, políticos y económicos han impuesto ciertamente, en estos últimos 200 años el reconocimiento de nuevos derechos. Hace mucho tiempo el Derecho establecía medios de reparación en caso de agresiones de hecho contra la vida y los bienes. Progresivamente, el ámbito de los derechos del hombre se fue ensanchando y hoy en día, el derecho a la vida supone una calidad de la vida, el derecho a ser libre garantiza el ejercicio de un amplio haz de derechos subjetivos, y el término propiedad abarca, en su significado actual, todo tipo de derechos de dominio, tanto tangibles como intangibles.[1]

En plena era de la sociedad de la información, la utilización masiva de la tecnología *urbi et orbi* ha tenido como consecuencia intrusiones en la esfera de la vida privada de las personas, al tiempo que provocó el nacimiento de un nuevo derecho denominado derecho a la protección de datos personales que consiste en el poder de disposición que tiene toda persona sobre su información, para decidir quién, cuándo y para qué utiliza dicha información personal. Se trata de un derecho de acuñación eminentemente europea distinto al derecho a la intimidad, pero que ha ido implantándose y adquiriendo carta de naturalización en todo el mundo.

El artículo pretende darle al lector un panorama general de las obligaciones que los Estados adquieren al ratificar instrumentos internacionales de derechos humanos en materia de protección a la vida privada y en particular, en el caso específico de México, de qué forma se ha dado recepción al derecho de protección de datos de carácter personal y las asignaturas pendientes en torno al tema.

2. Obligaciones del Estado en materia de privacidad en los instrumentos internacionales de derechos humanos

Los tratados de derechos humanos establecen obligaciones específicas para los Estados que los ratifican. Tales obligaciones se agrupan en dos vertientes. Por una parte la obligación de respetar y, por la otra, la obligación de garantizar los derechos humanos.

La primera implica la existencia de límites al ejercicio del poder público. En la teoría de los derechos humanos esto se traduce en que los Estados no pueden intervenir en las esferas individuales; se trata de la no injerencia del Estado en el ámbito privado. Como consecuencia, la función pública no puede violar los atributos inherentes a la persona humana directa o indirectamente.

Por su parte, el segundo grupo de obligaciones contiene la garantía del gobernado para que el Estado adopte las medidas necesarias que permitan el goce pleno y efectivo de los derechos humanos por parte de los individuos. Sobre los alcances de esta obligación, la Corte Interamericana de Derechos Humanos ha señalado lo siguiente:

"La segunda obligación de los Estados partes es la de 'garantizar' el libre y pleno ejercicio de los derechos reconocidos en la Convención a toda persona sujeta a su jurisdicción. Esta obligación implica el deber de los Estados partes de organizar todo el aparato gubernamental y, en general, todas las estructuras a través de las cuales se manifiesta el ejercicio del poder público, de manera tal que sean capaces de asegurar jurídicamente el libre y pleno ejercicio de los derechos humanos. Como consecuencia de esta obligación los Estados deben prevenir, investigar y sancionar toda violación de los derechos reconocidos por la Convención y procurar, además, el restablecimiento, si es posible, del derecho conculcado y, en su caso, la reparación de los daños producidos por la violación de los derechos humanos".[2]

Las medidas mencionadas comprenden la eliminación de los obstáculos para el goce de esos derechos en condiciones de igualdad; la instrucción a la población y a los funcionarios del Estado en materia de derechos humanos, y el ajuste de la legislación interna a fin de dar efecto a las obligaciones enunciadas en los instrumentos internacionales de derechos humanos.[3]

En este mismo sentido, el Tribunal Europeo de Derechos Humanos confirma que *"si bien la principal finalidad del Artículo 8 del Convenio Europeo de Derechos Humanos es proteger a las personas contra las injerencias arbitrarias del poder público, puede además imponer obligaciones positivas para que se respete efectivamente la vida privada, aunque sujetas al margen de apreciación del Estado"*,[4] precisando que estas obligaciones positivas *"pueden implicar la adopción de medidas tendientes a asegurar el respeto de la vida privada incluso en las relaciones de los individuos"*.[5]

Por lo tanto, el derecho a la vida privada tiene el doble carácter de derecho de libertad y de derecho de protección. A la hora de establecer si del Artículo 8, en el caso concreto, se deriva una obligación positiva para el Estado, el Tribunal emplea la prueba del *"justo equilibrio entre los intereses de la comunidad y los del particular"*, que funciona en la práctica como trasunto del principio de proporcionalidad.[6] El derecho a la vida privada como derecho de protección se dirige no sólo frente al legislador o la administración, sino también frente a los jueces a los que se les exige que en la resolución judicial de un conflicto entre particulares protejan de manera suficiente el interés del particular en el respeto de su vida privada.[7] En este orden de ideas, la obligación de garantizar también comprende la obligación de prevenir, la de investigar, la de sancionar y la de reparar los daños producidos en perjuicio de las personas.

Conviene resaltar que la Corte Interamericana de Derechos Humanos desarrolló el siguiente principio:[8]

"172. Es, pues, claro que, en principio, es imputable al Estado toda violación a los derechos reconocidos por la Convención cumplida por un acto del poder público o de personas que actúan prevalidas de los poderes que ostentan por su carácter oficial. No obstante, no se agotan allí las situaciones en las cuales un Estado está obligado a prevenir, investigar y sancionar las violaciones a los derechos humanos, ni los supuestos en que su responsabilidad puede verse comprometida por efecto de una lesión a esos derechos. En efecto, un hecho ilícito violatorio de los derechos humanos que inicialmente no resulte imputable directamente a un Estado, por ejemplo, por ser obra de un particular o por no haberse identificado al autor de la transgresión, puede acarrear la responsabilidad internacional del Estado, no por ese hecho en sí mismo, sino por falta de la debida diligencia para prevenir la violación o para tratarla en los términos requeridos por la Convención".

Por lo que respecta a esta responsabilidad del Estado por actos de particulares, éste tiene un deber de diligencia debida de prevenir, investigar y castigar las violaciones al derecho internacional y pagar una

* • Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública.
• Es egresada de la Facultad de Derecho de la Universidad de Guadalajara y es maestra en Derecho Internacional por la Universidad Libre de Bruselas.
• Coordina subgrupos de trabajo de la Red Iberoamericana de Protección de Datos Personales.

justa indemnización. No obstante lo anterior, pocas legislaciones en el mundo prevén la restitución a la víctima por la violación de su derecho a la protección de sus datos personales.

3. Instrumentos Internacionales ratificados por México

La Declaración Universal de los Derechos del Hombre establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques.[9]

En el mismo sentido, el Artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales,[10] reconoce el derecho de la persona al respeto de su vida privada y familiar de su domicilio y correspondencia.

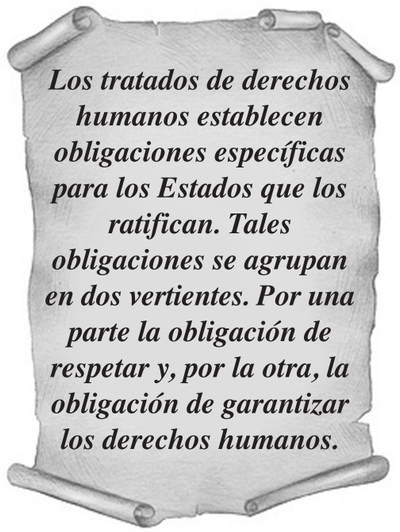
Por su parte, el Artículo del Pacto Internacional de Derechos Civiles y Políticos señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.[11]

En el mismo tenor, la Convención Americana sobre Derechos Humanos dispone que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.[12]

México ha ratificado los tratados de derechos humanos enunciados con anterioridad, los cuales son ley suprema de la nación de conformidad con el Artículo 133 de la Constitución Federal. Es decir, el Estado asume la responsabilidad del cumplimiento de las obligaciones adquiridas por la ratificación de tratados.

4. Cumplimiento de las obligaciones de México en materia de protección de datos personales

Anteriormente a la ratificación de los instrumentos internacionales de derechos humanos por parte de México, desde la Constitución Política de 1917, se establecieron derechos relativos a la libertad individual en lo concerniente a la vida privada, tales como inviolabilidad de correspondencia y domicilio y el secreto a las comunicaciones privadas. El Artículo 16 establece que 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 de procedimiento. Este derecho fue concebido más bien como un derecho pasivo



de no injerencia, mientras que el derecho a la protección de datos o a la autodeterminación informativa es un derecho activo por medio del cual el individuo toma decisiones y acciones sobre el uso de la información que le concierne.

No es hasta el año 2007 cuando se aprobó una reforma al Artículo 6º Constitucional mediante la cual se establece que la información referente a la vida privada y datos personales será protegida en los términos y con las excepciones que fijen las leyes.

La disposición anteriormente mencionada tiene la virtud de ser el primer reconocimiento expreso al derecho a la protección de los datos personales dentro de los derechos fundamentales previstos por nuestra Carta Magna; hecho que constituye la continuidad del ejercicio del derecho de acceso a la información y el cumplimiento de las obligaciones adquiridas por México en los instrumentos internacionales de derechos humanos. A través de la aprobación de las reformas mencionadas, México cumple con las obligaciones de respetar, contenidas en los instrumentos internacionales de derechos humanos mediante, el establecimiento disposiciones que imponen límites al ejercicio del poder público respecto al tratamiento de datos personales.

Sin embargo, este nuevo derecho reconocido en el Artículo 6º, garantiza al individuo la protección de los datos personales que se encuentren en los archivos gubernamentales en los tres órdenes de gobierno, mas no de aquellos que se encuentran en posesión de los particulares. Las reformas del 6º derivan del desarrollo que ha tenido el derecho a la protección de datos personales desde la publicación en el *Diario Oficial de la Federación* en el año 2002, de la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, la cual reconoce el derecho a la protección de datos personales y establece los derechos y principios de protección que deberán ser observados por los entes gubernamentales en el ámbito federal.

Como ya se apuntó anteriormente, respecto a las obligaciones de garantía, no obstante México ha ajustado su legislación interna a fin de dar efecto a las obligaciones enunciadas en los instrumentos internacionales de derechos humanos. Esto no ha sido de manera comprensiva ya que únicamente se protegen los datos en posesión de entes gubernamentales y no se le otorga al gobernado la garantía de conocer el tratamiento que se le da a su información por el sector privado, ni de acceder, rectificar, cancelar u oponerse a la utilización de los datos que le conciernen.

En ese sentido, es importante señalar que existen diversos foros y organismos internacionales de los cuales México es integrante, que cuentan con marcos de privacidad como referentes para permitir el flujo transfronterizo de datos, al tiempo que se garantiza por los Estados Miembros un mínimo de protección a los datos personales. Tal es el caso de la Organización para la Cooperación y el Desarrollo Económico (OCDE)[13]; la Organización de las Naciones Unidas (ONU)[14]; el Foro de Cooperación Economíca Asia Pacífico (APEC)[15]. Asimismo, tanto el Tratado de Libre Comercio de Norteamérica, como el Acuerdo de asociación económica, concertación política y cooperación entre la Comunidad Europea y sus Estados miembros, también denominado Tratado de Libre Comercio con la Unión Europea (TLCUE) prevén disposiciones sobre la protección de datos personales. En este último acuerdo México se compromete a contar con un nivel adecuado de protección. Finalmente es importante señalar que México es miembro de la Red Iberoamericana de Protección de Datos Personales, en el seno de la cual se aprobaron las Directrices para la armonización de la protección de datos en la comunidad Iberoamericana. Éstas constituyen un modelo acerca de lo que debe contener una legislación en los Estados miembros.

Derivado de lo anterior, en el H. Congreso de la Unión se han presentado dos iniciativas de reformas constitucionales a los Artículos 16 y 73. El primer artículo prevé el reconocimiento del derecho de protección de datos personales como un derecho fundamental y autónomo, así como los principios y derechos fundamentales que deben regir todo tratamiento de datos personales.[16] La reforma al Artículo 73 Constitucional tiene por objeto dotar de facultades al Congreso Federal para que legisle en materia de protección de datos personales en posesión de los particulares.[17]

5- Conclusión

A manera de conclusión podemos decir que el derecho a la protección de datos personales en México ha tenido una evolución para implantarse en el marco normativo. Primero a través de las disposiciones en materia de derecho a la vida privada contenidas en los tratados internacionales del Sistema Universal e Interamericano de Derechos Humanos. Posteriormente, la recepción del derecho concebido como un derecho autónomo y distinto al derecho a la vida privada e intimidad, se dio gracias al impulso de las leyes de transparencia y acceso a la información hasta reconocerlo a nivel constitucional en el Artículo Sexto. La membresía de México en diversos foros y organismos internacionales que prevén la protección de datos personales ha sido un factor, entre otros, que impulsan una nueva generación de reformas constitucionales a los Artículos 16 y 73, para preparar las condiciones que permitan la creación de una Ley de Protección de Datos aplicable también al sector privado. Los alcances de la misma están por definirse.

1 Vid. WARREN, Samuel y BRANDEIS Louis. *El derecho a la intimidad*, Editorial Civitas, Madrid. Traducción al castellano: Benigno Pendás y Pilar Balsega, 1995, pp. 21 y 22.
2 Velázquez Rodríguez, Sentencia de 29 de julio de 1988. Serie C N° 4, párrafo 166._
3 COMITÉ DE DERECHOS HUMANOS Observación General N° 28, párrafo 3._
4 Ress c. Reino Unido, 17 de octubre de 1986
5 Ver X e Y c. Países Bajos, sentencia de 26 de marzo de 1985
6 López Ostra c. España, sentencia de 9 de diciembre de 1994.
7 Abdulziz, Cabales y Balkandali c. Reino Unido, 28 de mayo de 1985.
8 Caso Velásquez Rodriguez, Sentencia de 29 de julio de 1988, párrafo 172.
9 Artículo 12, *Declaración Universal de los Derechos Humanos*, 10 de diciembre de 1948, disponible en http:www.un.org/spanish/aboutun/hrights.htm
10 http://www.derechos.org/nizkor/espana/doc/conveudh50.html.
11 Artículo 17, *Pacto Internacional de Derechos Civiles y Políticos*, 16 de diciembre de 1966, disponible en http://www.derechos.org/nizor/espana/doc/conveudh50.html
12 Artículo 11, apartado 2, *Convención Americana sobre Derechos Humanos,* 22 e noviembre de 1969, disponible en http://www.oas.org/juridico/spanis/Tratados/b-32.html
13 Directrices relativas a la protección de la intimidad privacidad y de la circulación transfronteriza de datos personales. Documento adoptado por el Consejo de la OCDE el 23 de septiembre de 1980.
14 Directrices para la regulación de los archivos de datos personales informatizados. Resolución 45/85 de la Asamblea General adoptada el 14 de diciembre de 1990.
15 Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, publicado en el año 2005.
16 Esta iniciativa fue presentada a la Cámara de Senadores, la cual el 18 de abril de 2006 fue aprobada y enviada para su revisión a la Cámara de Diputados. El 20 de septiembre de 2007, la Cámara de Diputados aprobó la iniciativa con ligeras variaciones respecto al texto original, enviándola a la Cámara de Senadores con fecha 25 de septiembre de 2007, para su aprobación en virtud de las variaciones del texto original.
17 La iniciativa al Artículo 73 Constitucional se presentó ante el Pleno de la Cámara de Diputados el 27 de marzo de 2007, misma que fue aprobada el 20 de septiembre de 2007 sin variaciones al texto propuesto. Asimismo, la Cámara de Diputados envió la Minuta respectiva al Senado de la República para su revisión con fecha 25 de septiembre de 2007

Las autoridades de protección de datos;
Ante el reto de la protección de datos de carácter personal

Antonio Troncoso Reigada*

En general, hay que asumir que cualquier Autoridad de Protección de Datos es pequeña en relación con la función atribuida de velar por el cumplimiento del derecho a la protección de datos personales en las sociedades modernas.

Las Agencias de Protección deben plantearse nuevas estrategias para los próximos años con la finalidad de mejorar el cumplimiento de la legislación de protección de datos personales. Así, se ha puesto en marcha recientemente el *London Initiative Workshop*, un grupo de trabajo del que forma parte la Agencia de Protección de Datos de la Comunidad de Madrid, con la finalidad de definir una estrategia que mejore la efectividad del trabajo de las Autoridades de Protección de Datos.[1] Las Autoridades de Protección de Datos cumplen distintas funciones: una función de control de ficheros, de tutela de derechos y de ejercicio de la potestad sancionadora, una función normativa o reguladora; una función vinculada a la publicidad y al Registro de Ficheros y una función de promoción del derecho fundamental a la protección de datos, asesorando a los responsables de ficheros e informando y atendiendo a los ciudadanos.[2]

La cuestión que corresponde debatir es qué función debe ser prevalente teniendo en cuenta que el objetivo es alcanzar el máximo nivel de cumplimiento de la legislación de protección de datos personales. Hay que tener presente un conjunto de circunstancias como el incremento del número de reclamaciones, sobre todo de aquellas en las que la protección de datos no es un tema principal sino accesorio a otras cuestiones -políticas y laborales- que suponen, en muchos casos, un abuso del sistema. A esto se le une que los recursos humanos y económicos de las agencias son limitados, lo que hace que se acumulen los asuntos pendientes[3]. En general, hay que asumir que cualquier Autoridad de Protección de Datos es pequeña en relación con la función atribuida de velar por el cumplimiento del derecho a la protección de datos personales en las sociedades modernas. Se ha planteado, por ello, la necesidad de que las Agencias de Protección de Datos sean selectivas -*Selective to be effective*- lo que les permita decidir su propia agenda, de forma que su actividad tenga más efectividad e influencia en la vida real de los ciudadanos.

Sin embargo, hay que señalar que el modelo español de protección de datos -a nuestro juicio también el modelo europeo presente en la Directiva 95/46/CE- está basado en el reconocimiento de un derecho fundamental a la protección de datos personales. Esto supone que como derecho fundamental debe ser tutelado por los poderes públicos, tanto por las Autoridades de Protección de Datos como por los Tribunales. De esta forma, todas las personas a las que se les vulnere su derecho fundamental a la protección de datos personales tienen que tener una tutela administrativa por una autoridad independiente de control y una tutela jurisdiccional. Es, por tanto, un modelo basado en derechos donde no es posible la selección de los casos ya que la legislación establece que todos deben ser tramitados y nadie puede quedarse indefenso sin una tutela administrativa y jurisdiccional efectiva. Las Agencias de Protección de Datos desarrollan, como hemos señalado en otra ocasión, una función materialmente jurisdiccional y, como los jueces ordinarios, no priorizan ni seleccionan los casos que les llegan. Por ello, el *Selective to be effective* aplicado a las denuncias de particulares tiene un impacto negativo sobre los derechos de las personas y sobre sus garantías; sobre la protección real y efectiva que merecen todos los ciudadanos. De esta forma, una Agencia de Protección de Datos que elija los asuntos en los que se va a ocupar -por ser más importantes o porque suponga más riesgos- se aleja del modelo basado en derechos.[4] Ya le ha correspondido al legislador determinar en la tipificación de las infracciones y las sanciones qué conductas le parecen más graves o suponen más riesgos[5]. Además, como hemos señalado en otra ocasión, la actividad inspectora y sancionadora es necesaria para la credibilidad de una autoridad de control. La selección de algunos casos y el rechazo de otros dañan la legitimidad de una autoridad de control desde la perspectiva de los ciudadanos. De hecho, una de las principales causas de divergencia en el cumplimiento de la Directiva Europea 95/46/CE de protección de datos personales es el distinto nivel -por no decir, la ausencia completa en algunos casos- *de enforcement* en algunos países.[6] Téngase en cuenta que un desfallecimiento de la actividad de control y de exigencia del cumplimiento de la legislación por parte de las agencias deja como único recurso los órganos jurisdiccionales -que carecen de la especialidad suficiente-, lo que debilita los derechos de los ciudadanos.[7] La selección de los temas por los órganos jurisdiccionales tiene sentido en las últimas instancias cuando se ha dado ya una tutela judicial efectiva pero no es aplicable en la primera tutela administrativa ya que supondría una limitación a los principios y derechos de protección de datos de los ciudadanos.[8]

La selección, si bien no puede aplicarse a las denuncias de los ciudadanos, sí puede tenerse en cuenta a la hora de ordenar los recursos en la propia tramitación de las denuncias. Siempre se pueden establecer criterios para no tratar todas las denuncias del mismo modo o para no invertir el mismo número de personas, teniendo en cuenta la complejidad de los temas, el daño que se puede causar y el número de personas implicadas. También es posible la selección en la actividad de inspección de oficio -cuando no existen denuncias de los ciudadanos- que debe centrarse en aquellas violaciones más severas de la protección de datos. Especialmente las agencias pueden ser selectivas en el desempeño de otras actividades como el desarrollo normativo, la actividad de consultoría o la educación y concienciación de los ciudadanos. Es, por tanto, necesario establecer unas prioridades estratégicas en la actividad de las Agencias de Protección de Datos. Lógicamente, el debate pasa ahora a centrarse en cuáles deben ser los criterios de selección, en la necesidad de establecer una metodología para determinar los riesgos más importantes que afectan a la protección de datos personales. Posiblemente la selección debe centrarse en el tipo de riesgo -por ejemplo, por la tipología de datos personales objeto de tratamiento (por ejemplo, datos especialmente protegidos)- teniendo en cuenta la repercusión en sus derechos o por ser temas que afecten a toda la sociedad -no ser casos individuales- (por ejemplo, el pago de un impuesto como el de Bienes Inmuebles).

En la labor de concienciación de los ciudadanos es necesario aprovechar la capacidad de influencia que tienen los medios de comunicación, teniendo en cuenta que las propias entidades públicas y privadas temen más la repercusión de un hecho en un medio de comunicación social que las propias sanciones económicas

Son muchas las iniciativas que las Agencias de Protección de Datos pueden impulsar para llegar a los ciudadanos y para ser más eficaces. En este texto hemos comentado algunas de ellas, como los Sellos de Privacidad -*Europrise*- o los Premios de Mejores Prácticas. Además, teniendo en cuenta los riesgos que las nuevas tecnologías suponen para la protección de datos personales, hay otros instrumentos que hay que mencionar como los *Privacy Impact Asessment* -PIAs-. En la labor de concienciación de los ciudadanos es necesario aprovechar la capacidad de influencia que tienen los medios de comunicación, teniendo en cuenta que las propias entidades públicas y privadas temen más la repercusión de un hecho en un medio de comunicación social que las propias sanciones económicas[9]. Es conveniente también llegar a acuerdos de cooperación con grupos y entidades que pueden ser aliados útiles en la defensa de este derecho fundamental. Si bien en la protección de datos personales no existe en muchas ocasiones una sociedad civil estructurada, sí hay algunas en-

* • Director de la Agencia de Protección de Datos de la Comunidad de Madrid
• Doctor en Derecho por la Universidad de Bolonia con la calificación summa cum laude y Primer Premio Nacional de Terminación de Estudios Universitarios.
• Profesor Titular de Derecho Constitucional

La falta de una actividad de supervisión y sanción por parte de distintas Autoridades de Protección de Datos ha generado divergencias en el cumplimiento de la Directiva, lo que ha repercutido no sólo en el respeto al derecho fundamental sino también en el propio funcionamiento del mercado interior

tidades -ONGs, sindicatos, asociaciones de consumidores- que puede ayudar en el trabajo de las agencias, alcanzando sinergias[10]. Igualmente, la firma de acuerdos con administraciones públicas y con entidades privadas sometidas a control puede ser una oportunidad para tejer una red de interlocutores que ayuden a las Agencias de Protección de Datos a cumplir su función.

Por último, es esencial para el desarrollo de la protección de datos la motivación de las personas que trabajan en las autoridades de control. Como he tenido la oportunidad de señalar recientemente, lo verdaderamente importante en las Autoridades de Protección de Datos no somos las personas que coyunturalmente ocupamos los puestos de dirección sino los empleados públicos que con el paso de los años han ido dando continuidad al trabajo administrativo de las Autoridades de Protección de Datos en beneficio de los ciudadanos.

[1] Forman parte de este grupo las autoridades de protección de Datos de España, Canadá y Saskatchewan, República Checa, Alemania, Supervisor Europeo, Rumanía, Reino Unido, Francia, Suecia, Irlanda, Italia y la Agencia de Protección de Datos de la Comunidad de Madrid. Este grupo también ha abordado otras cuestiones internas de la gestión de las Agencias de Protección de Datos como la formación y profesionalización del personal y la medida y evaluación del desempeño.

[2] Bennet y Raab han clasificado las distintas funciones de las agencias en las siguientes: *Ombudsman*, Auditor, Consultor, Educador, Negociador, *Policy Advisor* y *Enforcer*. Estas funciones pueden ser reducidas a tres: una función mediadora, una función controladora y una función formadora. Cfr. más ampliamente C. J. BENNET y CH. RAAB, *The Government of Privacy. Policy instruments in global perspective*, Ashgate Publishing Limited, Hampshire, 2003, págs. 91-120 y C. J. BENNETT, *Regulating privacy. Data Protection and Public Policy in Europe and the United Status,* Cornell University Press, Ithaca and London, 1992, especialmente el apartado *"The Choice of Policy Instruments"* págs. 153-193. En otras ocasiones he tenido la oportunidad de exponer el trabajo de la APDCM clasificándolo en diversas actividades: el desarrollo normativo, el apoyo a la declaración de ficheros y publicidad registral, la exigencia del cumplimiento de la legislación -que incluye la actividad de inspección y de tutela de derechos-la actividad consultiva y de asesoramiento jurídico a los responsables de ficheros y a los empleados públicos, la actividad formativa, las publicaciones y los proyectos de gestión del conocimiento, la actividad internacional, la atención al ciudadano y la actividad interna de la Agencia -la gestión económico-administrativa y de personal y el plan de calidad-. Cfr. A. TRONCOSO REIGADA, "La Agencia de Protección de Datos de la Comunidad de Madrid: régimen jurídico y funciones" en *Estudios sobre Administraciones Públicas y Protección de Datos Personales*, Civitas, Madrid, 2006, págs. 195-221; y "La actividad prestacional del derecho fundamental a la protección de datos pesonales: el ejemplo de la Agencia de Protección de Datos de la Comunidad de Madrid", en Estudios sobre Comunidades Autónomas y Protección de Datos Personales, Civitas, Madrid, 2006, págs. 277-312.

[3] *La Memoria de la Agencia Española de Protección de Datos 2006* recogía que había más de mil casos pendientes, algunos con dos años de antigüedad.

[4] Para un modelo basado en derechos no parece muy razonable que sean las agencias las que decidan las denuncias que van a ser tramitadas ya que cada denuncia es importante para el ciudadano que la presenta.

[5] Así, es posible que el legislador clasifique los distintos supuestos atendiendo a su mayor o menor peligrosidad, tratándoles de forma distinta, una posibilidad presente en algunas partes de la Directiva pero que no ha sido transpuesta en nuestro país.

[6] Algunas Autoridades de Protección de Datos han estado tradicionalmente más centradas en elaborar recomendaciones e informes para el Parlamento y para las instituciones nacionales pero poco preocupadas en exigir el cumplimiento de la legislación de protección de datos personales en sus respectivos países. La falta de una actividad de supervisión y sanción por parte de distintas Autoridades de Protección de Datos ha generado divergencias en el cumplimiento de la Directiva, lo que ha repercutido no sólo en el respeto al derecho fundamenta sino también en el propio funcionamiento del mercado interior -ya que ha originado deslocalizaciones de empresas-, uno de los objetivos de la Directiva. Cfr. sobre esta cuestión, A. TRONCOSO REIGADA *"Introduction and Presentation", An approach to data protection in Europe*, Thomson-Civitas-APDCM, Madrid, 2007, págs. 14-23. Sin embargo, parece que recientemente -en los últimos tres años- algunas autoridades europeas han descubierto el *enforcement*, una actividad que la Agencia Española de Protección de Datos -y las Agencias Autonómicas- han desarrollado desde su creación. Esta es una cuestión que también hemos comentado en A. Troncoso Reigada, "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público* núms. 19-20, 2003, págs. 314-315.

[7] La jurisdicción contencioso-administratriva cumple una función indispensable en el control de la actividad de las agencias pero el modelo europeo de protección de datos no ha querido que sean los Tribunales el único instrumento en este ámbito. Hay que señalar que en nuestro país, como señalan las Memorias de la Agencia Española de Protección de Datos, el 85% de las sentencias confirman las Resoluciones de la Agencia Española.

[8] Una primera reflexión sobre el carácter objetivo o subjetivo del recurso de amparo al Tribunal Constitucional lo hemos hecho en "Método jurídico, interpretación constitucional y principio democrático", en E. ESPÍN y F. J. DÍAZ REVORIO, *La justicia constitucional en el Estado democrático*, Tirant lo blanch, Valencia, 2000, págs. 440-450.

[9] Son muchas las sugerencias que se han hecho para facilitar que el mensaje de las Agencias de Protección de Datos cale en los medios de comunicación: comunicar malas noticias para mejorar la concienciación y atraer la atención de los medios; contar "el caso del mes" -una historia de cómo una vulneración de la protección de datos personales ha afectado la vida de una persona- que permita hacer que la privacidad sea visible, con cosas que le interesen a la gente; tener un enfoque oportunista, aprovechando cualquier ocasión para comunicar nuestro mensaje -*"riding the media tiger"*-.

[10] La Agencia de Protección de Datos de la Comunidad de Madrid ha firmado en los últimos años distintos Convenios de los que hemos dado cuenta en las distintas Memorias: ONG *Access Info Europe*, la Comisión de Libertades Informáticas, la Confederación Española de Consumidores y Usuarios, Asociaciones de Empresas de Telecomunicaciones, etc.

La Protección de **Datos Personales** en México: Avances en la Legislación Federal

Luis Gustavo Parra Noriega*

Hoy en día la circulación de los datos personales es prácticamente ilimitada. La informática ha tenido significativos avances y en consecuencia existe un alto grado de capacidad de almacenamiento de los ordenadores, así como de fórmulas que permiten correlacionar la información existente a velocidades inimaginables, y que en cuestión de segundos pueden elaborar perfiles bien definidos de las personas en base a su información personal.

Es innegable que los avances en el campo de la informática traen consigo beneficios importantísimos en diversos campos de la ciencia. Sin embargo, en forma paralela ha surgido una amenaza latente para los titulares de los datos personales. Ellos corren el riesgo de que sus datos sean usados para fines perversos que pueden generar desde simples actos de molestia consistentes, por ejemplo, en el constante ofrecimiento de créditos, hasta la comisión de delitos como el secuestro o el robo de identidad.

...corren el riesgo de que sus datos sean usados para fines perversos que pueden generar desde simples actos de molestia consistentes por ejemplo, en el constante ofrecimiento de créditos, hasta la comisión de delitos como el secuestro o el robo de identidad.

Cabe señalar que el respeto a la dignidad de la persona constituye la base fundamental de la protección de datos personales. Toda vez que este derecho se basa en el poder de disposición de los datos por su titular, lo anterior implica que la persona que tenga a su cargo el tratamiento de datos personales los deberá utilizar con estricto respeto a los derechos del interesado.

Por lo anterior, no cabe la menor duda de que es urgente en nuestro país contar con una regulación jurídica que garantice a las personas la protección necesaria frente a la intromisión de los demás en su esfera privada.

Actualmente en México existen referentes legales en materia de protección a la privacidad de la persona, tanto en la Constitución General de la República como en leyes federales. Sin duda un avance significativo lo es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como las recientes reformas al Artículo 6º Constitucional. Sin embargo la tarea está pendiente respecto a los datos personales en posesión de particulares. Hoy en día no contamos a nivel federal con una Ley de Protección de Datos Personales, a

* • Diputado Federal.
• Doctor en Teoria Política, Teoría Democrática y Administración Pública.
• Colaborador de la revista *"Bien Común y Gobierno"*.

Actualmente el Congreso de la Unión no cuenta con atribuciones expresas para legislar sobre la materia. Esto ha generado que entidades federativas como Colima cuenten con una legislación sobre protección de datos personales.

pesar de que existen diversas iniciativas de ley en la materia que han sido presentadas en distintas Legislaturas y por legisladores pertenecientes a distintos partidos políticos.

En la LVIII Legislatura el Senador Antonio García Torres presentó una Iniciativa de Ley Federal de Protección de Datos Personales,[1] con el objeto de asegurar que el trato de datos personales se realice con respeto a las garantías de las personas físicas. La Iniciativa fue dictaminada[2] favorablemente por las Comisiones de Puntos Constitucionales y de Estudios Legislativos del Senadode la República y remitida a la Cámara de Diputados, como Minuta del Senado que contiene, el proyecto de Ley Federal de Protección de Datos Personales.[3] La Comisión de Gobernación de la Cámara de Diputados, a la que fue turnada la Minuta, la dictaminó en sentido negativo estableciendo, en la parte considerativa del Dictamen, que ante la ausencia de un precepto constitucional que faculte al Congreso de la Unión para legislar en materia de datos personales, se entiende que estaríamos frente a una facultad concurrente entre la Federación, los estados y los municipios. Por ello el proyecto debería contener lineamientos generales de las facultades que a cada orden de gobierno corresponden, desarrollando el contenido de una ley general.

En la Cámara de Diputados de esa misma Legislatura, el entonces Diputado Miguel Barbosa Huerta, presentó una Iniciativa de Ley Federal de Protección de Datos Personales,[4] la cual toma en cuenta la Directiva 95/46 sobre Privacidad y Protección de Datos de la Unión Europea. En su artículo primero establece como objeto de la ley la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes.

Posteriormente, en la LIX Legislatura el Diputado Jesús Martínez Álvarez presentó el 1º de diciembre de 2005 una Iniciativa de Ley Federal de Protección de Datos Personales.[5] Esta tiene por objeto garantizar la protección de los datos personales que se encuentren contenidos en documentos, archivos, registros, bancos de datos, o bien, en otros medios tecnológicos de procesamiento de datos, sean de carácter públicos o privados, a efecto de proteger y garantizar la identidad personal, la privacidad, la imagen y el honor, así como el acceso a la información en los términos de los artículos 6, 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos.

En esa misma LIX Legislatura, el entonces Diputado David Hernández Pérez presentó el 23 de febrero de 2006, una iniciativa de Ley Federal de Protección de Datos Personales.[6] En ella establece como objeto proteger los datos personales de los titulares y regular su tratamiento por parte de los sujetos regulados por ésta.

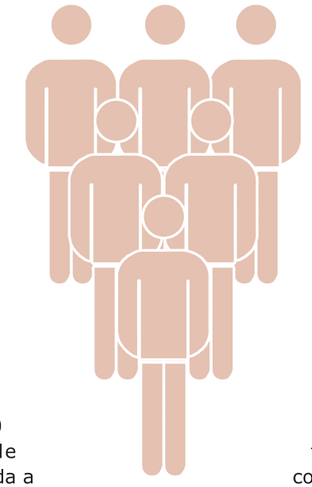
Posteriormente, el 22 de marzo de 2006, la Diputada Sheyla Fabiola Aragón Cortés presentó una Iniciativa de Ley Federal de Protección de Datos Personales,[7] la cual en su artículo primero establece como objeto, proteger los datos personales, así como regular el tratamiento que de los mismos realicen las entidades previstas en la propia iniciativa. Es importante mencionar que dicha propuesta sigue los lineamientos internacionales que en la materia han emitido la OCDE y la APEC.

Actualmente el Congreso de la Unión no cuenta con atribuciones expresas para legislar sobre la materia, lo que ha generado, que entidades federativas como Colima cuenten con una legislación sobre protección de datos personales. Con lo anterior, se genera el problema del ámbito espacial de aplicación de dicha normatividad, dado que un mismo sujeto obligado al cumplimiento de los preceptos en materia de protección de datos personales, deberá observar las disposiciones contenidas en dos instrumentos jurídicos de órdenes diferentes, que bien pudiesen ser contrapuestos entre sí, como lo son la normativa estatal y la federal.

En las Consideraciones del Dictamen se hace referencia a la relevancia de emitir un dictamen en el que, por primera vez en la historia de México, al máximo nivel de nuestra pirámide normativa se reconoce la existencia de un nuevo derecho distinto y fundamental a la protección de datos personales.

La protección de la privacidad de los datos personales se ha convertido en un tema prioritario de inmediata e inevitable atención. Sin embargo el Congreso de la Unión, en términos de nuestro esquema de división de competencias entre los órdenes de gobierno del Estado mexicano, no cuenta con facultades expresas para legislar sobre la materia. A la fecha, el establecimiento de marcos legislativos diversos en materia de protección de datos personales, por parte de las entidades federativas, puede 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 restrinjan el comercio entre las propias entidades federativas, y resultar contrarios a los lineamientos adoptados por los organismos internacionales de los cuales forma parte el Estado mexicano.

Lo anterior, así lo manifesté al presentar en la LX Legislatura la Iniciativa que reforma el Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos,[8] para facultar al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares. En dicha iniciativa reconozco la importancia de legislar en la materia al decir en la parte expositiva que: *"...debe destacarse que es impostergable la responsabilidad de esta soberanía para legislar en materia de protección de la privacidad de los datos personales de los individuos, no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino porque tiene un origen y efectos esenciales sobre la economía nacional y el aseguramiento del comercio irrestricto entre las entidades federativas, y con la regulación del comercio con otros estados extranjeros."*



La Iniciativa fue turnada a la Comisión de Puntos Constitucionales de la Cámara de Diputados. Posteriormente fue dictaminada positivamente[9] y aprobada en esa Cámara el jueves 20 de septiembre de 2007, siendo turnada a la Cámara de Senadores para los efectos constitucionales y actualmente se encuentra en proceso de dictaminación.

Otro avance legislativo importante en la materia que nos ocupa, es el Dictamen a la Minuta con proyecto de decreto por el que se adicionan dos párrafos al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos,[10] el cual fue aprobado en la Cámara de Diputados y devuelto a la Cámara de Senadores para los efectos de lo dispuesto en el Artículo 72 inciso e) de la Constitución Política de los Estados Unidos Mexicanos.

En las Consideraciones del Dictamen se hace referencia a la relevancia de emitir un dictamen en el que por primera vez en la historia de México al máximo nivel de nuestra pirámide normativa se reconoce la existencia de un nuevo derecho distinto y fundamental a la protección de datos personales, dentro del catálogo de garantías. Esta nueva garantía constitucional 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.

El dictamen reconoce 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, considerando que hasta ahora no se cuenta con una disposición a nivel constitucional en la que se establezcan el contenido y los alcances de este derecho, en cuanto a los principios, derechos y excepciones por los que se debe regir todo

Los dos párrafos que en el citado Dictamen, se propone adicionar al artículo 16 de nuestra Carta Magna son los siguientes:
"Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes.

tratamiento de datos personales.

Los dos párrafos que en el citado Dictamen, se propone adicionar al Artículo 16 de nuestra Carta Magna son los siguientes:

"Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes.

"La Ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud públicos o para proteger los derechos de tercero."

Por otra parte, cabe señalar que en días próximos estaré presentando ante el Pleno de la Cámara de Diputados, una iniciativa de Ley de Protección de Datos Personales en Posesión de Particulares, la cual contendrá principios fundamentales, siendo algunos de ellos el del consentimiento, la seguridad y la confidencialidad. Por otra parte, en el diseño del proyecto legislativo se establecerán derechos a favor de los titulares de los datos personales consistentes en los derechos de acceso, rectificación, cancelación y oposición, previendo el procedimiento respectivo para ejercerlos. Con la finalidad de dar certeza en la aplicación de la Ley, el proyecto establece y regula la autoridad encargada de hacer vigentes las disposiciones de la Ley, así como las sanciones que se aplicarán en caso de incumplimiento.

Finalmente, cabe señalar que el tema de la protección de datos personales en posesión de particulares plantea retos y desafíos importantes ante una eventual legislación. Estos tienen que ver con los temas de seguridad pública, respeto a los derechos fundamentales de las personas, desarrollo económico y comercial, así como combate a la discriminación. Concretamente en materia de desarrollo económico, es indispensable contar en nuestro país con un marco jurídico que ofrezca un adecuado nivel de protección de datos personales, que permita el intercambio comercial con otros países.

Vía

[1] Publicada la iniciativa en la *Gaceta Parlamentaria de la Cámara de Senadores.* Año IV, número 688, jueves 15 de febrero de 2001.
[2] Publicado el dictamen en la *Gaceta Parlamentaria de la Cámara de Senadores* Legislatura LVIII. Año 2, Gaceta Nº 55 de fecha 30 de abril de 2002.
[3] Publicada la Minuta en la *Gaceta Parlamentaria de la Cámara de Diputados* el 5 de septiembre de 2002.
[4] Publicada en la *Gaceta Parlamentaria de la Cámara de Diputados.*
[5] Publicada en la *Gaceta Parlamentaria de la Cámara de Diputados,* número 1895-I, jueves 1 de diciembre de 2005.
[6] Publicada en la *Gaceta Parlamentaria de la Cámara de Diputados,* número 1953-I, jueves 23 de febrero de 2006.
[7] Publicada en la *Gaceta Parlamentaria de la Cámara de Diputados*, número 1972-I, miércoles 22 de marzo de 2006.
[8] Publicada en la *Gaceta Parlamentaria de la Cámara de Diputados*, número 2221-I, martes 27 de marzo de 2007.
[9] Dictamen publicado en la *Gaceta Parlamentaria de la Cámara de Diputados.* Número 2339 de fecha miércoles 12 de septiembre de 2007.
[10] Dictamen publicado en la *Gaceta Parlamentaria de la Cámara de Diputados*. Número 2343-II de fecha martes 18 de septiembre de 2007.

Jurisprudencia Relevante Sobre el Derecho a La Información, **Caso Coahuila**

Sandrino Saucedo Contreras*

"Antes los derechos fundamentales sólo valían en el ámbito de la ley. Hoy la ley sólo vale en el ámbito de los derechos fundamentales."
H. Kruger

INTRODUCCIÓN.

El derecho a la información es un derecho nuevo, que alcanza nuevos horizontes con motivo de la reforma constitucional al artículo sexto,[1] en donde desde la propia norma fundamental del País se establecen principios y estándares mínimos para el ejercicio del derecho a la información en todo el territorio nacional. De esta forma se asegura una congruencia básica sobre una base sólida, que es la norma constitucional, que sirve para que los estados miembros de la Federación adecúen o, en su caso, emitan las leyes relativas a regular el derecho a la información.

En el año 2002, con motivo de la expedición de la *Ley Federal de Transparencia y Acceso a la Información*, se empezó a dar un movimiento en todo el país para reglamentar este derecho fundamental emitiendo las entidades federativas diversas leyes de la materia, algunas con mas aciertos que otras. Todas tenían en común establecer criterios de clasificación de información, procedimientos expeditos, instancias que garantizaran el derecho, recursos, obligación de conservar la documentación, etc.

Es por lo que en Coahuila, en el año 2003, el Congreso del Estado emitió la *Ley de Acceso a la Información Pública*, y crea un órgano constitucional autónomo denominado Instituto Coahuilense de Acceso a la Información Pública(ICAI). Al mismo tiempo el Ayuntamiento de Torreón, Coahuila emitía su Reglamento Municipal en la materia creando un órgano desconcentrado denominado Instituto Municipal de Transparencia, dotándolo de atribuciones para garantizar el derecho a la información al interior del municipio.

Con dicho antecedente, tarde o temprano tenia que existir un conflicto de competencias entre autoridades locales y municipales que se encargaban de garantizar el derecho a la información. El ICAI, por un lado, con competencia en los municipios para resolver conflictos entre particulares y entes públicos sobre acceso a la información y el Instituto Municipal de Transparencia de Torreón, Coahuila con competencia también para resolver conflictos entre particulares y sujetos obligados del propio municipio. Pero además, no sólo el conflicto versaba sobre instancias competentes, sino también sobre

* • Director Jurídico del Instituto Coahuilense de Acceso a la Información Pública.
• Licenciado en Derecho por la Facultad de Jurisprudencia UA de C.
• Ha sido catedrático de diversas materias, en la Universidad Autónoma de Coahuila, como la Facultad de Economía.

Es por lo que en Coahuila, en el año 2003, el Congreso del Estado emite la Ley de Acceso a la Información Pública, y crea un órgano constitucional autónomo denominado Instituto Coahuilense de Acceso a la Información Pública;

Se concluye que el Instituto Coahuilense de Acceso a la Información Pública, cuya existencia y facultades están consignadas en la Constitución y normas locales, no interfiere en el ejercicio del gobierno municipal

regulación o, si se quiere, legislación y reglamentación diversa sobre el mismo derecho fundamental. Éste incluye requisitos para acceder a la información, clasificación de información, medios de impugnación, dándose las denominadas antinomias entre el texto expreso de la *Ley de Acceso a la Información Pública y el Reglamento de Transparencia y Acceso a la Información Pública* del citado municipio.

Con lo anterior se puede percatar el lector de las incongruencias que se pueden dar entre los Reglamentos Municipales y las Leyes Estatales,[2] que se traducen en inseguridad jurídica para los ciudadanos, al no saber a qué atenerse sobre qué ley se debe aplicar o, dicho en otros términos, que norma es la "buena" para obedecerla y hacerla cumplir, porque obviamente, hay una de ellas que no es válida dentro de nuestro sistema jurídico. En ese sentido la Jurisprudencia que hoy se comenta tiene que ver precisamente con este aspecto.

1.Antecedentes de la Jurisprudencia citada: Controversia Constitucional 62/2005 promovida por el Ayuntamiento de Torreón vs Poder Legislativo, Ejecutivo e Instituto Coahuilense de Acceso a la Información Pública.

En el año 2005, el Ayuntamiento de Torreón, promovió ante la Suprema Corte de Justicia de la Nación(SCJN), una controversia Constitucional[3] demandando al Congreso del Estado, la emisión de la *Ley de Acceso a la Información Pública del Estado* y la *Ley del Instituto Coahuilense de Acceso a la Información*. Se le asignó el número estadístico 61/05, le tocó conocerla al Señor Ministro Jesús Gudiño Pelayo quien, en su momento, elaboró el proyecto de resolución para posteriormente presentarla al Pleno de la Suprema Corte de Justicia de la Nación, contando con los siguientes antecedentes:

El 6 de junio de 2003, se publica el *Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Torreón*, entrando en vigor al día siguiente de su publicación.

El 12 de agosto de 2003, el Congreso del Estado de Coahuila, aprueba las reformas a la Constitución Política local en materia de acceso a la información.

El 4 de noviembre de 2003, se pública la *Ley de Acceso a la Información Pública del Estado*.

El 1 de diciembre de 2004, inicia funciones el Instituto Coahuilense de Acceso a la Información Pública.

16 de agosto de 2005, se presenta solicitud de información por parte de un ciudadano al Municipio de Torreón, sobre estudios técnicos.

El 22 de agosto de 2005, el Ayuntamiento entrega sólo parte de la información solicitada. El resto lo considera como reservada, con fundamento en su reglamento.

El 6 de septiembre de 2005 la Secretaría del Ayuntamiento de Torreón recibe oficio del ICAI en donde se le pide que cumpla con la Información Pública Mínima y que proporcione la información restante al ciudadano.

El 27 de septiembre de 2005, el Instituto Coahuilense de Acceso a la Información Pública promueve acción de inconstitucionalidad en contra del *Reglamento de Transparencia y Acceso a la Información*, ya que se considera que el mismo es inconstitucional, entre otros motivos, por crear una instancia al interior del Municipio que resolvería en definitiva sobre las solicitudes de información diverso al Órgano Constitucional Autónomo creado para tal efecto.

El 30 de septiembre de 2005, se presenta demanda por parte del Municipio de Torreón en contra del H. Congreso del Estado, reclamando la inconstitucionalidad de varios artículos, y contra el ICAI por los actos de aplicación consistentes en requerir informes e iniciar un procedimiento ante el Instituto.

El 24 de enero de 2008, la Suprema Corte de Justicia de la Nación en sesión del Pleno resolvió la citada controversia constitucional que promoviera el Ayuntamiento declarándola infundada, pero sentando diversos criterios interpretativos con el carácter de jurisprudencia, mismos que se reproducen a continuación.

2. Principales Tesis emitidas por la SCJN.

Cabe destacar que la citada Controversia Constitucional 62/05, dió lugar a nueve tesis jurisprudenciales[4] por el Alto Tribunal del País. Por razones de espacio sólo se reproducen tres de ellas, las cuales se consideran las más importantes para el ámbito del derecho de acceso a la información pública en los estados.[5] Sin embargo, si al lector le interesa consultarlas en su totalidad, las mismas se encuentran disponibles en la página de la SCJN identificadas con los números: 52, 53, 54, 55, 56, 57, 58, 59 y 60 todas ellas del año 2008.

Las siguientes tesis fueron producto, en gran parte, de los argumentos planteados tanto en la demanda de controversia constitucional, y en las contestaciones del Poder Legislativo, Ejecutivo e Instituto Coahuilense de Acceso a la Información Pública, así como en las causales de improcedencia que sirvieron de base, directa e indirectamente, para la formulación de las mencionadas tesis.

TESIS JURISPRUDENCIAL Núm. 58/2008 (PLENO)

"INSTITUTO COAHUILENSE DE ACCESO A LA INFORMACIÓN PÚBLICA. NO INTERFIERE EN EL EJERCICIO DEL GOBIERNO MUNICIPAL. Si bien es cierto que el Municipio de Torreón cuenta con facultades exclusivas para ejercer actos de gobierno en su territorio, también lo es que se encuentra sujeto a sistemas estatales que permiten conocer el contenido de dichos actos. En este sentido, se concluye que el Instituto Coahuilense de Acceso a la Información Pública, cuya existencia y facultades están consignadas en la Constitución y normas locales, no interfiere en el ejercicio del gobierno municipal, pues de las atribuciones conferidas al referido Instituto no se advierte que irrumpa preponderante o decisivamente sobre las funciones que corresponden al órgano de Poder Municipal, sino que dichas facultades se limitan a proteger y garantizar el derecho a la información pública, el cual, por imperativo constitucional (tanto federal como local) debe promoverse por las autoridades del Estado y de sus Municipios."

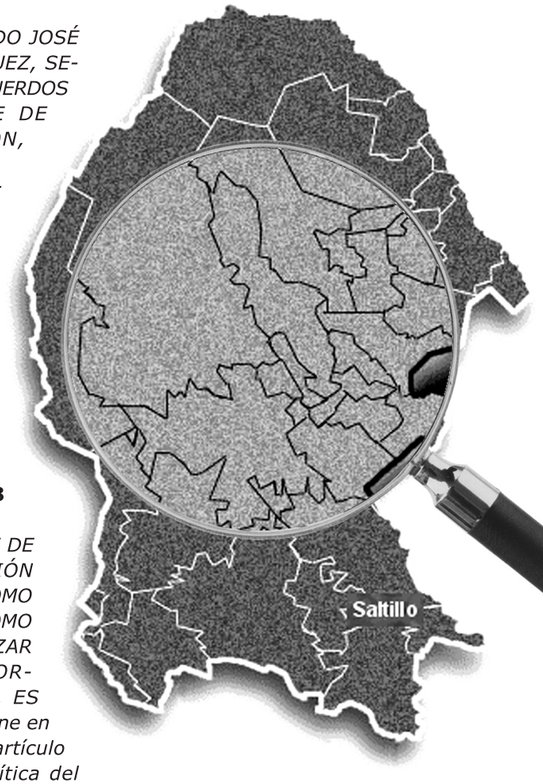
"Controversia constitucional 61/2005.- Actor: Municipio de Torreón, Estado de Coahuila.- 24 de enero de 2008.- Unanimidad de diez votos. (Ausente: José Ramón Cossío Díaz). Ponente: José de Jesús Gudiño Pelayo.- Secretaria: Carmina Cortés Rodríguez.

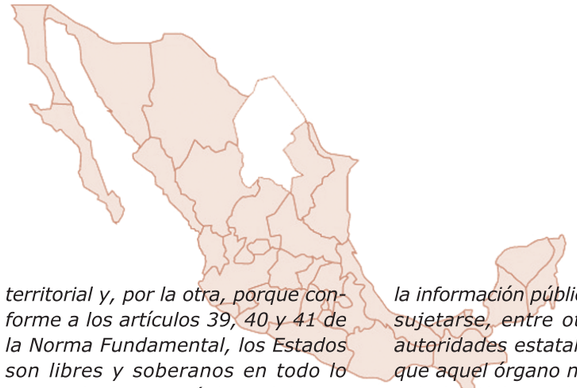
EL CIUDADANO LICENCIADO JOSÉ JAVIER AGUILAR DOMÍNGUEZ, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, C E R T I F I C A:

midad con lo dispuesto por el Tribunal Pleno en su sesión privada de quince de enero de dos mil siete, se aprobó hoy, con el número 58/2008, la tesis jurisprudencial que antecede. México, Distrito Federal, a doce de mayo de dos mil ocho."

TESIS JURISPRUDENCIAL Núm. 59/2008 (PLENO)

"INSTITUTO COAHUILENSE DE ACCESO A LA INFORMACIÓN PÚBLICA. SU CREACIÓN COMO ÓRGANO PÚBLICO AUTÓNOMO ENCARGADO DE GARANTIZAR EL DERECHO A LA INFORMACIÓN EN LA ENTIDAD, ES CONSTITUCIONAL. Si se tiene en cuenta que acorde con el artículo 7o. de la Constitución Política del Estado de Coahuila, el órgano reformador de la Constitución Local erige al Instituto Coahuilense de Acceso a la Información Pública como un organismo público autónomo con personalidad jurídica y patrimonio propio, es indudable que su creación, como órgano garante del derecho a la información en la entidad, no viola disposición alguna de la Constitución Política de los Estados Unidos Mexicanos. Ello es así, ya que, por una parte, el artículo 6o. de la Ley Suprema otorga implícitamente a cada una de las entidades federativas la facultad de regular el derecho a la información y, por ende, establecer las estructuras necesarias para el adecuado desarrollo de la garantía de ese derecho en el ámbito de su esfera





territorial y, por la otra, porque conforme a los artículos 39, 40 y 41 de la Norma Fundamental, los Estados son libres y soberanos en todo lo concerniente a su régimen interno; de ahí que es válido que el órgano reformador de la Constitución de Coahuila, en uso de sus facultades, haya creado un órgano garante del derecho de información."

"Controversia constitucional 61/2005.- Actor: Municipio de Torreón, Estado de Coahuila.- 24 de enero de 2008.- Unanimidad de diez votos. (Ausente: José Ramón Cossío Díaz).- Ponente: José de Jesús Gudiño Pelayo.- Secretaria: Carmina Cortés Rodríguez.
EL CIUDADANO LICENCIADO JOSÉ JAVIER AGUILAR DOMÍNGUEZ, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, C E R T I F I C A: De conformidad con lo dispuesto por el Tribunal Pleno en su sesión privada de quince de enero de dos mil siete, se aprobó hoy, con el número 59/2008, la tesis jurisprudencial que antecede. México, Distrito Federal, a doce de mayo de dos mil ocho."

TESIS JURISPRUDENCIAL Núm. 60/2008 (PLENO)
"INSTITUTO COAHUILENSE DE ACCESO A LA INFORMACIÓN PÚBLICA. NO CONSTITUYE UNA AUTORIDAD INTERMEDIA DE LAS PROHIBIDAS POR EL ARTÍCULO 115, FRACCIÓN I, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Si se atiende a que en términos del artículo 7o. de la Constitución Política del Estado de Coahuila, el referido Instituto es la única autoridad competente en materia de acceso a la información pública, y a ella deben sujetarse, entre otros, las propias autoridades estatales, es indudable que aquel órgano no constituye una autoridad intermedia de las prohibidas por el artículo 115, fracción I, de la Constitución. Lo anterior es así porque, en primer lugar, la comunicación sólo es dable entre el aludido Instituto y el Municipio, sin que intervengan otros órganos de la entidad federativa; en segundo lugar, porque con las facultades del Instituto mencionado, consistentes en promover la cultura de transparencia y el derecho a la información, así como vigilar el cumplimiento de la ley para salvaguardar y garantizar la observancia del derecho a la información, no se lesiona la autonomía municipal, suplantando o mediatizando sus facultades constitucionales ni se invade su esfera competencial, ya que las facultades de dicho Instituto no están conferidas al gobierno municipal; y en tercer lugar, porque la facultad reglamentaria del Municipio no se ve obstaculizada, pues ésta debe ajustarse a los lineamientos determinados en la legislación estatal de la materia, la cual incluye la normatividad que emita el propio organismo estatal especializado; de ahí que aun cuando por su naturaleza no es un poder propiamente dicho, el señalado Instituto sí forma parte del Estado de Coahuila y guarda un rango similar al de dichos poderes, asumiendo una función específica, por lo que no puede sostenerse que exista alguna interferencia entre el Municipio y el Estado."

"Controversia constitucional 61/2005.- Actor: Municipio de Torreón, Estado de Coahuila.- 24 de enero de 2008.- Unanimidad de diez votos. (Ausente: José Ramón Cossío Díaz).- Ponente: José de Jesús Gudiño Pelayo.- Secretaria: Carmina Cortés Rodríguez.
EL CIUDADANO LICENCIADO JOSÉ JAVIER AGUILAR DOMÍNGUEZ, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, C E R T I F I C A: De conformidad con lo dispuesto por el Tribunal Pleno en su sesión privada de quince de enero de dos mil siete, se aprobó hoy, con el número 60/2008, la tesis jurisprudencial que antecede. México, Distrito Federal, a doce de mayo de dos mil ocho."

3.- Importancia de tales precedentes.

Con estas tesis la Suprema Corte de Justicia de la Nación determina una serie de criterios interpretativos relacionados con el Instituto Coahuilense de Acceso a la Información Pública como organismo constitucional autónomo local.[6] Allí deja en claro que los Estados miembros de la Federación Mexicana son libres y soberanos para regular el derecho a la información y crear las instancias que estimen convenientes para garantizar el derecho a la información consagrado en el Artículo 6 de la norma fundamental del País y 7 de la Constitución Local, en uso de las facultades implícitas y residuales que le conceden los Artículos 6, 39, 40, 41, 73 fracción XXI, y 124 de la Constitución Política de los Estados Unidos Mexicanos, por lo que dicho organismo es constitucional.

De igual forma se consideró que los órganos constitucionales autónomos no interfieren en el ejercicio del gobierno municipal, ya que el ICAI es un órgano dotado de atribuciones constitucionales y legales para garantizar el derecho de acceso a la información al interior del Estado. Los municipios deben estar sujetos a la normatividad estatal creada para tal efecto, por lo que el Instituto no irrumpe las atribuciones con las que cuentan dichos municipios sino que se limita la protección del derecho a la información consagrado en la constitución.

Es de señalarse que el ICAI no es una autoridad intermedia de las prohibidas por el artículo 115 fracción I de la Constitución Política de los Estados Unidos Mexicanos, como señaló el Ayuntamiento de Torreón, Coahuila en su demanda de controversia constitucional[7] y es la única autoridad estatal competente en materia de acceso a la información. En sus facultades y/o atribuciones no lesiona ni vulnera la autonomía municipal, ni interfiere en las facultades que constitucionalmente tiene asignadas, por lo que dicho órgano constitucional autónomo forma parte del Estado de Coahuila y guarda un rango similar al de los otros poderes constituidos.[8] Cumple asi una función que el constituyente permanente local estimó indispensable confiar a este tipo de órganos. Acertadamente Manuel García Pelayo[9] señaló sus características que posteriormente la Suprema Corte de Justicia de la Nación retomó en su interpretación jurisprudencial para poder identificarlas.

Por último, el intérprete supremo de la norma fundamental del país, deja en claro que el Instituto Coahuilense de Acceso a la Información, garante del acceso a la información en el Estado, no invade la esfera competencial municipal, ya que las facultades que le fueron asignadas a dicho órgano constitucional autónomo, no están reservadas a los municipios en el Artículo 115 constitucional. Atendiendo al sistema de distribución de competencias de nuestro sistema federal que ha interpretado la SCJN, prevista en los artículos 39, 73, 115 y 124 del ordenamiento, en donde se advierte que es competencia de los congresos locales regular lo relativo al derecho a la información, creando las instancias que se consideran convenientes para dicho efecto. Los municipios deben ceñirse a la norma estatal, por lo que no es válido que el municipio, so pretexto de su facultad reglamentaria prevista en el 115, emita un ordenamiento que pretenda regular dicho derecho fundamental contraviniendo dichas disposiciones constitucionales.[10]

4.- Conclusión.

En síntesis, podemos concluir que la Jurisprudencia emitida por la Suprema Corte de Justicia de la Nación es sumamente relevante para el derecho a la información en México, porque deja en claro aspectos que hasta antes de la reforma al Artículo Sexto Constitucional de 2007, eran objeto de debate o discusión en nuestro sistema constitucional mexicano.

De igual forma, con dichos criterios, la Corte deja en claro que los ayuntamientos no están facultados para crear instancias al interior para garantizar el derecho de acceso a la información, sino que, en todo caso, esto corresponde al Estado a través de la ley que se emita para tal efecto. Incluso dichos criterios son congruentes hoy en día con la reforma constitucional citada, ya que no in-

cluye que los municipios puedan emitir reglamentación en dicha materia, por lo que deberán ajustarse a las normas estatales.

En ese sentido, los denominados órganos constitucionales autónomos, son necesarios y fundamentales en los Estados Constitucionales de Derecho, ya que desempeñan una función esencial y necesaria en el Estado como en el presente lo hace el Instituto Coahuilense de Acceso a la Información Pública. Éste tiene la obligación constitucional de garantizar el derecho a la información y la protección de los datos personales, fundamentalmente.

Por último, el intérprete supremo de la norma fundamental del país, deja en claro que el Instituto Coahuilense de Acceso a la Información, garante del acceso a la información en el Estado, no invade la esfera competencial municipal.

[1] En julio de 2007 se publica en el *Diario Oficial de la Federación* la reforma constitucional en materia de acceso a la información, añadiendo un segundo párrafo y siete fracciones al mencionado Artículo 6. A saber: "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. 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."
"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."
"III. 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."
"IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión."
"V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos."
"VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales."
"VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes."
[2] Se pueden citar como ejemplos que el Reglamento establecía el plazo de veinte días hábiles para contestar la solicitud de información, mientras que la Ley señalaba díez. Lo mismo puede decirse los medios de impugnación ya que el Reglamento establecía el de revisión competencia del Instituto Municipal de Transparencia, mientras que la ley actual señala los recursos de reconsideración y de protección de acceso a la información como competencia del superior jerárquico de la entidad pública y del Instituto Coahuilense de Acceso a la Información Pública.
[3] Cabe destacar que en esta fecha aun no era reformada la Constitución Federal en el artículo sexto agregándole el segundo párrafo y las siete fracciones.
[4] Ibidem.
[5] http://www.scjn.gob.mx/Portal SCJN/ActividadJur/Pleno/TesisJurisprudenciales/
[6] Véase Órganos Constitucionales Autónomos: sus características (SJF,9, XXVII, febrero 2008, p. 1871).
[7] También el Ayuntamiento de Torreón, Coahuila argumentaba en su demanda de controversia constitucional 62/05, que el Instituto no era autoridad competente en dicha materia, ya que el citado municipio consideraba que podía crear un organismo desconcentrado municipal para garantizar el derecho fundamental a la información y vía reglamento establecer las condiciones, requisitos, instancias, procedimientos, plazos de ese mismo derecho sin sujetarse a la normatividad estatal en la materia.
[8] Véase exposición de motivos de la iniciativa de la *Ley del Instituto Coahuilense de Acceso a la Información Pública* publicada en el *Periódico Oficial del Estado* el 04 de noviembre del año 2003.
[9] Carbonell Miguel, *Elementos de Derecho Constitucional*, pág 103.
[10] Cfr. Controversia Constitucional. distribución de competencias entre la Federación, las Entidades Federativas y los Municipios (SJF,9, VIII, Diciembre 1998, p. 788).

El Derecho Fundamental a la **Protección de Datos Personales.** Pasado, Presente y Futuro

Lourdes Hernández Crespo*

"El respeto a la esfera privada es el indicador del grado de tolerancia de una sociedad"
Locke

La intimidad y la confidencialidad que demanda la persona, por su misma naturaleza, penetra en un buen número de aspectos de la vida de cada individuo. La intimidad la percibimos como un derecho inherente a la persona, que no debe conquistarlo para poseerlo, ni se pierde por desconocerlo. Este derecho, que en muchas Constituciones como la nuestra tiene rango de derecho fundamental, tiene sus raíces en el derecho al respeto y la libertad de la persona, que se encuentra en la base de todo tipo de convivencia y de relaciones humanas.

Señala José Luis Piñar Mañas[1] que *"debido al enorme desarrollo de las autopistas de la información en los últimos años vivimos en un mundo de transmisiones de datos continuas, tanto entre entidades nacionales como internacionales. Es por ello por lo que en las últimas décadas ha surgido un gran interés, tanto en el ámbito internacional como en el puramente doméstico, por la regulación de la protección de los datos personales, con el fin de proteger nuestra intimidad frente los abusos que el tratamiento de éstos puede ocasionar".*

Así, el Artículo 18.4 de la Constitución Española establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Como señala Mónica Arenas Ramiro,[2] *"La Constitución española no reconoce de forma expresa un derecho fundamental a la protección de datos personales, pero contiene un mandato dirigido al legislador para que regule el uso de la informática y garantice los derechos de las personas, a partir del cual el Tribunal Constitucional ha reconocido la existencia de este derecho, afirmando que en su finalidad, objeto y contenido, es diferente al derecho a la intimidad"*.

Hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se desvanecieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona. El segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espa-

* • Jefe del Servicio de Gestión y Apoyo a la Inspección de la Agencia de Protección de Datos de la Comunidad de Madrid.

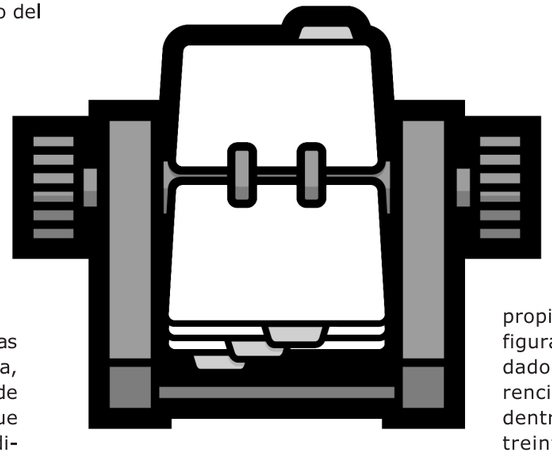
"la Constitución española no reconoce de forma expresa un derecho fundamental a la protección de datos personales, pero contiene un mandato dirigido al legislador para que regule el uso de la informática y garantice los derechos de las personas".

En España, el cambio hacia la consideración del Derecho a la protección de datos como un verdadero Derecho autónomo e independiente viene de la mano de dos importantísimas sentencias del Tribunal Constitucional: las números 290 y 292 de 2000.

cio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado «dinero plástico», sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los qué él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor; una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas.



La fijación de esa nueva frontera debe ser el objetivo de los legisladores y al cumplimiento de este objetivo deberían responder los desarrollos normativos presentes y futuros.

En España, el cambio hacia la consideración del derecho a la protección de datos como un verdadero derecho autónomo e independiente viene de la mano de dos importantísimas sentencias del Tribunal Constitucional: las números 290 y 292 de 2000, ambas de 30 de noviembre. La primera ratifica la constitucionalidad de la existencia de la Agencia Española de Protección de Datos, con competencias en todo el territorio nacional, en cuanto garante de un Derecho fundamental que debe tener un contenido homogéneo para todas las personas (físicas).[3] La segunda consolida una evolución jurisprudencial constitucional que ha ido configurando el derecho a la protección de datos, desde el reconocimiento del derecho a la intimidad y privacidad, pasando por el llamado derecho a la autodeterminación informática o informativa.[4]

Por otro lado, y a diferencia de lo que sucede en el caso de otros derechos fundamentales, de reconocimiento universal, el derecho fundamental de las personas a la protección de sus datos de carácter personal reviste dos características que prácticamente le son propias: es un derecho de configuración sumamente reciente, dado que sólo cabe hacer referencia con propiedad al mismo dentro de los últimos treinta o treinta y cinco años, y es un derecho cuya configuración se ha ido produciendo con el paso del tiempo, dentro de ese lapso al que acabamos de referirnos, de forma que sólo ha alcanzado el status de auténtico derecho fundamental en los últimos años.

A ello ha contribuido esencialmente la regulación de este derecho en los distintos Estados y, en aún mayor medida, la adopción de diversos instrumentos internacionales, con distinto valor normativo y adoptados con una finalidad muy diversa, que han venido a desarrollar los principios esenciales que configuran lo que hoy puede universalmente ser conocido como derecho fundamental a la protección de datos de carácter personal.

Entre estos instrumentos es obligado citar los siguientes:

* La Recomendación de la OCDE sobre circulación internacional de datos personales para la protección de la intimidad, conocida como *Las Directrices de la OCDE*, de septiembre de 1980.
* El Convenio del Consejo de Europa, de enero de 1981. Este texto fue además aplaudido por la Recomendación 81/679/CEE de la Comisión Europea, en la que se insta a los Estados Miembros, a su ratificación. España lo ratificó mediante Instrumento de 27 de enero de 1984.
* La Resolución 45/95 de la Asamblea General de las Naciones Unidas, sobre Principios rectores para la reglamentación de los ficheros computarizados de datos personales, conocida como *"Directrices de Protección de Datos de Naciones Unidas"*, que tuvo la virtud de ser el primer texto mundial en esta materia.
* La Directiva 95/46/CE, del Parlamento Europeo y del Consejo, 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.

A lo largo de estos textos se han ido estableciendo una serie de principios básicos que han de regir el tratamiento de los datos personales y presidir las legislaciones nacionales correspondientes, y que hoy en día conforman el contenido del derecho fundamental a la protección de datos personales, que va mucho más allá del sistema de *Habeas Data* imperante en los países Iberoamericanos.

Estos principios podrían resumirse en los siguientes:

*Principio del Consentimiento informado, con la aceptación de excepciones tasadas exclusivamente.
*El principio de calidad de los datos: proporcionalidad, exactitud, actualización.
*El principio de finalidad.
*El principio de seguridad.
*El principio de Control por parte de una autoridad independiente.

Este sistema ha de traducirse, además, en el reconocimiento de una serie de derechos a favor del titular de los datos, entre los que se ha de incluir, al menos los siguientes:
*El derecho a la información.
*El derecho de acceso, rectificación, cancelación y oposición.
*El derecho a ser indemnizados como consecuencia de los perjuicios que les fueran causados como consecuencia del tratamiento de sus datos.
* El derecho a no verse sometido a una decisión con efectos jurídicos sobre la persona o que le afecte de manera significativa, que se base en tratamientos de datos destinados a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, conducta, etc.

En España, el marco normativo que refleja el sistema de principios básicos al que acabo de referirme y que se encuentran recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, transpone el contenido de la Directiva 1995/46/CE, relativa a la protección de datos personales y a la libre circulación de éstos, y el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la citada Ley.

No voy a detenerme más en el contenido de este derecho, ni tampoco en la importancia evidente de los instrumentos internacionales que he mencionado. Sólo quiero hacer hincapié en la importancia que tienen, sobre todo a los efectos de la armonización de las legislaciones de los distintos Estados, incluidos los Iberoamericanos, como premisa básica para el establecimiento de un marco armonizado de protección de datos a nivel global que permita el establecimiento de un marco homogéneo de regulación del derecho la protección de datos, bien mediante la adopción de instrumentos supranacionales de carácter vinculante, bien mediante la adopción de Leyes nacionales que consagren el contenido esencial del derecho a la protección de datos personales.

[1] "El derecho fundamental a la protección de datos personales" en *Protección de datos de carácter personal en Iberoamérica*. Ed Tirant lo Blanch, Valencia, 2005.
[2] *El derecho fundamental a la protección de datos personales en Europa*. Ed. Tirant Lo Blanch. Valencia, 2006.
[3] España es un Estado descentralizado basado en el modelo de las llamadas Comunidades Autónomas, intermedio entre el estado regional y el federal. Quizá sea necesario recordar la doctrina del Tribunal Constitucional en relación con el reparto competencial entre Estado y Comunidades Autónomas en materia de protección de datos. El Tribunal, en la citada Sentencia 290/2000, centra su análisis en el estudio de las normas referidas a la existencia o inexistencia de una infracción del reparto competencial establecido en nuestra Constitución. En cuanto a este análisis, su fundamento jurídico 7 considera necesario "que el examen de la presente disputa competencial se lleve a cabo partiendo de dos presupuestos, a saber: el contenido del Derecho fundamental a la protección de datos personales y, en segundo término, los rasgos generales que caracterizan a la Agencia de Protección de Datos, dado que la función general de este órgano es la de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación", como se expresaba en el primer inciso del apartado a) del art. 36 LORTAD.
[4] E. Guichot, *Datos personales y Administración Pública*, Thomson-Civitas, Madrid, 2005, págs. 68 y ss.

Protección de la **Información Médica**

Javier Rodríguez Suárez*

Juramento Hipocrático

"Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no deba ser público, manteniendo estas cosas de manera que no se pueda hablar de ellas."

A través del tiempo, lo que era un asunto casi exclusivo del médico, se ha convertido en una situación compartida de derechos, obligaciones y responsabilidades. Este asunto, el de la información médica, ha tomado cada vez mayor relevancia a la luz de los derechos humanos, de la transparencia, de la responsabilidad legal y de los avances tecnológicos. La información médica o de salud, es aquella que se refiere al estado o condición física o mental de un individuo, referida a la historia o expediente clínico, que incluye aspectos de diagnóstico, de pronóstico y de tratamiento y que es obtenida por personal relacionado con la salud tanto en forma directa del paciente como a través de sus familiares. Incluye además, el nombre, dirección, teléfono, hábitos, estado emocional, estado socioeconómico, ocupación y otra características personales. De esta manera, todas las instituciones de salud de diferentes áreas, sean públicas o privadas, así como el personal de salud, incluyendo los de rehabilitación, quiroprácticos, terapistas de lenguaje, trabajadoras sociales, etc. y otras relacionadas que obtengan y manejen información de salud de pacientes, están obligados a respetar la confidencialidad de la misma.

Un aspecto de la mayor relevancia, es que generalmente la inquietud sobre la confidencialidad de la información se limita al expediente clínico, dejándose a un lado aquella que se vierte en documentos de investigación clínica y que también crean compromisos tanto de las instituciones de salud como de los pacientes y laboratorios farmacéuticos. Adicionalmente, los servicios que ofrecen los seguros médicos, plantean retos en el manejo adecuado de la información, así como en otros aspectos no menos relevantes que todavía no reciben la debida atención.

Por otra parte, la propiedad intelectual tanto del documento clínico en su totalidad como de sus contenidos, todavía no ha sido explicitado lo suficiente, existiendo todavía vacíos éticos y legales que deben resolverse.

El expediente clínico convencional y el electrónico

Aún cuando los pacientes deberían sentirse libres para dar información completa a sus médicos, con frecuencia manifiestan dudas en cuanto a la confidencialidad de la misma, lo cual puede afectar en gran medida la integración del expediente. Los contenidos del documento deben ser adecuados, lo que significa que deben incluir datos suficientes y significativos, de tal manera que cualquier lector autorizado pueda entender la situación clínica, las conclusiones diagnósticas y el tratamiento instituido. Esta integración, es la mejor respuesta para resolver inquietudes y problemas tanto médicos como legales. Aún cuando existe gran controversia en cuanto a la propiedad del expediente clínico, resulta obvio que la información contenida en él es del paciente, y éste tiene derecho a exigir su protección, así como obtener una copia tanto del expediente o de los expedientes originales como de las modificaciones que se vayan dando a través del tiempo conforme va recibiendo atención con diferentes médicos. Sin embargo, la serie de consideraciones diagnósticas, de tratamiento y de pronóstico que ha hecho el médico, así como opiniones, comentarios, explicación del por qué de las decisiones y justificaciones, así como las interpretaciones de los datos, son manejados de hecho como de su propiedad. Toda esta información, sirve para la comunicación interprofesional a través de publicaciones en revistas científicas, conferencias, reuniones científicas etc., así como para evaluación de la calidad de la atención médica. De cualquier manera el médico tiene la obligación de proteger los datos del paciente pero también tiene el derecho de proteger su propia información. Esto último es de la máxima importancia a la luz de las tendencias internacionales para evitar en la medida de lo posible la comisión de eventos adversos que dañan a los pacientes. Como parte de las acciones orientadas a contender con este problema, se promueve a través de la Organización Mundial de la Salud, el registro voluntario de incidentes en los que puede haber o no daño a los enfermos, esfuerzo que se ha visto disminuido por el temor del personal de salud de que pueda utilizarse en su contra y que suscite controversia entre la necesidad de reconocer los problemas y la tendencia a la sanción. Dado que la seguridad de los pacientes podría incrementarse significativamente con la identificación de incidentes, debe promoverse su reconocimiento sin sanción, toda vez que dicho reconocimiento se haría de buena fe, con la idea de corregir las fallas de los sistemas de atención a la salud.

> ***"Un aspecto de la mayor relevancia, es que generalmente la inquietud sobre la confidencialidad de la información se limita al expediente clínico, dejándose a un lado aquella que se vierte en documentos de investigación clínica y que también crean compromisos tanto de las instituciones de salud como de los pacientes y laboratorios farmacéuticos."***

Por otro lado, el uso de las computadoras en medicina, crea una obligación moral adicional y requiere además de estándares específicos de operación que refuercen la seguridad de la información. Sin embargo, junto con las medidas para incrementarla, siempre van otras ilegales orientadas a tener acceso a la misma. Por ello, la información electrónica y la documental convencional deben protegerse con legislaciones apropiadas, educación intensiva y la creación de una cultura en este renglón tanto de los prestadores de los servicios como de los pacientes. Esta confidencialidad implica que no puede existir una apertura de la información deliberada sin permiso explícito del paciente o de su familia, así como del médico tratante. En el caso de los expedientes electrónicos que permiten compartir información a distancia, la responsabilidad no desaparece, sólo cambia la modalidad de transmisión.

En este sentido, las organizaciones de salud están tendiendo a unirse a través de infraestructura para compartir información a través de redes de telecomunicación. Esto permitirá la transferencia de datos de una institución a otra para coordinar servicios de atención médica, permitiendo además la integración longitudinal de los expedientes clínicos desde diferentes instituciones y por distintos médicos. De esta manera, la información no será generada por un solo médico o por una sola institución como tampoco será sencillo asignar la propiedad a alguien en particular. La introducción reciente de tarjetas inteligentes que puedan contener información clínica, representa otro reto en cuanto a la confidencialidad de la información y entra en el rubro de la información computarizada y deberá regirse por los mismos principios aún cuando sea información fraccionada. Con todas estas innovaciones, la legislación tendrá que ser más comprensiva, tratando además de mantenerse al día con las innovaciones tecnológicas.

Investigación clínica y protección de la información

Los aspectos de investigación han sido obviados prácticamente en forma

* •Director General de Difusión e Investigación de la Comisión Nacional de Arbitraje Médico.
•Médico Cirujano por la Facultad de Medicina de la UNAM.
•Miembro del Comité Editorial de la Facultad de Medicina, así como de la Revista del Hospital General "Dr. Manuel Gea González".

total. La convocatoria para ser candidatos a protocolos clínicos para probar nuevos medicamentos, sólo está sujeta a comités de ética locales que pueden o no sancionar los aspectos relacionados con la confidencialidad. Sin embargo, no existe transparencia en estos aspectos en cuanto a la forma como se maneja tanto la convocatoria y la selección de los sujetos experimentales, así como la forma en que se manejará la información. Se plantea además el problema de la propiedad de la información generada como consecuencia de los resultados de las investigaciones, además de los contenidos del propio expediente clínico. Por otra parte, para que un laboratorio pueda obtener el permiso de las instancias de salud encargadas de autorizar el uso de fármacos, estos deben haber pasado por su aplicación clínica en pacientes. En estos casos, a veces los propios médicos que atienden a los pacientes son los que realizan estos trabajos de investigación y se abre otra puerta para descubrir los datos de los pacientes, motivo por el cual éstos deben autorizar el uso de la información contenida en los mismos para un propósito diferente al clínico y bajo las mismas condiciones de confidencialidad. En estas condiciones, la autorización puede ser restringida para un uso temporal o permanente de información relacionada con su persona, e incluso debe quedar establecido que pueda ser revocada en cualquier momento si así lo considera conveniente el sujeto que haya aceptado inicialmente participar en un protocolo. En estos casos, deberá también haber un consentimiento informado, al igual que existe para efectos de la toma de decisión de los pacientes con respecto a estudios invasivos o de tratamientos médicos y quirúrgicos. En dicho consentimiento deberá estipularse exactamente en qué consiste el protocolo y a qué se compromete el sujeto a participar, no debiéndose extender el propósito en ningún otro sentido y manteniéndose además la protección de la información contenida en este documento.

Aseguradoras médicas y la protección de la información

Otro aspecto importante es el que corresponde al uso de la información por compañías aseguradoras. El acceso a la información contractual aparentemente existe, pero es opacado por su número así como por su complejidad e inclinación a la ambigüedad, quedando el usuario a merced a las decisiones finales de las empresas. En estos casos, cuando ya existe un expediente que utilizan los seguros, es difícil pensar que la información no será compartida para otros fines diferentes para el cual se obtuvo. Aquí son muy necesarias las legislaciones para regular el derecho de las empresas a intercambiar información de los expedientes con otras compañías aseguradoras.

Por otra parte, el compartir la información sobre los diferentes aspectos de la salud de un individuo, puede condicionar diferentes problemas que afecten sus posibilidades para conseguir trabajo, oportunidades de educación, crédito, así como satisfacer otras necesidades de diferente índole. Tampoco puede descartarse la tentación de compartirla entre compañías aseguradoras después de que exista alguna reclamación por parte de los pacientes y en la que las empresas puedan sentirse agredidas económicamente, marcando como un usuario indeseable a ese paciente.

De acuerdo a las consideraciones anteriores, es necesario encontrar puntos bien definidos de equilibrio entre el derecho a la información y la protección de la misma, ya que la ponderación del peso hacia uno u otro lado depende muchas veces de cada caso en particular, siendo criterios variables los que definen la razón. Existen todavía grandes vacíos éticos y legales que deben ser atendidos, con el fin de proteger al máximo la información que se genera tanto en el proceso de la atención médica como en el de la investigación clínica.

La Vida de los Otros

José Manuel Gil Navarro*

La premisa básica para la reflexión en torno a la relación que tiene el acceso a la información y la protección de datos personales es aquella que señala que en los regímenes no democráticos los ciudadanos saben poco de gobierno y el gobierno mucho de sus ciudadanos y que en contraparte en aquellos regímenes claramente democráticos se modifica la ecuación; El gobierno sabe poco, o lo estrictamente necesario de sus ciudadanos mientras que los ciudadanos conocen todo o casi todo del gobierno, salvo lo necesariamente debe permanecer lejano a la publicidad. La cinta alemana *"La vida de los otros" ('Das Leben der Anderen')* ejemplifica perfectamente bien la ecuación de los regímenes no democráticos. Esta cinta tiene la estructura de un thriller tradicional. Suspenso, héroes, misterio y sorpresas. Pero detrás del misterio de los espías, se expone una gran historia humana. La película alemana que le ganó en buena lid el Óscar a la mejor película extranjera a la cinta hispano-mexicana "El Laberinto del Fauno" se sitúa en 1984 en la República Democrática Alemana. Me parece que situarla en 1984 tiene un doble sentido. En el 84 faltan cinco años para la caída del Muro pero no hay signos todavía del debilitamiento del régimen, pero también hace una clara alusión a la pesadilla totalitaria que George Orwell predijo en 1984. La atmósfera de no era sólo sofocante, era carcelaria en el sentido anticipado por el propio Orwell. La policía estatal, *"la STASI",* era el Big Brother omnipotente, omnisciente y sobre todo omnipresente, que espiaba la vida de los otros, y los otros eran en realidad todos, incluidos los propios espías. En aquel lugar cercado hacia afuera y cableado hacia adentro, no existía espacio posible para la intimidad. Solo por poner algunos datos, las fuentes que la propia autoridad consideraba más importantes eran los colaboradores no oficiales. Según los documentos internos, en 1988, el último año de Alemania Oriental, el Ministerio de Seguridad del Estado tenía más de 170 mil colaboradores no oficiales. De éstos,

* • Consejero Presidente del Instituto Coahuilense de Acceso a la Información Pública.
• Licenciado en Derecho por la Universidad Iberoamericana Laguna.
• Catedrático de la Facultad de Jurisprudencia de la UA de C.

...en los regímenes no democráticos los ciudadanos saben poco de gobierno y el gobierno mucho de sus ciudadanos y que en contraparte en aquellos regímenes claramente democráticos se modifica la ecuación; El gobierno sabe poco, o lo estrictamente necesario de sus ciudadanos mientras que los ciudadanos conocen todo o casi todo del gobierno...

La cinta alemana "La vida de los otros" ('Das Leben der Anderen') ejemplifica perfectamente bien la ecuación de los regímenes no democráticos. Esta cinta tiene la estructura de un thriller tradicional. Suspenso, héroes, misterio y sorpresas. Pero detrás del misterio de los espías, se expone una gran historia humana. La película alemana que le ganó en buena lid el Óscar a la mejor película extranjera a la cinta hispano-mexicana "El Laberinto del Fauno" se sitúa en 1984.

unos 110 mil eran informadores corrientes, mientras que los otros estaban relacionados con tareas 'conspiradoras' y solo sólo figuraban como contactos fiables. El Ministerio propiamente dicho tenía al menos cinco mil oficiales en la sección de los servicios de espionaje. Otro dato sorprendente es que según el primer rector occidental de la Universidad de Humboldt "uno de cada seis profesores y uno de cada diez empleados de la universidad habían trabajado para la policía secreta del antiguo régimen, o cooperado de algún modo con ella." En la relación entre espías y espiados se realiza la trama de esta extraordinaria cinta.

Weisler (interpretado por el ya fallecido Ulrich Muehe) es un especialista en el espionaje y descubrimiento de acciones "ilícitas" de los ciudadanos contra el régimen. El es capaz de detectar cualquier síntoma de rebeldía, utiliza todos los recursos para observar los movimientos de los sospechosos, los presiona y en el momento propicio los detiene e interroga con total eficacia, porque conoce sus puntos débiles. Meticuloso en extremo y con un estricto sentido del deber, convencido de las bondades del régimen, Weisler es un hombre solitario y dedicado en vida al trabajo, asiste a una función de teatro que va a dar origen a toda la trama. La mirada del espía cae sobre el joven autor de la obra representada, como potencial sospechoso, el escritor Georg Dreyman el cual es considerado por el Ministerio de Cultura como un artista oficial, incluso como uno de los mejores, como lo evidencia Anton Grubitz jefe de Weisler que al referirse a él señala que es *"Nuestro único escritor no subversivo a quien también leen en el extranjero."*. Weisler también es sorprendido por la belleza de la primera actriz, la pareja de Dreyman. Christa-Marie y su novio, son una pareja enamorada y feliz, a pesar del constante miedo a decir o hacer algo que ante los ojos y oídos del régimen fuera subversivo. Forman parte de un grupo de amigos intelectuales que, como ellos, trabajan y disfrutan de los relativos beneficios que les da su condición de artistas. La relación de la pareja tiene algunos aspectos negativos como la adicción de ella a ciertos fármacos y la condena del gobierno al trabajo de un querido amigo, mentor del grupo, Albert Jerzca. Las sospechas de Weisler resultan infundadas, los artistas no traman acciones disidentes, ni tienen ningún plan subversivo. Por desgracia, la belleza de Christa-Marie ha impactado al Ministro de Cultura del Partido, el cual le sugiere a Grubitz la necesidad de hallar cargos contra Dreyman para que la pareja se disuelva. Con la promesa de beneficios para su carrera y su economía, el sujeto comienza a maquinar la forma de lograrlo. Asigna la vigilancia a Weisler, quien instala toda clase de micrófonos en el departamento de los artistas y un centro de operaciones en piso de arriba del mismo edificio, donde escuchará y dará cuenta de la vida cotidiana de la pareja. El inicio del espionaje se da en una fiesta organizada en el departamento para celebrar el cumpleaños de Dreyman. Asisten todos los amigos de la pareja, llevando consigo afecto, camaradería, preocupaciones y modestos obsequios. Algunos comentarios políticos quedan registrados por el vigilante, pero en su cerebro dejan una impresión más poderosa cosas que hasta ese momento él no conocía, como la compañía, palabras amables, obsequios como un libro y una partitura musical de parte de Jerzca, los cuales jugaran un papel importante en la trama de la cinta, ya que Weisler en una de sus intromisiones a la casa de Dreyman roba el libro obsequiado que era de Berthold Brecht, autor para quien la libertad de pensamiento no puede ser contenida por ninguna clase de represión, lo cual empieza a cambiar la percepción de Weisler frente al régimen, aunado a que algo ha comenzado a hacer crisis en él, ya que se ha dado cuenta que el espionaje obedece al interés del Ministro de Cultura por la mujer de Dreyman no por su actividad política y que Grubitz no lo hace por la protección del régimen, sino por un ventaja personal que le dejara quedar bien con el Ministro. En contraparte descubre también la vida de los otros; es decir, la forma como sus espiados piensan y viven.

La película transcurre en un clima de tensión que va aumentando a medida que suceden eventos terribles para los personajes: la mujer de Dreyman es prácticamente violada por el jefe político, quien la amenaza con quitarles el trabajo a ella y a su amante, además de limitarle su acceso a los fármacos a los cuales es adicta si no accede a sus exigencias; Dreyman descubre la relación de Christa-Marie con el Ministro de Cultura, pero sobretodo un evento que marca el punto de inflexión en la cinta es cuando Jerzca, se suicida, incapaz de soportar el ostracismo al que el régimen lo condena. La tristeza que se presenta por la muerte del mentor y del amigo, da origen a una de las mejores escenas de la cinta, cuando Dreyman interpreta al piano la "Sonata para un Buen Hombre", cuya partitura fue el regalo de cumpleaños del difunto. Mientras el espía escucha, absolutamente conmovido por la situación y por la belleza de la música, Dreyman le comenta a Christa-Marie que *"Quien haya oído realmente esta partitura, no puede ser un mala persona"* y además platican una anécdota de Lenin quien, según propia confesión, experimentó tal emoción y conmoción al escuchar la Apassionata de Beethoven, que tuvo que dejar de hacerlo, pues de otro modo le hubiera sido imposible concluir la revolución.

A partir de este momento Dreyman es invitado a escribir un artículo en la revista de Alemania Occidental, Der Spiegel. El tema que el escritor decide abordar es el hecho de que los suicidios no son más contabilizados en la República Democrática Alemana. El hecho de que los ciudadanos no puedan saber algo tan simple como el número de los suicidios que se presentan en el país, pero en cambio el estado sepa tanto de los que los ciudadanos hacen como sus actividades, sus filias y fobias, ejemplifica bien el hecho de que en los regímenes totalitarios los gobiernos no dan acceso a la información pública y a cambio invaden los espacios más íntimos de los ciudadanos.

La redacción del artículo se vuelve muy compleja ya que necesitan conseguir una máquina de escribir que no esté registrada la cual pasan por la frontera y la tinta tiene tinta roja, y el artículo después de un gran periplo cruza la frontera para ser publicad. Weisler es testigo de todos estos hechos, pero por lo fascinado que se encuentra con la vida de sus espiados guarda silencio; los informes llegan alterados a las oficinas de la STASI, además Weisler contrasta los valores de la pareja con la mezquindad de sus jefes políticos y agradecido por lo que sin querer le han revelado, decide no denunciarlos. El artículo se publica y tanto Grubitz como el Ministro de Cultura sospechan de la protección del espía a la pareja, pero no encuentra pruebas.

Para hacer más dramática la cinta, la mujer de Dreyman, después de ser obligada a declarar en contra de su marido, muere atropellada. (La denuncia por parte de un hombre cercano o de la familias es una situación que se presentó con mucha

Las violaciones a la intimidad se siguen presentando en nuestro tiempo, y no solo buscan la reproducción del régimen político, sino también la mayor audiencia en los medios de comunicación, o una ventaja comercial frente a los competidores. El reto en las democracias supone, como lo dice Fernando González Escalante, 'hacer que lo público sea transparente y que lo privado esté a salvo de cualquier mirada indiscreta'.

frecuencia según lo han documentado el historiador inglés Timothy Garthon Ash). Weisler termina su carrera de espía en los sótanos del Ministerio, husmeando en la correspondencia ajena, derivado del Boicot de Grubitz y del Ministro de Cultura. Tiempo después, ya con la caída del Muro, se encuentra Dreyman con el ex ministro de Cultura en la sala del teatro donde se expone la obra de Dreyman escribió acerca de su trágica historia con Christa-Marie. Ninguno de los dos puede soportar la melancolía que les produce ver la obra de teatro que años atrás había unido sus vidas. Dreyman no oculta cierto desprecio por el personaje, y el ex jerarca lo observa a su vez con ironía. "¿Yo también fui vigilado?", le pregunta el poeta con ingenuidad. "Por supuesto que sí. Fuiste más vigilado que nadie. Ve y revisa en tu departamento los interruptores. Sabíamos todo de tí, absolutamente todo, incluso las dificultades que tenías para satisfacer a tu bella esposa...". Efectivamente Dreyman va a su departamento revisa y se da cuenta de que está llena de micrófonos y cables. Sorprendido por eso acude a las ex oficinas de la STASI donde descubre dos cosas que lo impactan. Primero que fue denunciado por su ex pareja Christa-Marie y por otra que el responsable de espiarlo el agente HGW XX/7, número oficial de Weisler era quien lo había protegido de caer en manos de la STASI. Dreyman lo busca para agradecérselo. Lo ve siendo Weisler ya un cartero y, en contra de lo que todos queremos y esperamos, no se acerca. Pero a cambio, después de algún tiempo le dedica un libro, "Sonata para un buen hombre", en cual es comprado por Weisler en una librería. Las violaciones a la intimidad se siguen presentando en nuestro tiempo, y no solo buscan la reproducción del régimen político, sino también la mayor audiencia en los medios de comunicación, o una ventaja comercial frente a los competidores. El reto en las democracias supone, como lo dice Fernando González Escalante, "*hacer que lo público sea transparente y que lo privado esté a salvo de cualquier mirada indiscreta*".

Seguridad
y protección de datos en la legislación española

Ricard Martínez Martínez*

1. Una aproximación extrajurídica a la seguridad. 2. El estado de la técnica. 3. Usuarios reticentes: el deber de secreto. 4. Los costes de la seguridad. 5. Seguridad ¿Por qué?

1. Una aproximación extrajurídica a la seguridad.

La aplicación de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (LOPD) ofrece al jurista una oportunidad única de lo que podríamos definir como una aproximación "problemática" a la aplicación del Derecho.[1]

En protección de datos el operador jurídico, sea o no profesional del derecho, se enfrenta a la necesidad de conocer los hechos con todo detalle, de identificar el origen de los datos, el uso que se hace de ellos, las personas o departamentos que tratan los datos, los eventuales destinatarios de la información... En una palabra, no puede aplicarse la norma sin esquematizar previamente el flujo de datos y contar con un mapa de la realidad lo más fidedigno posible. Si se permite la exageración, aquí no sirve la vieja, y a veces mal entendida, técnica de la subsunción cuando ésta se concibe como pura aplicación mecánica de la norma forzando, si hace falta, la realidad de los hechos. Aquí resulta indispensable tener un cabal entendimiento de la realidad material sobre la que se aplica la LOPD y, a la par, un profundo conocimiento del sector jurídico sobre el que se aplica la ley debido al carácter instrumental y/o transversal del derecho fundamental a la protección de datos.

Esta afirmación adquiere mayor valor, si cabe, cuando se refiere a la aplicación de las medidas de seguridad previstas por el *Real Decreto* 1720/2007, de 21 de diciembre, por el que se aprueba el *Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal*, en adelante RDLOPD.[2]

2. El estado de la técnica.

La primera apreciación a la que se enfrentará cualquier profesional que opere con la aplicación de las normas sobre protección de datos ante los problemas de seguridad podría resumirse con una sola palabra: "imposible". Como más adelante se examinará, la primera percepción que se tiene del RDLOPD, como por otra parte ocurre con la propia Ley Orgánica, es una sensación de impotencia. El responsable percibe la seguridad como un conjunto de obligaciones leoninas, exageradas e inalcanzables. Nada más lejos de la realidad. Según la *Ley de Moore* el número de transistores en un chip se duplica cada 18 meses y con ello la capacidad de los sistemas para tratar y almacenar información con un mantenimiento prácticamente constante de los costes de producción y adquisición. En este sentido, cualquier usuario de productos informáticos puede constatar que las generaciones de ordenadores se suceden a un ritmo de 9 a 12 meses. Esta evolución tecnológica debe ser entendida desde una doble perspectiva:

* El aumento de la velocidad y capacidad de proceso, el cada vez mayor espacio para el almacenamiento de información y las prestaciones que nos ofrece la "Galaxia Internet" incrementan el uso de las tecnologías de la información y las comunicaciones y, paralelamente, los riesgos que comportan.

* Ahora bien, los cambios no se producen únicamente en el plano del *hardware*. También evoluciona el *software* tanto en los sistemas operativos como en el conjunto de aplicaciones y gestores de bases de datos relacionados con los tratamientos. Y otro tanto sucede con programas complementarios como antivirus, cortafuegos, gestores de correo electrónico o detectores de *spyware* y/o *malware*.

Por tanto, en muchas ocasiones los problemas no derivarán tanto de la propia naturaleza del tratamiento como del estado de actualización de los equipos y del *software* que los trata. Aquí se constata ciertamente un problema cultural de naturaleza extrajurídica. ¿Realmente es consciente el responsable del fichero de la importancia que para su negocio posee una adecuada inversión en

* • Coordinador de Estudios de la Agencia Española de Protección de Datos.
• Profesor de Derecho Constitucional de la Universitat Oberta de Catalunya, y Dta Protection Officer de la Universitat de Valéncia.
• Autor del libro Tecnologías de la Información, Policía y Constitución.

El deber de secreto no es otra cosa que una manifestación específica y reforzada del secreto profesional que incumbe al personal de cualquier organización respecto de la información a la que accede.

hardware y *software*? Con independencia de la respuesta a esta pregunta, más propia de un estudio sociológico que jurídico, lo cierto es que la mayor parte de exigencias vinculadas a la seguridad resultan resolubles con la mayor parte de productos existentes en el mercado y con la aplicación del más elemental sentido común.

3. Usuarios reticentes: el deber de secreto.

El siguiente elemento a considerar en esta aproximación no estrictamente jurídica a la seguridad tiene mucho que ver con la percepción subjetiva del usuario que vendrá obligado a velar por la seguridad, a diseñar la misma o, simplemente a cumplir con ciertas reglas básicas de conducta.

En este sentido, el usuario concibe las obligaciones legales[3] y el RDLOPD como una obligación adicional "excesiva". Así, desde el responsable del fichero, pasando por los profesionales de la informática al último usuario del sistema viven la seguridad como una pesada carga. Generalmente, debe tenerse en cuenta que no se interiorizan los beneficios que la aplicación de las medidas de seguridad proporciona. No se percibe la seguridad como un conjunto de actuaciones que tenderán a mejorar las condiciones del trabajo, la calidad de la información y, sobre todo, no se alcanza a comprender que la implementación de medidas de seguridad creará un contexto en el que sea posible atribuir la responsabilidad de modo individual.

Sin embargo, desde el punto de vista del usuario de los sistemas de información resulta evidente que la obligación de garantizar la seguridad en la medida en que tiene por objeto garantizar el deber de confidencialidad no es sino una de las manifestaciones del deber de secreto del artículo 10 LOPD[4]. El deber de secreto no es otra cosa que una manifestación específica y reforzada del secreto profesional que incumbe al personal de cualquier organización respecto de la información a la que accede. En tal sentido, en la mayor parte de profesiones existe este deber, si bien en algunas resulta especialmente cualificado, habida cuenta del ejercicio de funciones públicas, del acceso a información sanitaria[5], e incluso de la prestación de servicios de naturaleza religiosa. Aquí, sin embargo, este deber de secreto se acentúa por cuanto su papel se ordena a la protección de un derecho fundamental. Este hecho, la protección de la información personal objeto de tratamiento, justifica por sí solo que cualquier usuario que mantenga relación con un fichero o tratamiento venga vinculado por el deber de secreto. Se trata, por tanto, de un deber que se proyecta respecto de todos los que intervengan en cualquier fase del tratamiento. Ello incluye a todo el personal que materialmente acceda a las aplicaciones o a los resultados derivados de su funcionamiento, e incluso a aquellos que no accedan directamente a la base de datos pero sí materialmente a las explotaciones de datos que a partir de éstas se obtengan.

Por último, una interpretación integrada del deber de secreto con el principio de seguridad induce a considerar que el deber de secreto alcanza a cualquier información cuyo conocimiento por terceros pudiera poner en riesgo el sistema de información. En este sentido, la revelación de un usuario y una contraseña que permita acceder a una aplicación que trata datos no sólo infringiría la seguridad sino también el deber de secreto. Es más, suele existir personal informático cuya tarea no comporta el acceso a datos personales pero la revelación de cuyos conocimientos podría poner en peligro la información contenida en un sistema de información. Del mismo modo, existen usuarios que no acceden al recurso informático pero acceden a datos personales y vienen vinculados por el deber de secreto. Piénsese a titulo de ejemplo en aquellos casos en los que un informe, un etiquetado, o una explotación de datos para ser sometida a un análisis concreto no ha sido protegida o simplemente ha sido puesta a disposición de terceros.

Aún así, el artículo 10 LOPD debe entenderse como un reforzamiento específico del deber de secreto más que como una obligación añadida. En tal sentido, el natural entendimiento de los principios de buena fe y de diligencia profesional comporta de suyo el que cualquier sujeto que tenga algún tipo de relación con datos de carácter personal venga obligado por este deber. En cualquier caso, la particular naturaleza del derecho fundamental a la protección de datos obligaba de algún modo a contemplar dicho deber expresamente.

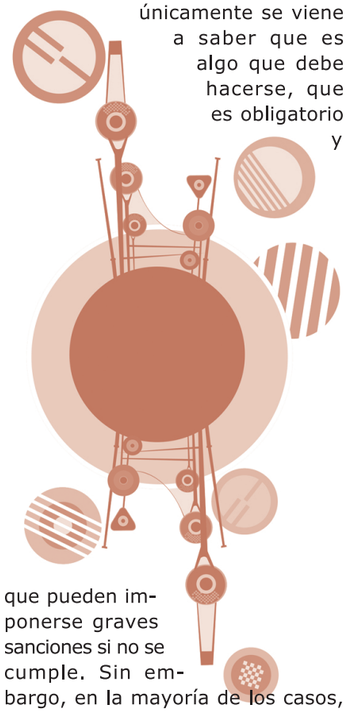
En otro orden de cosas, y por último, debe destacarse que no siempre existe una conciencia en los responsables de alto nivel sobre la prioridad de las necesidades derivadas del cumplimiento normativo. Y, desde una perspectiva centrada en la realidad práctica, resulta fundamental obtener su implicación. Existe un conjunto de valores cuya interiorización resulta estratégica por parte de todos y cada uno de los usuarios relacionados con un sistema de información:

* La información y los sistemas que la soportan constituyen activos valiosos e importantes para la organización. Por tanto, el normal desenvolvimiento de las tareas depende de la seguridad tanto como de otros factores.
* La seguridad permite depositar la suficiente confianza sobre la capacidad de la información y de los sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la organización.
* La seguridad proporciona confianza tanto interna, para los propios gestores, como externa para el cliente o administrado.
* La seguridad es presupuesto para la eficiencia en el manejo de la información y, lógicamente, para la de los procesos decisorios basados en la información personal y en el uso de las tecnologías de la información y las comunicaciones.
* No existe ningún proceso vinculado a la búsqueda de calidad y excelencia que no requiera un adecuado cumplimiento de la LOPD y del RDLOPD.
* La seguridad constituye un presupuesto más para la garantía del derecho fundamental a la protección de datos.

Transmitir este conjunto de valores y hacerlo de un modo positivo puede resultar esencial para una adecuada implementación del RDLOPD.

4. Los costes de la seguridad.

Otro de los elementos disuasorios para una adecuada implementación de la seguridad reside en que las organizaciones, especialmente en el entorno de la pequeña empresa, conciben la seguridad como algo extraordinariamente costoso. Y ello se debe a diversas razones que no siempre les son imputables. En primer lugar, existe un desconocimiento absoluto de las propias medidas de seguridad de modo que únicamente se viene a saber que es algo que debe hacerse, que es obligatorio y



que pueden imponerse graves sanciones si no se cumple. Sin embargo, en la mayoría de los casos, las medidas del RDLOPD responden al sentido común y a la más elemental traslación de las conductas de seguridad del mundo físico al virtual.

Por otra parte, en muchas ocasiones el responsable del fichero no ha invertido en *software* para el tratamiento y acude a programas muy básicos que no siempre reúnen las especificaciones de seguridad que corresponden al nivel del fichero. Así, difícilmente podrá gestionarse desde el punto de vista del RDLOPD un fichero que contenga datos de salud si no se adquiere *software* adecuado. En otras ocasiones, cada vez menos, son los propios responsables del diseño y comercialización del *software* quienes no lo han implementado convenientemente.[6] De ahí que el responsable del fichero también considere entre los costes que deberá soportar los propios de la adquisición de nuevos programas.

Sin embargo, el responsable no tiene en cuenta los aspectos positivos de la aplicación de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* y del RDLOPD. Por ello, en seguridad resulta altamente conveniente explicitar los valores positivos con la finalidad de obtener una implicación de la organización. En este sentido la implementación de las medidas de seguridad:

* Proporciona un conocimiento cabal de los riesgos y vulnerabilidades y también, en muchas ocasiones, permite identificar los modos en los que se tratan los datos, suprimir tratamientos innecesarios o centralizar aquellos que lo requieran.
* Contribuye a garantizar la corrección de las decisiones de la organización ya que se basan en información confiable y no manipulada.
* Ofrece confianza al titular de los datos: su perfil informativo será el adecuado y no variará arbitrariamente.
* Garantiza el funcionamiento normal de la organización.
* Permite restaurar los sistemas ante cualquier evento imprevisto y facilita la respuesta en todos los casos incluso ante las catástrofes.

En la práctica la seguridad afecta a todas las formas de información y sus soportes así como a cualquier método usado para transmitir conocimiento, datos o ideas. Debe tenerse

en cuenta que tanto la información como los sistemas que la soportan constituyen activos valiosos e importantes para la organización. La implementación de medidas de seguridad permite depositar la suficiente confianza sobre la capacidad de dicha información y de los sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la organización. Por lo tanto, resulta evidente que la aplicación del RDLOPD no sólo puede concebirse desde una perspectiva de costes ya que se trata de algo valioso en si mismo.

5. Seguridad ¿Por qué?

La respuesta a este interrogante es doble. En primer lugar, existe un argumento sencillo y evidente. Vivimos en una sociedad cuyo valor principal comienza a ser la información y el conocimiento. En muchos sectores de producción, y sin ninguna duda en el conjunto de la administración, la información y el conocimiento poseen un valor estratégico. Pues bien la seguridad, aunque venga de la mano del RDLOPD, resulta fundamental para garantizar el adecuado funcionamiento de todos los sistemas, traten o no datos de carácter personal. Además, resulta esencial en cualquier proceso de gestión que requiera uso de tecnologías de la información y, en la práctica, se proyecta sobre el modo de ordenar la actividad de las organizaciones. El objetivo primario de la seguridad es proteger recursos valiosos: información, *hardware* y *software*. Es un instrumento que garantiza el funcionamiento de la organización. Todo ello, amén de los beneficios que se apuntaron en el epígrafe anterior.

Sin embargo, los responsables de los ficheros acaban siendo más receptivos a otro planteamiento. Deben adoptarse medidas de seguridad en cualquier caso ya que es una obligación legal impuesta por el Art. 9 de la Ley Orgánica 15/1999 y desarrollada por RDLOPD.

Desgraciadamente, se pierde de vista en muchas ocasiones un aspecto esencial. El responsable del fichero cuando trata datos personales adquiere un compromiso ineludible con el respeto del derecho a la protección de datos. Y la garantía de la seguridad -en sus dimensiones de confidencialidad, integridad, y disponibilidad- resulta un instrumento fundamental para asegurar este derecho.

[1] De hecho, la aplicación de las normas sobre protección de datos se vive en la práctica como algo que «presenta dificultades o que causa problemas». Sin embargo, nada más alejado de lo que se pretende transmitir con la primera afirmación. Se emplea aquí el término problema en el sentido que le atribuye la RAE como «planteamiento de una situación cuya respuesta desconocida debe obtenerse a través de métodos científicos». Ciertamente, se está muy lejos de afirmar que el método de interpretación y aplicación del Derecho sea exactamente el mismo que el empleado por las ciencias empíricas y no se trata aquí de reproducir el eterno debate sobre la existencia de una "Ciencia del Derecho".

[2] Normas disponibles en https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/index-ides-idphp.php.

[3] La LOPD dispone:
«Artículo 9. Seguridad de los datos.
1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.
Artículo 10. Deber de secreto.
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

[4] GARCÍA MACHO, RICARDO JESÚS. «Protección de datos personales y deber de secreto profesional», en VV.AA. MARTÍNEZ VÁZQUEZ DE CASTRO, LUIS FERNANDO, COORD. *Historia y Derecho* : estudios jurídicos en homenaje al profesor Arcadio García Sanz. Tirant lo Blanch, 1995, págs. 289-304.

[5] Existen profesionales, como los sanitarios, para los que la satisfacción del deber de secreto resulta particularmente exigente. Véase 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. Esta norma y alguno de sus desarrollos autonómicos contienen criterios respecto del tratamiento informático de la información clínica.
CALVO SÁNCHEZ, MARÍA DOLORES. «Protección de datos personales a través del secreto profesional en el ámbito de la administración sanitaria local», en *Revista de estudios de la administración local y autonómica*, núm. 300-301, 200 , págs. 361-370.

[6] Es por ello que la Disposición Adicional Única del RDLOPD obliga a que «Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar».

Protección de **Datos Personales** en los **Poderes Judiciales** de México
(INFORMACIÓN PÚBLICA, CONFIDENCIAL y RESERVADA)

Lic. Ricardo Cantú Aguillén*

"El acceso sin dificultad a la información del dominio público es esencial... como lo es la protección de dicha información contra toda apropiación indebida...".

Alejandro Alfonso, UNESCO[1]

Una Discusión Actual y Vigente/SCJN Vs. IFAI

Un tema por demás interesante, polémico y muy discutido en materia de acceso a la información en México, es el relativo a qué tipo de datos o documentos constituyen la información judicial pública, qué tipos de datos constituyen la información judicial confidencial y, qué tipos de datos constituyen la información judicial de carácter reservado. La transparencia sobre la información o datos contenidos en los expedientes judiciales, es decir, la información confidencial y reservada que se encuentra en posesión del poder judicial de la federación y de los poderes judiciales de las entidades federativas de la República Mexicana, se constituye en un tema por demás difícil y complicado de resolver.[2] ¿Hasta dónde debemos llegar en cuanto al acceso a la información de los expedientes judiciales? ¿Debe prevalecer el derecho de acceso a la información judicial sobre el derecho a la intimidad y a la privacidad de las personas involucradas o no? ¿Seguiremos la corriente de preeminencia del *habeas data* en sentido impropio de Estados Unidos o bien la corriente de preeminencia del *habeas data* en sentido propio de Europa?[3] ¿Qué en cuanto a la llamada ponderación de derechos en conflicto de colisión?[4] ¿Cómo desvincular a las personas de sus datos personales?[5]

Ponderación de Derechos en Conflicto de Colisión
EQUILIBRIO ENTRE DERECHOS O GARANTÍAS

Siempre que nos enfrentamos a la disyuntiva de determinar si el derecho de acceso a la información -y a la libertad de expresión- debe prevalecer o no, sobre el derecho a la privacidad -a la intimidad y al honor-, nos encontraremos frente a lo que en la doctrina se le ha denominado "ponderación de derechos en conflicto de colisión",[6] en donde para llegar a una solución justa, equitativa y válida entre la aplicación de un derecho sobre otro u otros, debemos primeramente determinar el equilibrio entre ambos derechos -crisis de legislaturas-, ponderar entre uno y otro para determinar cuál debe prevalecer en una situación determinada, y así encontrar una armonía entre los derechos que se encuentren en colisión -situación que como bien lo ha expresado Carlos G. Gregorio, no es nada fácil, pero tampoco imposible de resolver- trátese de libertad de expresión, acceso a información pública, acceso a la justicia, autodeterminación informativa, derecho al honor y a la intimidad o cualquier otro que se encuentre íntimamente relacionado.[7]

Con la introducción de las nuevas tecnologías de información y comunicación (TIC´S), han surgido problemas nuevos, que hasta hace apenas unos pocos años no se tenían. La simple publicación en Internet de las resoluciones judiciales plantea precisamente este problema, dado que mediante los motores de búsqueda es posible encontrar específicamente asuntos relacionados con personas en particular, violando de esta forma el derecho a la privacidad y a la intimidad. En este sentido, Carlos G. Gregorio lo ha sintetizado claramente de la siguiente forma:

"... parecería que algunos poderes judiciales están dispuestos sólo a anonimizar los casos que incluyen datos sensibles. Esto pone a América

* • Coordinador General de Transparencia de la Oficina del Comisionado para la Transparencia Municipal de Monterrey.
• Profesor de la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León.
• Autor del libro "Derecho de la Información en América Latina y en México", UANL, México: 2006.

La simple publicación en Internet de las resoluciones judiciales plantea precisamente este problema, dado que mediante los motores de búsqueda es posible encontrar específicamente asuntos relacionados con personas en particular, violando de esta forma el derecho a la privacidad y a la intimidad.

Latina en una posición equidistante entre Europa y Estados Unidos, donde la gran mayoría de las sentencias se considera publicable, excepto los casos en los que el juez ha admitido la posibilidad de que alguna de las partes litigue bajo pseudónimo. Esta equidistancia es apreciable en las *Reglas de Heredia*, que delimitan tres tipos de casos a los fines de su difusión en Internet, viz casos con datos personales sensibles, casos de personas públicas, y todos los demás casos que no entran en esas categorías. Para los primeros, se propone la anonimización. Cuando una persona pública es parte en un proceso, la difusión del texto de la sentencia no podría ocultar su nombre si la decisión está relacionada con las razones de su notoriedad. En los demás casos, las Reglas sólo establecen que los datos personales no deberían estar al alcance de los motores de búsqueda. Una consecuencia inmediata de estas Reglas es que la protección de la vida privada de las partes es abordable -en términos económicos- por la mayoría de los poderes judiciales y editoriales jurídicas de América Latina." [8]

Una solución que representa un "equilibrio real" para ponderar los derechos en colisión mencionados, lo constituye la forma en que el Poder Judicial del Estado de Nayarit publica las listas de acuerdos en el boletín judicial de primera y segunda instancias, sin mencionar los nombres ni apellidos de las partes. En tal suerte, la información proporcionada es únicamente el número de expediente, el año, el tipo de juicio y el acuerdo respectivo, por lo que solamente las partes interesadas pueden tener la identificación plena en los procesos, sin exponer los datos personales y la vida privada de las partes.[9] No estamos totalmente de acuerdo con la opinión que vierte el autor Carlos G. Gregorio al decir que es imposible en la práctica disponer de una regla de carácter general, para poder lograr un equilibrio entre el derecho de acceso a la información y otros derechos e intereses, si nos lo proponemos. Creo que lograremos encontrar una solución a dicho problema,[10] donde -como dijera Ernesto Villanueva-, ciertamente falta un largo camino por recorrer, pero se están dando los primeros pasos para lograr un verdadero equilibrio entre derechos.[11]

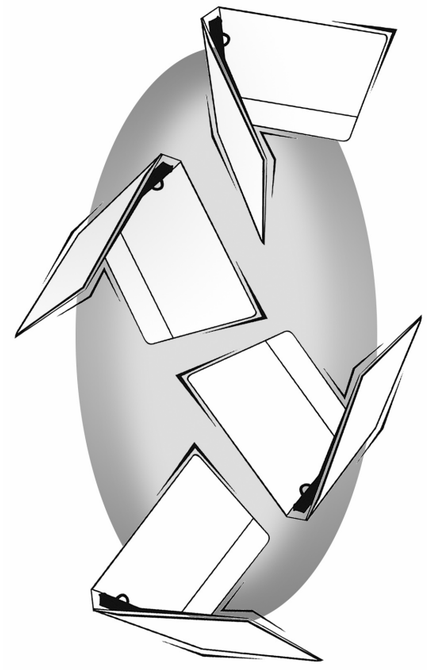
Etapas de interpretación del Tribunal Constitucional Español

El autor chileno Enoch Albertí, nos menciona que el Tribunal Constitucional español ha pasado por algunas etapas de interpretación en este tema de la ponderación de derechos en colisión, a las que nosotros hemos denominado de la siguiente manera:[12] 1) Aplicación mecánica, literal y estricta.- Debido a que originalmente interpretó que el honor y la intimidad operaban siempre como un límite al derecho de la información y libertad de expresión, reconociéndose de plano una preferencia sobre los derechos de expresión y de información; 2) Exigencia de ponderación.- Modificó su primera interpretación literal y estricta, para pasar a otro criterio en donde pasó a exigir una ponderación de los diversos derechos fundamentales en colisión; y por último, 3) Establecimiento de criterios de ponderación.- Siendo insuficiente lo anterior, dicho tribunal pasó a la etapa de establecer los criterios que debían orientar dicha ponderación, revisando que el juez ordinario aplicara de manera concreta las cuestiones planteadas de colisión.

El derecho de información y la libertad de expresión -dice este autor chileno- prevalecen sobre el derecho a la intimidad, a la privacidad y al honor, pero únicamente cuando nos encontramos frente a una dimensión colectiva o pública, por lo que los primeros derechos tienen una mayor fuerza, debiendo concurrir dos condiciones esenciales: a) Que se trate de información de gran relevancia pública, y b) Que se trate realmente de información verdadera o veraz.[13]

Las Reglas de Heredia de Costa Rica sobre Información judicial por Internet[14]

Específicamente en relación con el tema de la información judicial disponible por Internet, como ya hemos mencionado a nivel internacional se discute este tema en coloquios y eventos internacionales en América Latina, por lo que es importante recalcar las recomendaciones llevadas a cabo recientemente en Costa Rica por algunos Poderes Judiciales de América Latina y el Caribe -conocidas como las *Reglas de Heredia*-;[15] por lo que del simple estudio de las posturas adoptadas por algunos países de Europa y América Latina, pueden destacarse claramente que en los poderes judiciales a nivel internacional, existen principalmente tres corrientes sobre el acceso a la información judicial y la protección de datos personales,[16] las cuales son: 1) Preeminencia del acceso a la información -*habeas data* en sentido impropio-, vgr. Estados Unidos;[17] 2) Preeminencia del resguardo de los datos personales -*habeas data* en sentido propio-, vgr. Europa; y 3) Plano de igualdad -*habeas data* en ambos sentidos-, vgr. países redactores de las *Reglas de Heredia.*



En este sentido tenemos aún muchos temas por discutir y analizar, como por ejemplo definir adecuadamente la finalidad de la acumulación y diseminación de la información judicial, la adecuación de los motores de búsqueda, etc.[18]

Clasificación de la información judicial

PÚBLICA, RESERVADA, CONFIDENCIAL

Después de hacer un estudio de la legislación nacional existente sobre la materia de derecho de la información, creemos que el problema principal estriba -no tanto en si se encuentra clasificada o no como reservada la información que se encuentra contenida en los expedientes judiciales federales o estatales-, sino en que dicha información debería pasar a la mesa de discusión nacional sobre la posibilidad de emitirse criterios o lineamientos para clasificar como información pública, confidencial o reservada la información judicial, dado que el malestar o la polémica suscitada estriba precisamente en ello -sin dejar de mencionar los múltiples problemas de carácter jurídico con que contamos actualmente- uno de ellos, en cuanto al interés jurídico predominante en la mayoría de las legislaciones nacionales y estatales.

En este sentido, por regla general, tanto la legislación federal como las legislaciones estatales, establecen como información reservada la contenida en los expedientes judiciales y administrativos hasta que estos causen estado, y no puedan ser susceptibles de recurso alguno de impugnación, incluyéndose el amparo, a excepción de las recientes reformas en el Estado de Nuevo León, que eliminaron este concepto de "interés jurídico" para poder acceder a la información judicial de carácter reservado, lo cual consideramos un grave error, no tan solo doctrinal, sino violatorio de la protección de datos personales -*habeas data* en sentido propio-, inconstitucional en cuanto contradice al Artículo 6° de nuestra Carta Magna, y contradictorio a la tendencia nacional en cuanto a la

materia.[19]

A excepción del Estado de Sinaloa, el cual ha establecido que la información contenida en expedientes judiciales sobre divorcio, alimentos, paternidad, filiación, adopción, tutela de menores y violencia familiar, aun cuando causen estado, constituye información reservada, según el acuerdo general que norma la aplicación de la Ley de Acceso a la Información Pública de Sinaloa, mediante el cual se clasifica como reservada información contenida en procesos jurisdiccionales, emitido por el pleno del Supremo Tribunal de Justicia del estado de Sinaloa, en sesión plenaria ordinaria del ocho de mayo de dos mil tres.[20]

Lo anterior significa que la información contenida en los expedientes judiciales por regla general se encuentra temporalmente restringida por un período breve de tiempo, después del cual cualquier persona podrá tener acceso a dicha información debido a que al concluirse el período de reserva, ésta tendrá la categoría de información pública, respetándose obviamente los datos personales o confidenciales contenidos dentro de dichos expedientes.

Corrientes actuales sobre Información Judicial en México LIBERAL, EXCEPCIONAL Y CONSERVADORA

La discusión estriba en el sentido de que la clasificación contenida en los expedientes judiciales o jurisdiccionales como información judicial reservada -según la propia legislación federal, como la mayoría de los estados de la República Mexicana-, debería ser modificada y, en este sentido, podemos observar tres diferentes posturas o corrientes del tema, que pudiéramos clasificar de la siguiente manera: liberal (organizaciones de ciudadanos), excepcional (ámbito gubernamental) y conservadora (poder judicial federal):

LIBERAL La concerniente a que la información judicial contenida en los expedientes, debe clasificarse como información pública, sin ninguna restricción en cualquier etapa.

EXCEPCIONAL La concerniente a que la información judicial contenida en los expedientes debe clasificarse como información pública, pero con algunas excepciones (rubros penal y familiar principalmente).

CONSERVADORA La concerniente a que la información judicial contenida en los expedientes, no puede estar abierta al público, dado el principio del interés jurídico.

Otro aspecto no menos importante tocante a la clasificación de la información judicial reservada, estriba en qué tipo de información judicial pueden darse a conocer una vez transcurrido el término legal de reserva de información. Es decir, existe la corriente o idea de que algunos tipos de procedimientos no deben darse a conocer jamás, principalmente tenemos a los del tipo penal y a los asuntos de índole familiar. Para un mejor entendimiento de este tema, debemos hacer un recuento de las definiciones dadas a los conceptos de información pública, información reservada e información confidencial, al principio de publicidad de la información, así como observar detenidamente el articulado específico al tema de la información judicial en resguardo de los poderes judiciales, contenidas tanto en la legislación federal, como en la de las entidades de la República Mexicana.

El tema de acceso a la información judicial reservada debe ser estudiado bajo dos puntos de vista diferentes: acceso a la información administrativa judicial y acceso a los expedientes judiciales. La primera bajo la temática de que no se requiere ningún requisito ni justificación alguna, ni demostrar interés alguno (interés simple). El segundo, considerado tanto por la legislación federal (LFTAIPG), como por la mayoría de las legislaciones estatales sobre la materia, como información reservada y confidencial por los datos personales contenidos en dichos expedientes. En este tenor, discrepamos de la opinión de Hugo A. Concha Cantú, cuando afirma que la forma en que deben de proveer de información a la sociedad los poderes judiciales, es radicalmente distinta a la forma en que deben de proporcionarla los demás órganos de poder, como lo son el poder ejecutivo y el poder legislativo.[21] No es la forma en que se provee información lo que se está discutiendo a nivel federal y en las entidades federativas. Lo que está en discusión es en realidad la clasificación de información reservada y confidencial que se le ha otorgado a la información contenida en los expedientes judiciales, por lo que se pretende cambiar dicha clasificación para darle el carácter de información pública a la contenida en los expedientes judiciales, como ha sucedido con las desafortunadas reformas en Nuevo León, que pretendieron aparentemente eliminar el interés jurídico en la *Ley de Acceso a la Información Pública*, en el *Código de Procedimientos Civiles*, en el *Código de Procedimientos Penales* y en la *Ley de Justicia Administrativa* del Estado.

> ***En el plano internacional, actualmente el dato personal más sensible de todos es el ADN humano, del cual se están definiendo reglas y normas técnicas para la integración de datos biométricos -huellas dactilares, reconocimiento facial, etc.-***

Por otro lado, coincidimos con el citado A. Concha, en el sentido de que es demasiado pronto para esperar por una parte, que los gobiernos de las entidades federativas y por otra, que los poderes judiciales estatales o las judicaturas locales -como las mencionа-, muestren avances en la materia de acceso a la información, específicamente en relación con la información judicial confidencial y reservada, así como todo lo que ello implica.[22] Tal y como lo estableciera Ernesto Villanueva, podemos concluir que el acceso a la información que obra en los poderes judiciales de México, no puede ser de ninguna manera absoluto. Tiene especificado ciertas limitaciones, y cierto tipo de información o documentos deben permanecer bajo resguardo o sigilo. Dicho autor lo expone de la siguiente manera:

"El proceso de la transparencia y apertura en el Poder Judicial no puede ser absoluto. Hay ciertas informa-

ciones que deben permanecer bajo sigilo. En la experiencia comparada lo que se hace público es el cuerpo del expediente y de la sentencia, en su caso, pero sin los nombres de las personas que intervienen, particularmente si se trata de casos de derecho familiar, penal y en algunos casos de violencia doméstica y donde intervienen menores. Debe haber un equilibrio entre el principio de la máxima apertura y la protección del derecho a la vida privada y a la autodeterminación informativa."

Para finalizar, debemos mencionar que en el plano internacional, actualmente el dato personal más sensible de todos es el ADN humano, del cual se están definiendo reglas y normas técnicas para la integración de datos biométricos -huellas dactilares, reconocimiento facial, etc.-en los pasaportes y documentos de viaje, en la lucha contra el terrorismo por parte de la Organización de Aviación Civil Internacional (OACI),[23] y también se analiza y discute sobre la utilización de datos personales en las comunicaciones políticas.[24]

[1] Véase la versión estenográfica de la mesa 3 "Transparencia y Acceso a la Información en América Latina", p. 16, Alejandro Alfonso, Consejero Regional para la Comunicación de la UNESCO, dentro del marco de la Semana Nacional de Transparencia 2004, Transparencia y Buen Gobierno, organizado por el Instituto Federal de Acceso a la Información (IFAI), 14 de junio de 2004, visible en: <http://www.ifai.org.mx/snt/mesa3.pdf>.

[2] En este sentido, el estado de Sinaloa ha sido una de las primeras entidades federativas en resolver sobre la problemática actual del acceso a la información judicial reservada en posesión de los poderes judiciales de la República Mexicana, al expedir en sesión extraordinaria un acuerdo general que establece el órgano, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información pública del Poder Judicial del Estado, que norma la aplicación de la *Ley de Acceso a la Información Pública*, de fecha veintidós de abril de dos mil tres, así como un acuerdo del pleno del Supremo Tribunal de ese Estado, por el que se clasifica como reservada información del Poder Judicial, en sesión plenaria ordinaria del ocho de mayo de dos mil tres, visibles en: http://www.stj-sin.gob.mx/ . Al efecto, dicho acuerdo puede verse un poco más adelante en las notas a pie página.

[3] Cfr. Carlos Ruiz Miguel, *"La configuración constitucional del derecho a la intimidad"*, Ed. Tecnos, Madrid, 1995, quien nos menciona que para entender el derecho de toda persona al respeto de su intimidad algunos autores alemanes han elaborado la teoría de las esferas de la personalidad, como Karl Larenz, Bodo Pieroth y Bernhard Schlink, denominada como la esfera más interna (esfera de la intimidad), la cual excluye la injerencia tanto del Estado como de los particulares. Es decir, un sector inviolable que veda a cualquier poder publico su intervención, como atinadamente se defiende en la *Ley Fundamental de la Republica Federal de Alemania* (articulo 2.1), p. 19 y 20.

[4] Sobre este tema véase el excelente estudio de Carlos G. Gregorio, "Transparencia en la Administración de Justicia y Acceso a la información Judicial", el cual forma parte de un proyecto de investigación financiado por el *Internacional Development Research Center* (IDRC), véase: *(continua en siguiente página)*

<http://www.juridicas.unam.mx/publica/librev/rev/refjud/cont/2/aij/aij8.pdf>. Del mismo autor puede verse el artículo "Protección de Datos Personales: Europa Vs. Estados Unidos, todo un dilema para América Latina", en *"Transparentar al Estado: la experiencia mexicana de Acceso a la Información"*, Hugo A. Concha Cantú, Sergio López -Ayllón y Lucy Tacher Epelstein (coordinadores), Instituto de Investigaciones Jurídicas de la UNAM, México: 2004, p. 299-325, en: <http://www.bibliojuridica.org/libros/libro.htm?l=1407>.

[5] Recordando la frase "... las personas son ellas y sus datos", expresada por José Luis Pinar Mañas, Director de la Agencia Española de Protección de Datos y Presidente de la Red Iberoamericana de Protección de Datos Personales, "Protección de Datos Personales en España", al efecto puede verse en la siguiente dirección: <http://www.cpacf.org.ar/verde/vAA_Doct/archDoctri/PMa%F1as.htm>.

[6] Es pertinente mencionar que el término "ponderación" ha sido utilizado en varias jurisprudencias relativas al derecho de la información emitidas por la Suprema Corte de Justicia de México.

[7] Carlos G. Gregorio, "Transparencia en la Administración de Justicia y Acceso a la información Judicial", Op. Cit. p. 133.

[8] Carlos G. Gregorio, "Acceso a la Información Judicial: Un equilibrio de derechos", en *El acceso a la información judicial en México: una visión comparada*, Caballero Juárez, José Antonio, Gregorio, Carlos G., Popkin, Margaret, y Villanueva Ernesto (editores), Instituto de Investigaciones Jurídicas de la UNAM, México: 2005, p. 278, en: <http://www.bibliojuridica.org/libros/libro.htm?l=1646>.

[9] Véase la página del TSJ en: http://www.tsjnay.gob.mx/index1.htm>.

[10] Ver nota 8, p. 281.

[11] Véase a Ernesto Villanueva, "Derecho de acceso a la información en el poder judicial. Una aproximación al caso mexicano desde la perspectiva comparada", en *El acceso a la información judicial en México: una visión comparada*, publicado por el Instituto de Investigaciones Jurídicas de la UNAM, México: 2005, p. 188, de los editores Caballero Juárez, José Antonio, Gregorio, Carlos G., Popkin, Margaret, y Villanueva Ernesto, al efecto puede verse en: <http://www.bibliojuridica.org/libros/libro.htm?l=1646>.

[12] Cfr. Enoch Albertí Rovira, "Libertad de Información y Derecho a la Privacidad y al Honor en España y en la Convención Europea de Derechos Humanos", *Ius et praxis* año/vol. 6, número 001, Universidad de Talca, Talca, Chile, 2000, p. 59 y 60. Al efecto puede verse en: <http://derecho.utalca.cl/pgs/investigacion/iusetpraxis/6-1-2000/alber100.doc.pdf>.

[13] Idem, p. 61.

[14] Una excelente recopilación de documentos y sitios para analizar las *Reglas de Heredia* de San José, Costa Rica, es el proyecto "Internet y Sistema Judicial en América Latina y el Caribe", que dirige Carlos G. Gregorio: <http://www.iijusticia.edu.ar/internet_judicial.htm>. En dicha recopilación existen documentos relativos a información judicial, transparencia, participación y estadísticas, usos y usuarios de información judicial, vulnerabilidad derivada de la difusión de información judicial, marco normativo, soluciones normativas, soluciones informáticas y posibles líneas de acción para establecer un equilibrio entre transparencia, acceso a la información y derechos de intimidad y privacidad.

[15] Las "Reglas Mínimas para la difusión de Información Judicial en Internet", mejor conocidas como las *Reglas de Heredia* -tomando el nombre de la ciudad en donde se discutieron-, fueron aprobadas como recomendaciones durante el Seminario Internet y Sistema Judicial, realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003, organizado por el Instituto de Investigación para la Justicia de Argentina (IIJ), con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay. Véase en: <http://www.iijusticia.edu.ar/Reglas_de_Heredia.htm>. Cfr. Carlos G. Gregorio, "El equilibrio entre acceso a la información pública y autodeterminación informativa en las *Reglas de Heredia* (Uruguay)", *Revista de Derecho Informático Alfa-Redi* No. 119, Agosto 2003, <http://www.alfa-redi.org/revista/data/63-12.asp>.

[16] Sobre el tema de protección de datos personales, véase Oscar Raúl Puccinelli (Universidad Católica de Rosario, Argentina), "Hacia una convención americana de protección de los datos de carácter personal", V Convención Latinoamericana de Derecho, Cochabamba, Bolivia, 24-25 de noviembre de 2003, en donde se hace una excelente y valiosa investigación sobre la protección de datos personales a nivel internacional. Inédito, CD del Evento, 2003. Pablo Palazzi, "Alternativas legales para la protección de los bancos de datos y compilaciones electrónico de información (Argentina)", en *Revista de Derecho Informático Alfa-Redi* No. 119, Agosto 2003, <http://www.alfa-redi.org/revista/data/63-1.asp>. De Rosa Elena Di Martino, "Protección de datos de carácter personal en el Paraguay", *Revista de Derecho Informático Alfa-Redi* No. 119, agosto 2003, visible en: <http://www.alfa-redi.org/revista/data/63-6.asp>. Así como el excelente estudio de Lucy Tacher Epelstein, "Guía de las leyes de acceso a la información y datos personales en el mundo", en *Transparentar al Estado: La experiencia mexicana de acceso a la información*, de Hugo A. Concha Cantú, Sergio López-Ayllón y Lucy Tacher Epelstein, p. 327 y ss. Véase en: <http://www.bibliojuridica.org/libros/libro.htm?l=1407>.

[17] Para más información sobre el acceso a la información judicial en los Estados Unidos, puede verse el artículo de Miguel Carbonell, *"The Right to Access Information and The Federal Judicial Branch of Government"*, en la revista *Comparative Media Law Journal*, No. 3, january - june 2004, IIJ-UNAM, véase en: <http://www.juridicas.unam.mx/publica/rev/indice.htm?r=comlawj&n=3>.

[18] Respecto de un tema más enfocado a la informática jurídica que al derecho informático, el de limitar la capacidad en los motores de búsqueda en los sitios de los poderes judiciales. Artículo 24 de la Ley relativa al marco jurídico de las tecnologías de la información de Canadá, véase en: <http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/ley_161%20es.pdf>.

[19] Las reformas modificaron recientemente diversas legislaciones del Estado de Nuevo León, como puede verse más adelante cuando estudiemos dicha legislación.

[20] Dicho acuerdo establece textualmente los siguientes puntos: "... De conformidad con lo precedentemente expuesto y con fundamento en las disposiciones legales citadas, este Supremo Tribunal de Justicia en Pleno, expide el siguiente: Acuerdo por el que se clasifica como reservada información del poder judicial: PRIMERO.- Se clasifica como reservada la información contenida en los expedientes de procesos jurisdiccionales radicados y que se radiquen ante las Salas del Supremo Tribunal de Justicia, las Salas de Circuito, los Juzgados de Primera Instancia y los Juzgados Menores, todos del Poder Judicial del Estado de Sinaloa, en virtud de encontrarse contemplada en el supuesto previsto por el artículo 20, fracción III, de la Ley de Acceso a la Información Pública del Estado de Sinaloa. Dicha información se reserva en su totalidad, hasta en tanto no causen legalmente estado los procesos jurisdiccionales de mérito. SEGUNDO.- Se clasifica igualmente como información reservada la información contenida en expedientes de procesos jurisdiccionales de divorcio, alimentos, paternidad, filiación, adopción, tutela de menores y violencia familiar, aun cuando hayan causado o causen, legalmente estado, que hayan sido sustanciados ante cualquiera de los órganos jurisdiccionales del Poder Judicial del estado de Sinaloa, en virtud de encontrarse contemplada en el supuesto previsto en el artículo 20, fracción VI, de la Ley, en relación con lo dispuesto por los artículos 14, inciso 1, del Pacto Internacional de Derechos Civiles y Políticos; 3, inciso 1), y 16 de la Convención de las Naciones Unidas sobre los Derechos del Niño; y, 17, fracción III, del Acuerdo general que establece los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información pública del Poder Judicial del Estado de Sinaloa. Dicha información se reserva en su totalidad, sin sujeción a plazo alguno. TERCERO.- Serán autoridades responsables de la conservación de la información clasificada como reservada en el presente Acuerdo, los titulares de cada uno de los órganos jurisdiccionales de mérito, en el caso de la referida en el punto primero de este Acuerdo, y el Encargado del Archivo General del Poder Judicial del estado de Sinaloa, en el caso de la referida en el punto segundo." Puede verse en: http://www.stj-sin.gob.mx/.

[21] Concha Cantú, Hugo A., López-Ayllón, Sergio y Tacher Epelstein, Lucy (Coordinadores). "El acceso a la información de los Poderes Judiciales en México", en *Transparentar el Estado: La Experiencia Mexicana de Acceso a la Información*. Instituto de Investigaciones Jurídicas de la UNAM, México: 2004. P. 159.

[22] Idem. P. 183 y 184.

[23] Véase http://www.privacyconference2005.org. 27° Conferencia: "Resolución sobre el uso de la biometría en pasaportes, tarjetas de identificad y documentos de viaje".

[24] Véase http://www.privacyconference2005.org. 27° Conferencia: "Resolución sobre el uso de datos personales para la comunicación política".

Estudio en materia de transparencia de otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

SERGIO **LÓPEZ-AYLLÓN**
DAVID **ARELLANO GAULT**
Coordinadores

CIDE

ifai

La Protección de Datos Personales en los Estados de la República Mexicana

Con motivo de la reforma al Artículo 6 de la Constitución Federal, en la que se sentaron los nuevos principios para el ejercicio del derecho de acceso a la información pública y la protección de datos personales, surgió la necesidad de que todos los Estados miembros del pacto federal legislaran al respecto y particularmente en materia de datos personales.

Así tenemos que los Estados de Colima, Guanajuato y Oaxaca cuentan con leyes específicas en protección de datos personales.

La de Colima se denomina *Ley de Protección de Datos Personales*. Cuenta con seis capítulos en los que se abordan disposiciones generales, los datos de carácter personal, la creación de los datos personales, los archivos, la comisión que los protege, así como las infracciones y sanciones. Cuenta con veintitrés artículos.

La de Guanajuato se denomina *Ley de Protección de Datos Personales para el Estado y los municipios de Guanajuato*. Tiene seis títulos divididos en capítulos, en los que se abordan disposiciones generales, tratamiento de datos personales, obligaciones de los sujetos obligados, los derechos de los titulares, las solicitudes, la cesión de datos personales, autoridades, el Instituto que los protege y su atribuciones, así como las del director general del organismo; el registro estatal de protección de datos personales, los medios de impugnación, dentro de los que se encuentra el recurso de queja, y por último las infracciones y sanciones, en un total de treinta y seis artículos.

La de Oaxaca se denomina *Ley de Protección de Datos Personales del Estado de Oaxaca*. Tiene un título dividido en varios capítulos en los que se trata: las disposiciones generales, los principios generales de los datos personales; los derechos del titular de los datos personales, deberes de los sujetos obligados, la cesión de datos personales, el procedimiento de acceso a la información personal, dentro del cual se encuentra el *habeas data* y el recurso de revisión; las facultades del Instituto garante y las responsabilidades. Cuenta con cuarenta y seis artículos.

En los restantes veintiocho estados y en el Distrito Federal no existe una Ley de Protección de Datos Personales, o sin embargo, el tema de los datos personales se aborda en las respectivas Leyes de Transparencia y Acceso a la Información Pública.

La tabla adjunta muestra el Estado de la República, el número del título y capítulo en que se aborda la protección de los datos personales y el número de artículos que tratan el tema.

Estado	Título y Capítulo	Número de artículo
Aguascalientes	Capítulo IV	6
Campeche	Título primero, Capítulo VII	8
Chiapas	Título tercero, Capítulo II	4
Chihuahua	Título tercero, Capítulo III	7
Coahuila	Capítulo VI	38
Durango	Capítulo VII	9
Guerrero	Título segundo, Capítulo IV	5
Hidalgo	Título cuarto, Capítulo I	13
Estado de México	Título cuarto, Capítulo V	6
Michoacán	Capítulo VI	6
Morelos	Título cuarto, Capítulo II	14
Nuevo León	Título segundo, Capítulo I	37
Puebla	Capítulo I	5
Quintana Roo	Título primero, Capítulo VI	5
San Luis Potosí	Título quinto, Capítulo II	14
Sinaloa	Capítulo VI	4
Tabasco	Capítulo VIII	4
Tlaxcala	Título cuarto Capítulo I	16
Tamaulipas	Título segundo, Capítulo III	16
Veracruz	Título primero Capítulo V	7
Yucatán	Título primero Capítulo V	7
Zacatecas	Capítulo VI	5

Otro aspecto importante a destacar es que cinco estados de la Republica, incluyen en sus leyes de Transparencia, Acceso a la Información y Datos Personales, textualmente el concepto *habeas data*, cuyo significado podemos decir es la protección de los datos personales frente a posibles excesos del poder de registración de información de carácter personal. Los estados son: Chihuahua, Colima, Morelos, Sinaloa y Tamaulipas.

Información: Lic. Luis González Briseño
• Director General - ICAI.

Italia

Descubren estudiantes italianos "Talón de Aquiles" de Google

Investigadores y estudiantes de la Universidad de Génova, al norte de Italia, descubrieron un "Talón de Aquiles" en el buscador en Internet Google, que dejó al descubierto fallas en uno de sus sistemas de seguridad de datos.

La vulnerabilidad fue hallada en el servicio de paga *"Single Sign-On"* de la compañía estadunidense, que permite a las empresas usar el motor de búsqueda como gestor de correo electrónico, calendarios, agendas en línea y otras ventajas para sus empleados.

http://www.zocalo.com.mx/seccion/articulo/17604

U.S.A.

Facebook: La información y los riesgos asociados

Andrés Pumarino
Abogado especializado en TI
www.pumarino.cl

El acceso a las redes sociales y su mayor extensión nos permite encontrarnos con antiguos amigos o conocidos. Sin embargo, también nos lleva a entregar información tanto propia como de terceros sin que nos estemos dando cuenta. Todo ello tiene un costo no menor ya que al inscribirse en *Facebook*, por ejemplo, uno de los peligros es que muchos omiten restringir el acceso a información personal. Así, los amigos de los amigos pueden llegar a conocer gustos, vínculos e interrelaciones con terceros. Si analizamos la cantidad de información que maneja esta red social nos encontraremos con datos como que *Facebook* tiene 80 millones de suscriptores; diariamente suben 14 millones de fotografías. Todo esto puede llevar a que otras personas tengan información de nuestra información.

Si leemos las condiciones de privacidad de esta red, algo que no se suele hacer, nos encontraremos con cláusulas como la siguiente: "Tú publicas contenido de usuario en el sitio bajo tu propio riesgo. Aunque permitamos que pongas opciones de privacidad que limitan el acceso a tus páginas, por favor ten claro que ninguna medida de seguridad es perfecta o impenetrable".

http://www.mundoenlinea.cl/noticia.php?noticia_id=14078&categoria_id=31

España

La proliferación de cámaras de seguridad incrementa las quejas ciudadanas

Las oficinas de bancos tienen cámaras, algunos garajes y muchos comercios, también. Incluso en el bar donde desayuna es probable que haya instalada una. Esta proliferación de dispositivos de videovigilancia en España ha acabado calando, hasta verse reflejada en última instancia en un incremento de las quejas de los ciudadanos. Las investigaciones y denuncias por este tipo de sistemas de seguridad lo acreditan. Según la Agencia Española de Protección de Datos (AEPD), los ciudadanos presentaron en 2007 hasta cinco veces más reclamaciones sobre videovigilancia que el año anterior. "Se ha producido una eclosión de denuncias, que expresan una singular preocupación de los ciudadanos. Si en 2006 se presentaron 24 reclamaciones, en 2007 llegaron a las 123. Mientras, en el primer semestre se recibieron 112 denuncias, así que este año es previsible que al menos se dupliquen", asegura Artemi Rallo, director de la AEPD.

http://www.lavanguardia.es/lv24h/20080822/53524556289.html

Argentina

Qué hace "Google" con todos los datos personales de los usuarios

Google Argentina, en sus oficinas de Puerto Madero, recibió a la prensa para contar acerca de los servicios que presta, la seguridad, la privacidad de los datos y la publicidad que hace posible que esta empresa funcione.

Millones de personas utilizan el buscador y el correo eletrónico de la compañía.

http://www.rafaela.com/portal/modules.php?name=News&file=article&sid=11992

India

Roban los datos de millones de clientes de los hoteles Best Western

El sistema de reservas *online* de los hoteles Best Western ha sido atacado por un *hacker* indio, que ha conseguido robar los datos personales de ocho millones de clientes de sus hoteles en Europa. Por lo visto, la información hurtada era totalmente confidencial, ya que contenía nombres, direcciones, teléfonos e incluso números de tarjetas de crédito. Ya ha aparecido a la venta en una red mafiosa rusa por 3,500 millones de euros. La noticia llega después de otros robos de datos sonados, que parece que no paran de sucederse.

El ataque del *hacker* tuvo lugar la noche del pasado jueves 21 de agosto, mediante un virus troyano que penetró en los ordenadores que contenían esta información. Aunque la cadena hotelera frenó el ataque a las pocas horas de ser avisada por los periodistas del diario *The Sunday Herald*, se estima que éste sea uno de los mayores delitos cometidos en la red, en materia de robo de datos personales.

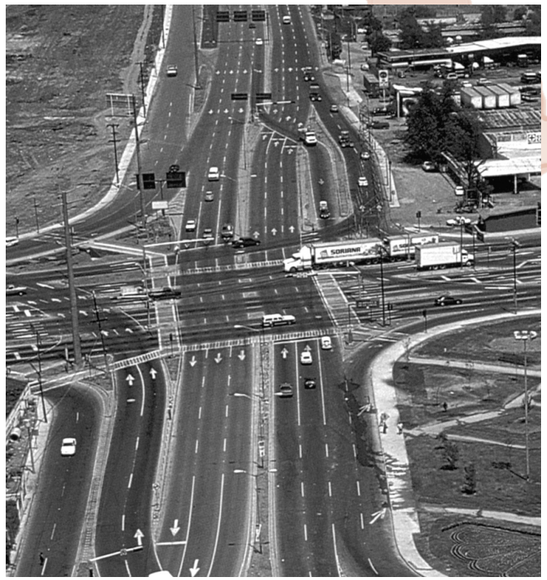
http://www.tuexperto.com/2008/08/26/roban-los-datos-de-millones-de-clientes-de-los-hoteles-best-western/

Durango

Presentan iniciativa para proteger datos personales

El origen racial o étnico, características físicas, vida afectiva o familiar, domicilio, número telefónico, entre otras cosas, son catalogados como datos personales, y la propuesta de la fracción parlamentaria del PAN es que se protejan con el respaldo de la ley.
En sesión ordinaria, los diputados de Acción Nacional (PAN) presentaron la iniciativa de la *Ley de Protección de Datos Personales para el Estado y los Municipios de Durango*.

http://www.elsiglodedurango.com.mx/noticia/180143.



Distrito Federal

Destacan necesidad de una Ley de Protección de Datos Personales

Cinco años después de que entró en vigor la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, sus dos leyes complementarias siguen atoradas.

Especialistas consultados indicaron que la ausencia de una Ley de Archivos y otra de Protección de Datos Personales ha permitido que los acervos documentales del Gobierno sigan desordenados y que no esté regulado aún el uso de datos personales en manos de particulares.

http://www.diario.com.mx/nota.php?notaid=9317084dd20e92c85ba45270a4a342f6

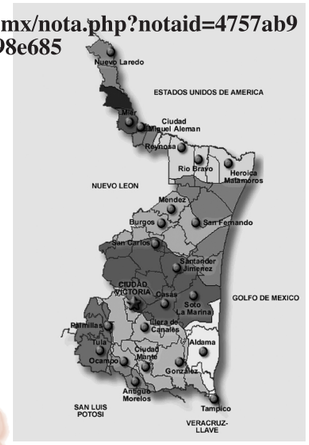
Tamaulipas

'Incitan' al robo de identidad datos recabados en puentes

Expertos consideraron que el almacenamiento por hasta 75 años de datos personales de extranjeros, y de 15 años para residentes y ciudadanos, cuando cruzan los puentes internacionales -dentro del programa denominado Información de Cruces Fronterizos (BCI)- pudiera propiciar el robo de identidad y hasta ser perjudicial para pedir un beneficio migratorio.

El director del Proyecto de Libertad, Seguridad y Tecnología del Centro para la Democracia y la Tecnología (CDT), Grez Nojeim, aseguró que las agencias de gobierno "han demostrado que a veces no son cuidadosos de proteger la información que se supone es confidencial".

http://www.diario.com.mx/nota.php?notaid=4757ab9ac4ab11e36d97d7d12998e685



Distrito Federal

Buscan integrar CURP en credenciales de elector

El Instituto Federal Electoral y la Secretaría de Gobernación suscribirán un convenio para que el órgano electoral pueda cumplir con la obligación legal de incorporar la Clave Unica del Registro de Población (CURP) a la credencial para votar con fotografía.
El convenio será presentados al Consejo General, a través de un informe de la Dirección Ejecutiva del Registro Federal de Electores sobre las acciones llevadas a cabo para la celebración del convenio.

http://eleconomista.com.mx/politica/2008/08/19/1169/integraran-curp-a-crede/

Distrito Federal

Rehúsa el IFE prestar el padrón electoral a SG; "pondría en riesgo datos confidenciales"

Por tanto, la Secretaría de Gobernación (SG) deberá procurar, con sus propios medios, la base de datos necesaria para la emisión de la cédula de identidad, es uno de los compromisos asumidos en el Acuerdo Nacional por la Seguridad, la Legalidad y la Justicia. "El IFE no va a poner en riesgo los datos confidenciales de los ciudadanos que están incluidos en el padrón electoral. No vamos a dar acceso a esos datos a ninguna autoridad del gobierno federal", advirtió ayer el presidente del IFE, Leonardo Valdés Zurita.

http://www.jornada.unam.mx/2008/08/23/index.php?section=politica&article=008n1pol

Guía de Buenas Prácticas en

Políticas de Privacidad

para las bases de datos del ámbito público

Juan Antonio Travieso*

Conforme lo dispuesto en el Decreto Nº 163/05, la Direccion Nacional De Proteccion de Datos Personales de Argentina tiene la función de coordinar las actividades de la Administración Pública Nacional referidas a la protección de datos personales.

En ese contexto y teniendo en cuenta las facultades que le otorga la Ley Nº 25.326 y su Decreto Reglamentario Nº 1558/01, se propician las siguientes medidas para un mejor desenvolvimiento de las actividades públicas que involucren tratamiento de datos personales:

1. GUÍA DE BUENAS PRACTICAS EN POLÍTICAS DE PRIVACIDAD PARA LAS BASES DE DATOS DEL ÁMBITO PUBLICO: Instrumento orientativo en materia de reglas de privacidad y confidencialidad en el tratamiento de datos personales, en el que se aporta información relacionada con los principios generales aplicables al tratamiento de datos personales. Allí se explicitan los tratamientos básicos regulados, las obligaciones del responsable del banco de datos y los derechos de los titulares de los datos.

2.CONVENIO DE CONFIDENCIALIDAD: Texto modelo por el que los funcionarios públicos se comprometen a mantener reserva de los datos personales a que pudieran acceder en ejercicio de sus funciones.

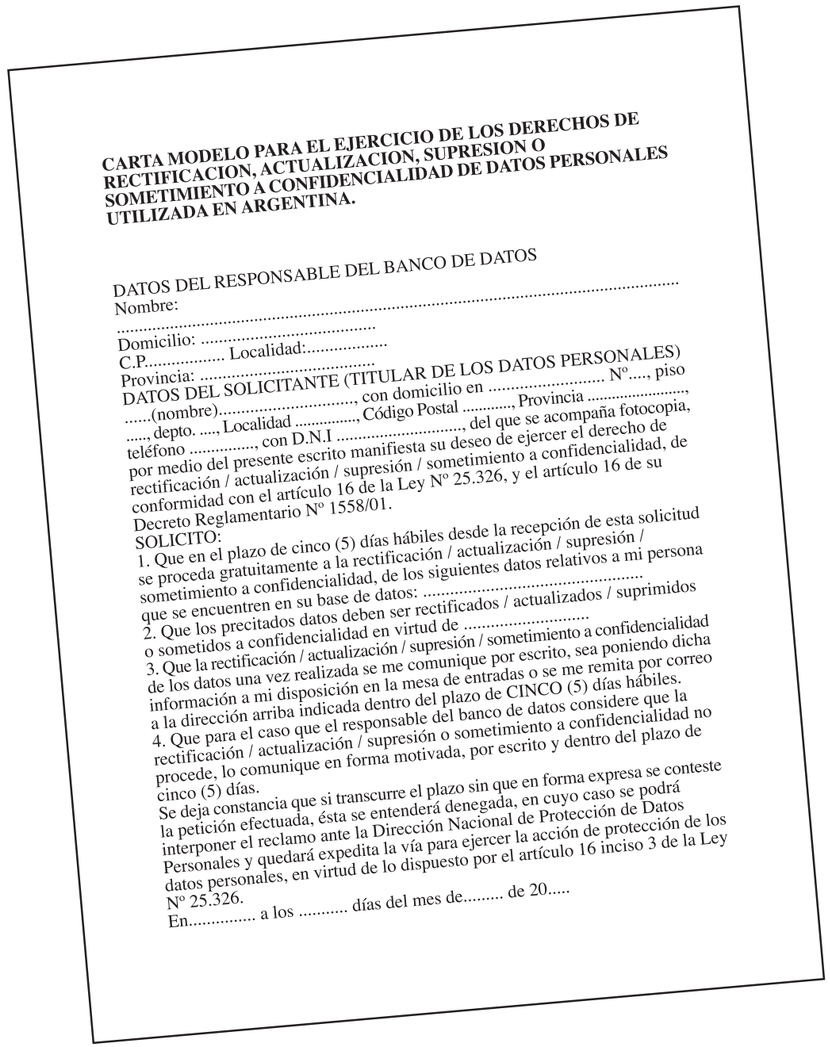
3. SELLO ARGENTINO DE PRIVACIDAD: Identificación diseñada para que los administrados conozcan qué organismos públicos han adoptado la guía que se aprueba por la presente y que podrá ser solicitada por cada organismo e incluida en su página web estableciendo asimismo un enlace a la página web, de la Dirección Nacional de Protección de Datos Personales en la que se publica el listado de los adherentes a la citada guía.

4. FORO DE PROTECCIÓN DE DATOS PERSONALES: Ámbito de participación, intercambio de experiencias y discusión de temas relacionados con la protección de los datos personales en el ámbito estatal.

5. INSTRUCCIONES Y MODELOS DE ESCRITOS PARA EL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, ACTUALIZACIÓN, SUPRESIÓN Y SOMETIMIENTO A CONFIDENCIALIDAD POR PARTE DE LOS TITULARES DE LOS DATOS: Para facilitar la tarea de las dependencias que deban cumplir con la misión de otorgar el ejercicio de los derechos enumerados, se ponen a disposición de las mismas instrucciones y modelos de escritos que éstas podrán proporcionar a los titulares de los datos interesados en el ejercicio de alguno de los citados derechos.

6. MESA DE AYUDA: Ámbito de consulta para atender particularmente las necesidades de los organismos que se adhieran a la guía que se aprueba por este acto.

"2008 - Año de la Enseñanza de las Ciencias"



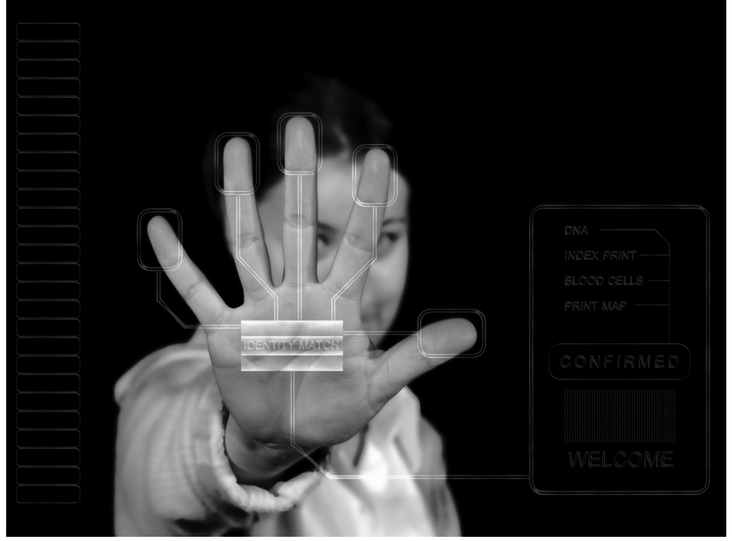
CARTA MODELO PARA EL EJERCICIO DE LOS DERECHOS DE RECTIFICACION, ACTUALIZACION, SUPRESION O SOMETIMIENTO A CONFIDENCIALIDAD DE DATOS PERSONALES UTILIZADA EN ARGENTINA.

DATOS DEL RESPONSABLE DEL BANCO DE DATOS
Nombre:
.....
Domicilio: .....
C.P..... Localidad:.....
Provincia: .....
DATOS DEL SOLICITANTE (TITULAR DE LOS DATOS PERSONALES)
.....(nombre)....., con domicilio en ..... Nº...., piso ....., depto. ...., Localidad ....., Código Postal ....., Provincia ....., teléfono ....., con D.N.I ....., del que se acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer el derecho de rectificación / actualización / supresión / sometimiento a confidencialidad, de conformidad con el artículo 16 de la Ley Nº 25.326, y el artículo 16 de su Decreto Reglamentario Nº 1558/01.
SOLICITO:
1. Que en el plazo de cinco (5) días hábiles desde la recepción de esta solicitud se proceda gratuitamente a la rectificación / actualización / supresión / sometimiento a confidencialidad, de los siguientes datos relativos a mi persona que se encuentren en su base de datos: .....
2. Que los precitados datos deben ser rectificados / actualizados / suprimidos o sometidos a confidencialidad en virtud de .....
3. Que la rectificación / actualización / supresión / sometimiento a confidencialidad de los datos una vez realizada se me comunique por escrito, sea poniendo dicha información a mi disposición en la mesa de entradas o se me remita por correo a la dirección arriba indicada dentro del plazo de CINCO (5) días hábiles.
4. Que para el caso que el responsable del banco de datos considere que la rectificación / actualización / supresión o sometimiento a confidencialidad no procede, lo comunique en forma motivada, por escrito y dentro del plazo de cinco (5) días.
Se deja constancia que si transcurre el plazo sin que en forma expresa se conteste la petición efectuada, ésta se entenderá denegada, en cuyo caso se podrá interponer el reclamo ante la Dirección Nacional de Protección de Datos Personales y quedará expedita la vía para ejercer la acción de protección de los datos personales, en virtud de lo dispuesto por el artículo 16 inciso 3 de la Ley Nº 25.326.
En..... a los ..... días del mes de..... de 20.....

* • Director Nacional de Protección de Datos Personales, de Argentina; cargo en el que fue designado por concurso.
• Es Abogado y Doctor en Derecho y Ciencias Sociales de la Universidad de Buenos Aires.
• Tiene premios nacionales e internacionales como el Premio UNESCO.

BUENAS PRÁCTICAS DE PRIVACIDAD

LOS DATOS PERSONALES Y LAS TECNOLOGÍAS DE INFORMACIÓN



Informes recientes, revelan que la información en general alojada en grandes, medianas y pequeñas bases de datos, no está del todo segura. Nos hablan de equipos de cómputo robados, medios de almacenamiento de información perdidos, *hackers* que violan las medidas de seguridad para tener acceso a la información deseada, robos de identidad, comercialización de bases de datos, entre otras experiencias.

¿Pero qué son los datos personales? Es la información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a una persona, identificada o identificable: el nombre asociado al origen étnico o racial, o las características físicas, morales o emocionales, a la vida afectiva y familiar; el domicilio, número de teléfono, cuenta personal de correo electrónico, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas, los estados de salud físicos, o mentales, las preferencias sexuales, la huella dactilar, el ADN, la fotografía y el número de seguridad social.

Recientemente se publicó un artículo en www.idg.es por la periodista Natalia Mosquera, en el que indica que el Reino Unido ha perdido la información de las personas en grandes cantidades y por distintas causas.

El Reino Unido ha perdido información personal de hasta 4 millones de habitantes sólo en un año, información de 45,000 personas almacenada en computadoras portátiles, dispositivos de seguridad y documentos, según lo declarado por el Ministro de Justicia. Además, el Ministerio de Transporte perdió la información de 3 millones de conductores y el Ministerio Exterior también extravió información que afecta a 190 personas.

Además de lo anterior un artículo publicado por "*El Mundo*" nos indica que *Revenue & Customs*, la Agencia Tributaria del Reino Unido, había perdido en el correo dos disquetes con detalles bancarios de 25 millones de ciudadanos.

En mayo del presente año publicaron una noticia en www.fayerwayer.com que decía textualmente, en el encabezado de la nota, lo siguiente: "Alerta, se filtran los datos personales de 6 millones de Chilenos vía Internet". Según la noticia, la información se presentaba en formato CSV, y estos archivos habían sido tomados de instituciones públicas. Alguna de la información que contenían estos archivos era el famoso RUN (Rol Único Nacional), el número de identificación Chileno, lo que vendría siendo la CURP en México.

En noviembre de 2007 una nota en www.jornada.unam.mx decía en su encabezado: "La base de datos del IFE-Querétaro, a la venta por Internet en $200".

En el año 2003 una noticia estremeció a todo México. Nos decían que la base de datos del padrón electoral del país había sido vendida a la empresa estadounidense *Choise Point*.

El manejo de los datos personales es una responsabilidad enorme, no solo en el cuidado sino en la administración correcta de los mismos. En el año 2003 el *Universal* comunicó que una auditoría realizada por la Secretaría de Gobernación (Segob) reveló que 17 millones de registros de la Clave Única de Registro de Población (CURP), de un total de 90 millones, tienen errores e inconsistencias, que van desde la duplicidad hasta equivocaciones en los registros.

Hablando de robo o pérdida de información, no podemos dejar de hablar de los famosos sitios *phishing*. El término *phishing* proviene de la palabra en inglés *fishing* (pesca) haciendo alusión al acto de pescar usuarios mediante señuelos cada vez más sofisticados, y de este modo obtener información financiera y contraseñas.

***Phishing** en MSN*

Dos de los ejemplos más recientes son las páginas "quienteadmite" y "noadmitido" destinadas a robar el nombre y contraseña de los usuarios de MSN a cambio de mostrarle a los visitantes que las utilicen, quien los ha borrado de su lista de contactos.

En México, a la fecha se están llevando a cabo grandes acciones para el manejo óptimo de los datos personales. Tal es el caso del gran proyecto que es llevado a cabo por parte de la Secretaría de Salud a nivel federal, con el cual pretende implementar el "expediente clínico electrónico". El objetivo de este ambicioso proyecto es lograr que los datos que se manejen en esta plataforma tecnológica que administrará dichos expedientes sean confiables y actualizados, de tal manera que el historial clínico de cada persona pueda ser consultado por cualquier clínica en México. Para este efecto, la Secretaría de Salud, realizó una prueba de interoperabilidad entre los estados de Nuevo León, Sinaloa y el propio ISSSTE, en la cual se logró compartir información a pesar de contar con distintas plataformas informáticas.

Actualmente las grandes compañías tanto de *software* como de *hardware* tienen puesta la mirada en soluciones para la protección de datos personales. Son compañías como Symantec, Adobe, F5 Networks, SUN Microsystems, Websense, entre otras. Estas empresas estuvieron presentes en la reunión que se realizó en la Ciudad de México el pasado mes de julio denominada "Las Tecnologías de la Información y el Aseguramiento de los Datos Personales en el Sector Público Mexicano". En ella expusieron algunas de las acciones que están llevando a cabo para el adecuado manejo y protección de datos personales.

Conclusiones:

Es importante proteger los datos con que se cuenta en cada una de las instituciones públicas, e implementar acciones para el manejo adecuado de los mismos, sin embargo, es necesario también realizar un análisis exaustivo de la información que se maneja para determinar si las herramientas informáticas que se utilizan son las óptimas, si las estructuras de las bases de datos son las adecuadas, y si la información que se recopila en las instituciones es en verdad suficiente o es inecesaria.

Información: César A. Muñiz Motas
• Director de Unidad Datos Personales y Sistemas - ICAI.

Otras PUBLICACIONES

Derechos humanos de los niños: una propuesta de fundamentación

Mónica González Contró

Tamaño 15 x 22 cm
XIV-568 páginas

Los derechos de los niños constituyen una verdadera prueba para las teorías de los derechos humanos, pues a partir de las fundamentaciones tradicionales resulta complicado sostener su titularidad durante la etapa infantil. La presente obra pretende aportar una nueva fundamentación de los derechos de los niños y adolescentes que permita su consideración como titulares de derechos humanos, desde un enfoque interdisciplinario y utilizando como criterio las necesidades básicas.

A lo largo de la investigación se ponen en tela de juicio los paradigmas de los cuales se ha partido usualmente, con el fin de encontrar las ideas y creencias subyacentes al discurso sobre los niños y lanzar una mirada crítica para repensar sus derechos. Así, utilizando los conocimientos aportados por las disciplinas especializadas en el estudio del desarrollo y las necesidades humanas, se someten a pruebas las teorías de los derechos subjetivos y los derechos humanos para elaborar una argumentación en favor de los derechos del niño. Para comprobar la validez de la explicación se hace una revisión de la Convención sobre los Derechos del Niño, utilizando las conceptualizaciones propuestas.

La presente obra representa un punto de vista sobre el tema que pone en duda algunas de las creencias imperantes sobre la infancia y el ejercicio de los derechos durante esta etapa de la vida humana.

www.juridicas.unam.mx / www.bibliojuridica.org

Instituto de Investigaciones Jurídicas
Coordinación de Distribución, Promoción y Fomento Editorial
Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación en Humanidades, Ciudad Universitaria, Coyoacán, 04510 México, D. F. Tels. 5622 7474 ext. 1704, fax. 5665 2193
carola@servidor.unam.mx