compendio de lecturas y legislación

Protección DE DATOS personales

Protección de datos personales

Tiro Corto Editores
MÉXICO 2010

Protección de datos personales

Compendio de lecturas y legislación

H. Cámara de Diputados

IFAI ITAM

H. Cámara de Diputados

Diputado Javier Corral Jurado
Presidente de la Comisión de Gobernación

Beatriz Solís Leree
Asesora de la Comisión de Gobernación

Instituto Federal de Acceso a la Información Pública

Integrantes del Pleno del IFAI

Jacqueline Peschard Mariscal
Comisionada Presidenta

Sigrid Arzt Colunga
Comisionada

Ángel Trinidad Zaldívar
Comisionado

María Marván Laborde
Comisionada

María Elena Pérez-Jaén Zermeño
Comisionada

Cecilia Azuara Arai
Secretaria de Acuerdos

Alejandro del Conde Ugarte
Secretario Ejecutivo

La H. Cámara de Diputados y el IFAI agradecen la colaboración del

Seminario de Derecho y Ciencia
Departamento Académico de Derecho
Instituto Tecnológico Autónomo de México

en las personas de:

Sofía Charvel Orozco
Coordinadora General

y la doctora Isabel Davara F. de Marcos
Coordinadora del diplomado en Derecho de las Tecnologías de la Información y las Telecomunicaciones

Primera edición, 2010

Guadalupe 100

Col. Lomas de San Ángel Inn

México D.F. 01790

tirocorto@gmail.com

Impreso en México

Presentación

Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros.

Los datos personales son necesarios para que un individuo pueda interactuar con otros o con una o más organizaciones sin que sea confundido con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes. Asimismo, hacen posible la generación de flujos de información que redunda en crecimiento económico y el mejoramiento de bienes y servicios.

Sin embargo, el uso extensivo de las tecnologías de la información y las telecomunicaciones ha permitido que en muchas ocasiones, los datos personales sean tratados para fines distintos para los que originalmente fueron recabados, así como transmitidos sin el conocimiento del titular, rebasando los límites de la esfera de privacidad de la persona, y lesionando en ocasiones otros derechos y libertades.

A fin de equilibrar las fuerzas entre un individuo y aquellas organizaciones –públicas o privadas- que recaban o colectan datos sobre tal individuo, surge en Europa el concepto de la protección de datos personales. Un concepto similar surgió en los Estados Unidos de América --el concepto de "privacidad"-- aunque con alcances distintos.

Bajo el concepto de protección de datos personales, el titular (o dueño) de dichos datos es el propio individuo. En naciones avanzadas, la protección de datos personales es quizá el más nuevo de los derechos que goza un ciudadano.

Luego de una evolución normativa en el ámbito internacional, el 26 de abril del 2006 el Comité de Ministros del Consejo de Europa resolvió declarar el 28 de enero como el "Día de la protección de los Datos Personales", con motivo del aniversario de la firma del Convenio 108 sobre la protección de los datos personales.

El Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito en 1981, es el primer instrumento vinculatorio de carácter internacional en materia de protección de datos y es el resultado de la decisión del Consejo de Europa, ante el rápido avance en el campo del procesa-

miento electrónico de información y la aparición de las primeras bases de datos usadas por las grandes empresas y los gobiernos estatales. Los objetivos de dicho Convenio consisten en otorgar un marco legal con principios y normas concretas para prevenir la recolección y el tratamiento ilegal de datos personales.

Por medio del Convenio 108 los países firmantes se comprometen a realizar las reformas necesarias en su legislación nacional para implementar los principios contenidos en dicho instrumento; los cuales se refieren, en primer lugar, a que los datos personales deben recolectarse y tratarse con fines legítimos y no para otros propósitos; que no deben conservarse más de lo estrictamente necesario de acuerdo con el fin para el cual fueron recolectados; que sean verdaderos, y que no sean excesivos.

Asimismo, prevé que deberá garantizarse la confidencialidad de los datos sensibles y reconoce el derecho de los individuos para tener acceso y en su caso, solicitar la corrección de sus datos.

A iniciativa del propio Consejo de Europa, se invita a las autoridades de distintos países alrededor del mundo, para generar un espacio de reflexión y promoción entre su población acerca de la importancia que tiene para cualquier individuo, el adecuado uso, obtención y transmisión de su información personal.

En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara, dada la ausencia de una disposición constitucional que les diera sustento. Si bien la reciente reforma constitucional en 2007 al artículo 6º establece en sus fracciones II y III que los datos personales y la información relativa a la vida privada será protegida, así como el derecho de acceder y corregir los datos personales que obren en archivos públicos, pero no creó un derecho fundamental independiente.

No es sino hasta la aprobación en 2009 de las reformas a los artículos 16 y 73 constitucionales que se introduce al más alto nivel de nuestra Constitución, el derecho de toda persona a la protección de su información. Lo anterior es relevante dado que los datos personales se encuentran en manos tanto de gobiernos como de particulares (empresas, organizaciones y profesionistas) y, porque con el uso indiscriminado de la tecnología, éstos pueden utilizarse para fines distintos de aquellos para los que fueron recabados, pudiendo causar afectaciones en las esferas de otros derechos de los titulares de dichos datos, tales como el robo de identidad o la discriminación.

El artículo 16 constitucional establece el derecho fundamental de los individuos a la adecuado tratamiento y la protección de sus datos personales. Por su parte, el artículo 73 faculta al Congreso Federal para expedir una Ley de Protección de datos en posesión de los particulares. La presencia de los derechos individuales de acceso, rectificación, cancelación y oposición en la Carta Magna, plantea retos tanto en el ámbito privado como

en el público. Por ello es insoslayable analizar los diseños legales e institucionales que se requieren para desplegar este nuevo derecho.

Por todo lo anterior, y en el marco de la conmemoración del día de la protección de datos personales, la Comisión de Gobernación de la Cámara de Diputados, el Instituto Federal de Acceso a la Información Pública, y el Instituto Tecnológico Autónomo de México convocan al Seminario: "Retos y perspectivas legales en materia de protección de datos, con el fin de abrir un espacio de discusión e intercambio de ideas que permita conocer los diseños institucionales y mecanismos regulatorios más adecuados para desplegar en toda su amplitud este nuevo derecho fundamental.

El presente compendio consta de lecturas introductorias al tema, así como de un acervo de regulación existente, tanto internacional como nacional, a efecto de servir como instrumento de consulta y apoyo en el ámbito de distintas instituciones tanto del sector público, como privado.

Estamos convencidos que este compendio brindará insumos indispensables para enriquecer la deliberación, en torno al derecho a la protección de datos personales.

México D.F. a 28 de enero de 2010

DIPUTADO JAVIER CORRAL JURADO
Presidente de la Comisión de Gobernación
H. Cámara de Diputados

COMISIONADA JACQUELINE PESCHARD MARISCAL
Comisionada Presidenta
Instituto Federal de Acceso a la Información Pública

Primera Parte
LECTURAS

A continuación se presenta con detalle la información bibliográfica sobre las lecturas aquí compiladas.

1. Piñar Mañas, José Luis, "¿Existe privacidad?", Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid, Madrid, España, 2008.

2. Ornelas Núñez, Lina y Sergio López Ayllón, "La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo", *Memorias del II Congreso Mexicano de Derecho Procesal Constitucional*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, 2007.

3. Davara Fernández de Marcos, Isabel, "Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual", México, 2010.

4. Peschard Mariscal, Jacqueline, "The Federal Institute of Access to Public Information as the Guarantor Entity for the Protection of Personal Data", *dataprotectionreview.eu*, número 10, Madrid, España, octubre, 2009.

5. Lujambio Irazábal, Alonso y Lina Ornelas N., "Personal Data Protection by the Government: the action of the Instituto Federal de Transparencia y Acceso a la Información Pública", *dataprotectionreview.eu*, Madrid, España, octubre, 2007.

6. Ornelas Núñez, Lina y Edgardo Martínez R., "Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad nacional", *Obra en homenaje al Dr. Héctor Fix Zamudio del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México*, Marcial Pons, España, 2007.

7. Ornelas Núñez, Lina, "El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: Evolución de derechos y su exigencia frente a las redes sociales", instituto de investigaciones para la justicia y el Centro Internacional de Investigaciones para el Desarrollo (Canadá) [en proceso de publicación].

8. Rubi Navarrete, Jesús, "Protección de datos clínicos", Revista CONAMED, Vol. 11, No. 8, octubre-diciembre, México, 2006.

9. Roldán Xopa, José, "Acceso al expediente médico", en *Derecho a saber. Balance y perspectivas cívicas*, Jonathan Fox, Fundar, México, 2007.

¿Existe privacidad? [1]

José Luis Piñar Mañas

Para conmemorar la más gloriosa
de las noches, el Gobierno de Su Majestad
se complace en devolverles a ustedes,
sus leales súbditos, el derecho a la privacidad.
Durante tres días, sus movimientos no serán vigilados
sus conversaciones no serán escuchadas…
y el "haz lo que quieras" será la única ley.
Buenas noches y que Dios les bendiga

Alan Moore y David Lloyd
V de Vendetta

El Presidente y co-fundador (en 1982) de Sun Microsytems, Scott McNealy, llegó a decir ya en 1999 que debemos resignarnos a no tener privacidad: "You already have zero privacy. Get over it"[3]. A veces ha matizado algo su afirmación, en un sentido en mi opinión igual de descorazonador (o más, si cabe): si tenemos privacidad es porque alguien tolera que la tengamos[4].

Soy consciente de que no pocos consideran que el término privacidad no es acertado. Asumo asimismo que es un concepto controvertido, neologismo para unos, barbarismo para otros[5], al que a veces se da un contenido que puede ser confuso[6]. Lo utilizo ahora, sin embargo, conscientemente, como término, además, no coincidente con el de intimidad, cuyos contornos y alcance son más limitados. En cualquier caso, está incluido en el Diccionario de la Real Academia, que define privacidad como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". El *Oxford English Dictionary* define *Privacy* como "estado en que uno no es observado o disturbado por otros" ("a state in which one is not observed or disturbed by others"). Y, sobre todo, es un concepto con presencia y contenido en el ámbito de las ciencias y de la investigación. Filósofos, sociólogos, psicólogos, arquitectos, ambientalistas, economistas, médicos y

Catedrático de Derecho Administrativo. Ex-Director de la Agencia Española de Protección de Datos

por supuesto juristas se han ocupado de la privacidad como tal. Por eso en los próximos minutos me atreveré a proponer algunas reflexiones sobre la misma. Reflexiones que girarán en torno a tres puntos. Primero, intentaré ofrecer una definición de privacidad; a continuación me referiré a los riesgos reales a los que la privacidad está hoy sometida; por último veremos las soluciones que desde el Derecho pueden ofrecerse para intentar garantizar un nivel mínimo de privacidad. Todo ello, por supuesto centrado en torno al ser humano en cuanto titular del derecho a la privacidad.

I. En torno al concepto de privacidad

Cuando hablo de privacidad no pretendo referirme en general a la "vida privada"[7], sino a un concepto más reciente, que en su configuración actual ha surgido seguramente a finales del siglo XIX. Desde luego no es nada sencillo definir la privacidad. Robert GELLMAN advierte que ninguna definición es posible ("no definition is possible")[8] y Judith Jarvis THOMSON ha dicho que "nadie parece tener una clara idea de lo que es" ("nobody seems to have any very clear idea what it is")[9]. El propio Tribunal Europeo de Derechos Humanos ha señalado que el de privacidad es "un concepto amplio no susceptible de una definición exhaustiva" ("Private life is a broad term not susceptible to exhaustive definition")[10].

Quizá ha sido en el campo de la psicosociología y la filosofía donde con más ímpetu se ha propuesto un concepto de privacidad[11]. Autores como ALTMAN[12], PEDERSEN[13] o NEWELL[14] son referencia obligada. También, por supuesto, en el campo del Derecho[15]. Aquí es obligada la referencia al juez americano Thomas COOLEY que ya en 1888 acuño la conocidísima definición de privacidad como "the right to be let alone" [16], el derecho a ser dejado solo, a ser dejado en paz; definición que hicieron famosa WARREN y BRANDEIS en su también famoso artículo "The Right to Privacy" [17], al que más adelante volveré a referirme. Tal concepto, aunque todavía digno de ser tenido muy en cuenta, ha sido desde luego superado[18]. En este sentido, las aportaciones de WESTIN son sin duda de capital importancia[19]. A él se debe precisamente la definición de privacidad en términos de autodeterminación, de "*self determination*"[20], concepto éste que más tarde fue expresamente asumido por el Tribunal Constitucional Federal Alemán en su conocida sentencia de 15 de diciembre de 1983 sobre el Censo, y que también ha sido utilizado por nuestro Tribunal Constitucional[21], como más adelante veremos.

WESTIN identificó cuatro tipos de privacidad, que PEDERSEN amplió hasta cinco: soledad, aislamiento, reserva, intimidad y anonimato. La primera, la soledad, se refiere a la situación en virtud de la cual los demás no pueden ver u oír lo que una persona está haciendo; el aislamiento implica la existencia de una distancia física para separarnos

de los demás; reserva significa controlar la revelación verbal de información a los otros; y el anonimato se consigue no siendo identificado entre la multitud. También, como señalaba, se habla de intimidad. Intimidad con los amigos e intimidad con la familia, que permitiría estar sólo con un grupo de personas excluyendo a los otros. GARZON VALDES ha distinguido entre lo íntimo y lo privado[22]. Pero lo que identifica por igual a los expresados tipos de privacidad es que en todos ellos el individuo debe poder controlar el nivel de interacción con los otros. La idea del control es la clave esencial de la privacidad, ocupa el papel central. WESTIN, como antes adelantaba, es quizá quien primero y con más énfasis ha resaltado la importancia del control: la privacidad implica libertad para elegir qué se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información[23]. Se ha hablado de la privacidad como "el derecho a controlar la información"[24].

Este poder de control ha de ponerse en íntima relación con el consentimiento, que ha de ser el título esencial que justifique ingerencias en nuestra privacidad. No el único, pues es posible prever supuestos en que, incluso sin consentimiento de la persona, se permita el uso legítimo de la información que le concierna. Pero estamos introduciendo ya elementos jurídicos en la definición que en principio quería tener un alcance más general.

Incluso estudios empíricos han demostrado que para el individuo ese control es capital: se ha constatado que quienes perciben que mantienen el control sobre el uso que se hace de sus datos tras haberlos facilitado a un tercero sienten su privacidad menos invadida que quienes piensan que han perdido el control sobre ellos. De hecho, la violación del derecho de una persona a controlar su esfera privada, sea ésta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. No es para ello necesario que la información sea más o menos importante o sensible. Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada[25]. Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información no por ello renuncia a su privacidad

Una reciente Sentencia de nuestro Tribunal Supremo[26], analizando el alcance del derecho a la intimidad[27], ha declarado que no es posible "fisgar" (*sic*) en la intimidad de las personas para satisfacer el "chismorreo" (*sic*) de la gente sin el consentimiento del interesado. Ratifica la condena a una revista "del corazón" y subraya que obtener fotografías a una famosa cantante en su finca particular sin su conocimiento y publicarlas sin su consentimiento constituye una intromisión ilegítima en la intimidad. El derecho a la propia imagen, dice la sentencia, tiene un aspecto positivo, que es la facultad del interesado de difundir o publicar su propia imagen, pero esto no elimina "su facultad

de no autorizar o impedir la reproducción de su imagen, siempre que no se encuentre en lugar público, al tratarse de una persona con proyección pública". Analiza también el alcance del consentimiento del afectado: el consentimiento prestado en otras ocasiones anteriores a que se publicasen fotografías tomadas en su finca "no puede suponer que se autorice para lo sucesivo que, de modo subrepticio y utilizando medios ópticos de fotografía capaces de obtener imágenes a notable distancia" se puedan reproducir las escenas captadas. El consentimiento "debe versar sobre la obtención de la imagen y sobre su concreta publicación en un determinado medio de comunicación social". Y deja claro que "los usos sociales no justifican indagar –"fisgar"- en los asuntos que pertenecen a la esfera exclusiva de otros y divulgar su resultado con el fin de satisfacer la curiosidad o el chismorreo de los consumidores de este tipo de revelaciones o comentarios". Como podemos comprobar se pone el acento en el control sobre la propia información, sobre ese poder de disposición a que me refiero.

El sentido de privacidad, la posibilidad de actuar y expresarse libremente, sin miedo a perder el control sobre la propia información, genera "bienestar físico y psicológico, así como espiritual" como se ha demostrado desde la psicología[28]. La pérdida de la privacidad le producía a William FAULKNER tal sentimiento que pensaba que con ello desaparecía el "sueño americano", el sueño del individuo libre[29]. Se ha afirmado incluso que la función principal de la privacidad es la protección de la estabilidad y del bienestar psicológico de las personas[30]. Estudios recientes, incluso, han empezado ha hablar del llamado *"Síndrome del Show de Truman",* en alusión a la conocida película: el pasado 29 de agosto, hace apenas unos días por tanto, algunos medios se hacía eco de la advertencia que algunos psiquiatras y psicólogos habían hecho afirmando que la sociedad de la vigilancia está provocando un nuevo tipo de psicosis generado por la idea de estar constantemente vigilado por video cámaras o a través de Internet[31].

Nuestro Tribunal Constitucional, en la Sentencia 233/2005, de 26 de septiembre (Fundamente Jurídico 4) afirma que "el derecho a la intimidad personal garantizado por el art. 18.1 CE, en cuanto derivación de la dignidad de la persona reconocida en el art. 10.1 CE, implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 70/2002, de 3 de abril, FJ 10.a; en el mismo sentido la STC 231/1988, de 2 de diciembre, FJ 3)". Incluso el desasosiego y las molestias difícilmente soportables que produce el exceso de ruido se han reconducido hacia su consideración como violación de la intimidad personal y familiar, como ya propusiera hace años entre nosotros Lorenzo MARTIN-RETORTILLO[32]

Esa posibilidad de control sobre la propia información, excluye, desde luego, el control por otros. Somos nosotros mismos los que hemos de poder controlar el grado de privacidad que deseamos tener, y hasta donde queremos abrirnos a los demás sin in-

gerencias externas injustificadas. Como recuerda RODOTA[33], L. M. FRIEDMAN ha señalado que la privacidad se basa en la "tutela de las opciones vitales contra cualquier forma de control público y de estigmatización social"[34] y F. RIGAUX ha llamado la atención acerca de la necesidad de garantizar "la libertad de las opciones existenciales"[35]. La privacidad es una condición de independencia respecto a la influencia y el poder de otros[36].

En definitiva, el fundamento de la privacidad se encuentra en el respeto a la identidad y dignidad de las personas[37], así como a la libertad. No creo que sea tan evidente la diferencia entre los modelos americano y europeo que en cuanto al lugar que ocupa la dignidad en este campo ha señalado WHITMAN[38], que parte de la inexistencia de una común "intuición" acerca de lo que debe entenderse por privacidad. No es cierto, dice, que la privacidad sea un valor absoluto en todo momento y lugar porque hay ejemplos en la historia y en las sociedades de situaciones que hoy consideramos claramente contrarias a la intimidad y que en absoluto eran tenidas como tales. Reconduciendo el dilema a parámetros jurídicos actuales, WHITMAN afirma que los sistemas europeos de protección de la privacidad son, en el fondo, "formas de protección del derecho a ser respetado y a la dignidad personal". En su esencia, el derecho a la privacidad es el derecho a la propia imagen, nombre y reputación; el derecho a controlar la información que se refiera a nosotros mismos, a la autodeterminación informativa, según el concepto acuñado por la doctrina alemana. Por el contrario, América se orienta hacia los valores de la libertad, y sobre todo libertad frente al Estado. El núcleo del derecho, en este caso, es el derecho a la libertad frente a las intrusiones del Estado. El principal riesgo es que "la santidad de nuestros hogares", "the sanctity of [our] homes," se vea amenazada por los poderes públicos. He aquí, para WHITMAN, la diferencia, el contraste entre ambos sistemas: "Por un lado tenemos un Viejo Mundo en el que aparece extraordinariamente importante no perder la propia imagen pública; por otro lado, un Nuevo Mundo en el que lo importante es preservar el propio hogar como fortaleza de la soberanía del individuo"[39]

Como antes decía, no creo que tal planteamiento sea correcto[40]. Ya hemos visto más atrás que, desde la obra de WESTIN, la idea del control sobre la propia información está también en la base de la moderna concepción norteamericana de privacidad. Ésta, allí y en Europa, es esencial para considerar respetada la dignidad del ser humano y para su propia libertad. Stefano RODOTA lo ha demostrado genialmente y hasta la saciedad[41]: sin privacidad, tanto la dignidad como la libertad resultan sustancialmente afectadas hasta el extremo de poder, sencillamente, desaparecer o ser meramente testimoniales.

La privacidad es, pues, condición indispensable para poder afirmar que una sociedad es democrática y respetuosa con los derechos fundamentales, pues sin ella, como acabo de decir, no puede hablarse ni de respeto a la dignidad ni de libertad. La pregunta

entonces es: ¿realmente vivimos en un mundo en el que puede afirmarse que la privacidad existe? ¿Es verdad que las amenazas y tensiones a que está sometida sólo pueden conducirnos, como aventuraba Scott McNEALY, a la resignación ante la idea de que no tenemos privacidad o, si la tenemos, es porque alguien así lo tolera? ¿Cuáles son los ataques a los que hoy está sometida la privacidad?

II. Los ataques a que hoy esta sometida la privacidad

En mi opinión la privacidad está sometida a diversos retos o tensiones que podrían reconducirse a las existentes en relación con la libertad de expresión, con la transparencia y acceso a la información, con los intereses y evolución del mercado y con la lucha por la seguridad ciudadana[42]. A ellas debe añadirse la derivada del siempre creciente interés por apropiarse de información ajena para fines delictivos. En muchas ocasiones la tensión se convierte en amenaza, sobre todo en lo que se refiere a la seguridad, el mercado[43] y las conductas delictivas. Y tienen siempre el común denominador de basarse en la utilización muchas veces torticera de las nuevas tecnologías, lo que al final puede llevarnos a considerar que la verdadera amenaza para la privacidad proviene del avance tecnológico que se produce en la era de la información. En particular, y en aras de una mayor seguridad mundial, la Patriot Act de 2001, aprobada en Estados Unidos tras los terribles y execrables atentados del 11 de septiembre, es una prueba más que evidente de cómo pueden justificarse medidas intrusivas de la privacidad puestas en práctica por los poderes públicos y apoyándose para ello en el uso de nuevas tecnologías, en ocasiones sin conocimiento de los afectados.

Como ya he señalado en otras ocasiones[44], nunca antes como hoy había sido posible, utilizando las tecnologías que están ya al alcance de casi cualquiera, invadir la privacidad de las personas hasta los límites a los que se está llegando. Pensemos que hoy es posible conocer los contenidos de los correos electrónicos, de las llamadas efectuadas o recibidas mediante teléfonos móviles; que pueden tratarse para múltiples finalidades los datos genéticos; que el uso de datos biométricos está casi a la orden del día; que las nuevas tecnologías pueden afectar grave e intensamente a los derechos fundamentales e incluso pueden condicionar el contenido de las normas jurídicas[45]; que mediante dispositivos de radiofrecuencia[46] es posible no sólo controlar las ventas en un centro comercial sino también localizar personas; que la capacidad de los ordenadores personales y sus funcionalidades se incrementan constantemente al tiempo que se reduce el coste de tales innovaciones -como expresa la llamada "Ley de MOORE"[47]- implicando riesgos potenciales para la privacidad y para la protección de datos personales[48]; que cada vez son más los casos en que se exigen tratamientos y transferencias internacionales de datos, así como

retenciones de datos en aras de la seguridad ciudadana; que la sociedad corre el riesgo de verse sometida a una videovigilancia constante[49].

Piénsese por ejemplo[50] en el uso de las tecnologías de radiofrecuencia (RFID), que permiten sin grandes complicaciones localizar a cualquier persona. Dispositivos tecnológicamente muy simples que hace apenas unos años se consideraban ciencia ficción. Isaac ASIMOV incluye esta conversación es su obra *Los Límites de la Fundación:*

Pelorat dijo:

—Me parece, Golan, que el avance de la civilización no es más que un ejercicio en la limitación de la intimidad.

—Quizá tenga razón. Sin embargo, antes o después tenemos que movernos por el hiperespacio o estaremos condenados a permanecer dentro de un radio de uno o dos pársecs de Términus durante el resto de nuestras vidas. Entonces seremos incapaces de emprender viajes interestelares. Además, al pasar por el hiperespacio sufrimos una discontinuidad en el espacio ordinario. Pasamos de aquí allí, y me refiero a un vacío de cientos de pársecs, algunas veces, en un instante de tiempo experimentado. De repente estamos enormemente lejos en una dirección que es muy difícil predecir y, en un sentido práctico, ya no podemos ser detectados.

—Lo comprendo. Sí.

—A menos, naturalmente, que hayan colocado un hiperrelé a bordo. El hiperrelé envía una señal a través del hiperespacio, una señal característica de esta nave, y las autoridades de Términus saben dónde estamos en todo momento. Esto responde a su pregunta, ¿verdad? No habría ningún lugar en la Galaxia donde pudiéramos escondernos y ninguna combinación de saltos por el hiperespacio nos permitiría eludir sus instrumentos.

—Pero, Golan -dijo Pelorat con suavidad-, ¿acaso no necesitamos la protección de la Fundación?

—Sí, Janov, pero no siempre. Usted ha dicho que el avance de la civilización significaba la continua restricción de la intimidad. Bueno, yo no quiero estar tan avanzado. Quiero libertad para moverme a mi antojo sin ser detectado, a menos que quiera protección. De modo que me sentiría mejor, mucho mejor, si no hubiera un hiperrelé a bordo.

— ¿Lo ha encontrado, Golan?

— No, aún no. En todo caso, podría volverlo inoperante de alguna manera.

— ¿Reconocería uno si lo viera?

— Esta es una de las dificultades. Quizá no lo reconociera. Sé cómo suele ser un hiperrelé y sé cómo examinar un objeto sospechoso..., pero ésta es una nave último modelo, diseñada para misiones especiales. El hiperrelé puede haber sido incorporado a su diseño de forma que no de ninguna muestra de su presencia.[51]

Dispositivos, pues, casi invisibles que a distancia nos controlan sin nosotros saberlo. Algo que ya no es un futurible, sino una realidad. El 19 de julio de 2004 el Primer Ministro Británico declaró que existía la intención de "etiquetar y controlar" vía satélite a los cinco mil criminales ingleses más peligrosos[52].

Piénsese también en el uso de datos genéticos, con consecuencias potencialmente gravísimas para las personas[53] pues puede llegarse a situaciones inimaginables de discriminación. No en vano el Congreso de los Estados Unidos, tras más de diez años de debate en la opinión pública y entre las fuerzas políticas, acaba de aprobar una Ley que prohíbe la discriminación por motivos genéticos, una vez aprobada por el Senado[54], basada en una lógica aplastante: nadie puede sufrir consecuencias negativas por algo que, como la herencia genética, está totalmente fuera de su control. Como ocurre con los datos raciales o étnicos, cuyo uso ilegítimo puede también producir situaciones gravemente discriminatorias para las personas[55]

Microsoft ha presentado ante la Oficina de Patentes de EEUU el programa "Monitoring System 500" que podría estar en el mercado dentro de un año y que permite controlar y analizar prácticamente todos los aspectos del comportamiento de los usuarios de equipos informáticos. El sistema opera mediante sensores inalámbricos instalados en el ordenador que permiten la captación y análisis de las palabras y números utilizados por el usuario así como las páginas web visitadas, pero también el ritmo cardíaco, la respiración, temperatura, presión arterial o expresión facial. A partir de la información obtenida, el sistema puede de inmediato (en tiempo real) detectar el estado de ánimo del usuario, sus frustraciones o situaciones de stress, pudiendo ofrecer en su caso las medidas que se consideren convenientes para superar la situación. Incluso podría detectarse información referente a la honestidad del usuario o, en manos de las fuerzas de seguridad, información sobre conductas ilícitas[56].

Mucho más avanzados están los sistemas de reconocimiento facial, face recognition technologies[57], que mediante cámaras de videovigilancia permiten el reconocimiento facial de las personas; sistema ya en aplicación en algunos lugares y que comenzó a implantarse tras los atentados del 11-S.

Hoy a través de los teléfonos móviles es posible localizar prácticamente a cualquier usuario, y lo malo es que puede hacerse sin conocimiento del interesado y por tanto sin su consentimiento. La Universidad de Bath viene experimentando desde hace tres años y ya puede poner en marcha programas de rastreo de personas a través del sistema de conexión Bluetooth[58]

El desarrollo de lo que se ha venido en llamar ubiquitous computing[59] puede llegar a permitir un seguimiento omnipresente de las personas mediante la interconexión de muy diferentes aparatos y sistemas, lo que a su vez permitirá obtener una información completa de aquéllas sin que tengan conciencia de ello.

La nanotecnología permite ya elaborar dispositivos capaces de captar y elaborar información hasta extremos insospechados y de un modo totalmente desapercibido; tal es el caso de los llamados roboflies, o de los nanobots[60].

La evolución tecnológica, además, no puede evaluarse en términos meramente cuantitativos. Una diferencia sustancial de la revolución tecnológica de ahora en relación con la revolución industrial o los avances científicos que se han producido hasta los años ochenta del siglo pasado es que ahora las nuevas tecnologías son capaces ellas mismas de generar conocimiento, lo que tiene una especial trascendencia al hablar de la privacidad y la protección de datos. El Premio Nobel Gerald EDELMAN ha confirmado ya que en el futuro (un futuro además no muy lejano) será posible crear máquinas conscientes, capaces de usar su memoria y aprender y adoptar estrategias.

Pero si lo que acabo de exponer son en parte proyectos de futuro (muy cercano, por lo demás, casi presente), lo cierto es que los supuestos reales de violación de la privacidad son cada vez más notorios y numerosos. Y no sólo en países con bajo nivel de desarrollo. Desde enero de 2005 hasta el 31 de julio de 2008 los fallos de seguridad informática notificados en Estados Unidos han afectado a un total de 234,467,328 ficheros[61]. En Alemania acaba de conocerse que por 850 Euros es posible acceder ilegalmente a más de seis millones de datos personales, entre ellos números de cuentas bancarias, direcciones, teléfonos, etc.[62] Deutsche Telekom, la mayor empresa de Telecomunicaciones de Europa, ha reconocido haber revisado ilegalmente grabaciones de llamadas telefónicas en 2005. En Reino Unido los casos se multiplican: un dispositivo informático con datos personales de 10.000 delincuentes reincidentes y de 84.000 presos internados en las cárceles de Inglaterra y Gales se ha extraviado recientemente en un nuevo caso de pérdida de documentos confidenciales, que ha confirmado el Ministerio del Interior; el Ministerio de Defensa admitió el pasado mes de julio el robo o el extravío de 747 ordenadores portátiles que guardaban información de ese departamento durante los últimos cuatro años; el Gobierno perdió en junio pasado documentos confidenciales en varios trenes de cercanías, algunos de ellos con datos sobre la red terrorista Al Qaeda y sobre Irak; a finales de 2007, igualmente, un disco informático que contenía nombres y números de cuentas bancarias de millones de personas que reciben subsidios en ese país se perdió cuando era enviado por correo desde una oficina gubernamental a otra. En Italia, a primeros del mes de mayo pasado se hicieron públicos durante unas horas en Internet los datos correspondientes a las declaraciones de la Renta de todos los contribuyentes italianos. Además, hace unos meses se hicieron públicas las conversaciones privadas de numerosas personas que habían sido sometidas a escuchas legales e ilegales. Hace apenas unos días se ha sabido que ocho millones de datos (entre ellos el número de cuenta corriente o tarjeta de crédito) de usuarios de la cadena Best Western han sido robados y, parece, puestos a disposición de grupos mafiosos.

Los ejemplos podrían multiplicarse casi hasta el infinito, y muy bien podría decirse que cualquier situación o circunstancia imaginable es ya posible. Pese a resultar un lugar común citarlo en estos casos, es necesario rememorar de nuevo la famosa denuncia orwelliana del Gran Hermano que todo lo sabe y todo lo escruta, sin posibilidad de eludir su insaciable afán de vigilante omnipresente. Vuelve incluso a recuperarse la idea del *Panópticon* de Jeremy BENTHAM, esa cárcel cuyo diseño permite al carcelero vigilar a todos los reclusos sin que estos sepan siquiera que están siendo observados, lo que haría de ellos dóciles sujetos, al saberse constantemente vigilados. Idea que más adelante teorizó Michael FOUCAULT[63] como forma de vigilancia constante y control social[64]. Se habla de la "vigilancia total"[65]. Algo que las nuevas tecnologías pueden hacer realidad[66]. Como Jeffrey ROSEN ha señalado, estamos sometidos a una "mirada no deseada", que puede destruir nuestra privacidad[67]

No son simples *"horror stories"* sobre el carácter intrusivo de las nuevas tecnologías, sobre el uso y abuso de datos personales[68]. Son situaciones reales que deben hacernos reflexionar sobre cómo es nuestra vida en el entorno de las nuevas tecnologías: cómo es nuestra vida, nuestra libertad y nuestra felicidad tras la explosión digital, según han estudiado ABELSON, LEDDEN y LEWIS[69]. Se ha hablado de la muerte de la privacidad en el Siglo XXI[70]. Desde luego es cierto que hay quien, como Amitai ATZIONI, considera que el exceso de privacidad es contraproducente para la sociedad, y, proponiendo un concepto "comunitario de privacidad" (*communitarian conception of privacy*) aboga por un mayor peso del interés general[71]. Pero aún así no es exagerado afirmar, no me canso de repetirlo, que la dignidad y la libertad están en juego. Y que para ello es imprescindible resaltar con decisión y convicción la importancia que tiene la privacidad y el derecho a la protección de datos de carácter personal. No podemos perder nuestra privacidad como consecuencia de la implantación de nuevas tecnologías[72]

Dicho lo anterior, debo hacer dos consideraciones a modo casi de advertencia.

Primera, hay un peligro extraordinariamente grave en relación con la situación que vengo exponiendo: el de considerar que todas esas medidas amenazantes para la privacidad del ser humano son no solo adecuadas, sino absolutamente necesarias para nuestra seguridad, y que por tanto debemos aceptarlas no sólo resignada sino convencidamente. Medidas que poco a poco van incorporándose a nuestra vida cotidiana y que aceptamos como algo inevitable e incluso positivo. Se incorporan a nuestro moderno y normal modo de vida como un integrante más que ya ni se cuestiona. Hace meses un conocido periodista llegó a escribir una pequeña columna titulada "Es nuestra seguridad, estúpidos", en la que abiertamente justificaba la adopción de medidas intrusivas para la privacidad en aras de una mayor seguridad. Venía de alguna manera a recuperar una vez más aquel ya viejo planteamiento de que quien quiere proteger su intimidad es porque tiene algo que ocultar. Quizá en este momento deberíamos recordar con especial convicción

la famosa frase de FRANKLIN: "Quien sacrifica la libertad en aras de la seguridad no merece ninguna de las dos" ("*He who sacrifices freedom for security deserves neither*").

Debemos reaccionar frente a quienes pretenden convencernos que son medidas beneficiosas para la Humanidad y siempre necesarias para garantizar nuestra seguridad, o que son consecuencias inevitables derivadas de nuestra convivencia con la tecnología. La realidad, muy al contrario, es que la alienación que produce el "juego" de otros con nuestra identidad (utilizando información personal, nuestros datos, y convirtiéndonos en uno más de un conjunto de elementos iguales) pone en riesgo la que Erich FROMM llama "libertad positiva", que "como realización del yo, implica la realización plena del carácter único del individuo"[73]. Por otra parte, al ser invadida nuestra privacidad, al ser sometidos a perfiles (al ser subsumidos o clasificados en perfiles) al diseñar nuestra identidad desde fuera como consecuencia del ataque desapercibido de nuestra privacidad, intimidad o datos personales, al ser o sentirnos constantemente vigilados ¿podemos ser espontáneos y por tanto libres en el sentido de FROMM?[74]. Es indudable que un sistema de vigilancia y control constante y omnicomprensivo es contrario a la espontaneidad y por tanto a la libertad. RODOTA ha señalado que "la posibilidad de construir libremente la propia esfera privada, deriva directamente de una situación en la cual no exista un programa que, de diversos modos, se imponga a la persona"[75], y se ha preguntado: "¿en qué se convertirán las ciudades, no ya concebidas como espacios de libertad, sino como lugares de vigilancia permanente?"[76].

Segunda. En la gran mayoría de las ocasiones, las violaciones a nuestra privacidad nos pasan desapercibidas. No somos ni siquiera conscientes de que se han producido o de que están produciéndose en un momento determinado. Cuando lo cierto es que en la era digital dejamos rastro de casi todo lo que hacemos o decimos, sin ser conscientes tampoco de ello, y sin serlo, por tanto, de que ese rastro puede ser fácilmente seguido, hasta el punto de afirmarse que ninguna faceta de nuestras vidas podrá escaparse de la posibilidad de ser digitalizada[77]. Estoy seguro de que la privacidad de todos los que estamos aquí ha sido hoy mismo amenazada cuando no violada por alguien en algún lugar cercano o remoto. Alguna videocámara, legal o ilegalmente instalada, ha tomado nuestras imágenes; alguien se ha hecho con nuestra dirección de correo electrónico; alguien está utilizando nuestra dirección postal para remitirnos publicidad no deseada. Pero del mismo modo nuestros datos están siendo recabados, sin saberlo, de forma legítima: la ley exige que los operadores de telecomunicaciones retengan los datos de las llamadas que efectuamos o recibimos por nuestros teléfonos móviles; las compañías aéreas deben retener y remitir a Estados Unidos todos los datos de los pasajeros que vayan a volar o ha hacer escala en aquél país; si hacemos una transferencia financiera internacional, los datos de la misma podrán ser consultados por el Departamento del Tesoro de Estados Unidos; cuando nos alojamos en un hotel, nuestros datos son pasados de inmediato a las Fuerzas y Cuerpos de Seguridad.

¿Debemos pues resignarnos a perder la privacidad? ¿Hay algo que podamos hacer?

Ante todo hemos de ser conscientes de que somos nosotros los que primero debemos actuar en defensa de nuestra privacidad. Como vimos más atrás, el control sobre la esfera privada es esencial para considerar respetada nuestra privacidad. En este sentido, son varias las dimensiones de la privacidad en sentido amplio. BURGOON[78] ha distinguido las dimensiones física, social, psicológica y la referente al tratamiento de nuestros datos personales ("information privacy"[79]). Y hay que decir que mientras que el control es más fácil en relación con la privacidad física y social, no lo es tanto respecto a sus dos ulteriores dimensiones. En el caso de la privacidad psicológica y la protección de datos, el acceso por terceros a la información personal puede implicar que el afectado pierda casi definitivamente el control sobre la misma. Esto significa que en relación con cierta información, el individuo sólo tiene la opción de revelarla o no, pues una vez que se pone a disposición de terceros, no tiene posibilidad de recuperarla, lo que hace diferente la gestión de los datos personales respecto a otras dimensiones de la privacidad, pues en este caso es posible cometer "errores irreversibles"[80]. Por eso, como digo, somos nosotros mismos los que primero hemos de poner todas las armas sobre la mesa y adoptar todas las cautelas posibles para proteger nuestra privacidad.

Pero si esa fuese la única solución estaríamos sin duda abocados a la más absoluta de las melancolías, pues poco podemos hacer por nosotros mismos ante la potencialidad de las nuevas tecnologías, que de forma invisible y, como antes decía, ajena a nuestro conocimiento y voluntad, son capaces de recabar información hasta niveles inimaginables. ¿Es entonces posible la defensa y garantía efectiva de la privacidad? ¿Qué podemos hacer, desde nuestra modesta posición, los juristas?

III. ¿Es posible la defensa y garantia efectivas de la privacidad?

Como más atrás ya adelantaba, en 1888 Thomas COOLEY habló ya del "derecho a ser dejado solo", a ser dejado en paz; "the right to be let alone"[81]. En 1890 Samuel WARREN y Louis BRANDEIS publican en la *Harvard Law Review*[82] su famoso artículo "The Right to Privacy". En aquel entonces WARREN y BRANDEIS, impulsados por la necesidad de poner coto a una situación personal en que se había encontrado la esposa de uno de ellos, que sufrió la invasión de su vida privada por diversos periodistas[83], hablaron de un nuevo derecho: "Los cambios políticos, sociales y económicos –expusieron entonces- traen consigo el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, acierta a satisfacer las nuevas demandas de la sociedad". Al principio el derecho actuaba sólo frente a las interferencias físicas de la vida y la propiedad. Más tarde se reconoció la naturaleza espiritual del hombre. Gradualmente el objeto de los

derechos se fue ampliando, y ahora el derecho a la vida ha pasado a significar derecho a disfrutar de la vida, que incluye el derecho a que te dejen estar solo. El derecho debe preservarnos frente a las invasiones de los "sagrados límites de nuestra vida privada y doméstica". El derecho a la privacidad supone, pues, el derecho a poder estar solo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir ingerencias no deseadas y sin interferir en el derecho de los demás[84].

La evolución que desde entonces se ha producido ha sido imparable. Los tribunales americanos comenzaron a aplicar y reconocer el nuevo derecho a la privacidad[85], aún más tras las aportaciones de PROSSER y su construcción teórica en torno al concepto de los daños derivados de la invasión de la privacidad (*privacy torts*)[86], mientras que en Europa tanto a nivel constitucional como legislativo y jurisprudencial se ha consolidado ya desde hace años el derecho a la intimidad, a la privacidad y, más recientemente (a partir de los años setenta del pasado siglo) el derecho a la protección de datos.

El derecho al respeto a la vida privada ha sido incorporado a la práctica totalidad de los grandes instrumentos internacionales de reconocimiento de derechos fundamentales. El artículo 12 de la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948[87], el artículo 11 de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica), de 1966[88], el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre del mismo año 1966[89], el artículo 8 del Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950[90] son ejemplo de ello. Como lo es la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000[91], sobre la que luego volveré. Por otra parte, la práctica totalidad de los textos Constitucionales reconocen asimismo el derecho a la intimidad o privacidad, cuya regulación se deja en manos de legislación específica.

Dicho lo anterior, es posible afirmar que el proceso normativo reciente en relación con la regulación del derecho a la privacidad nace en los años sesenta y setenta del siglo XX.

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los Derechos de las personas, especialmente en relación con su Derecho a no sufrir ingerencias en la vida privada. De tal Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo Europa sobre *"los Derechos humanos y los nuevos logros científicos y técnicos"*, que respondía a una inquietud existente en toda Europa.

Es lugar común citar la Ley de Protección de Datos del Estado alemán de Hesse, la primera ley de protección de datos de la historia. En 1973 el Departamento de Salud, Educación y Bienestar de Estados Unidos elabora un Informe sobre las bases de datos telemáticas del Gobierno[92] y propone un Código de buenas prácticas que recogería los principios que han de regir el uso de información por parte del Gobierno (*Fair Infor-*

mation Practices o *Fair Information Principles*): no deben existir bases de datos secretas, se ha de reconocer el derecho de acceso y rectificación de los datos personales, ha de respetarse el principio de finalidad, debe respetarse el principio de calidad y han de adoptarse medidas de seguridad. Un año más tarde, y en base a tal Informe, se aprueba la Privacy Act de Estados Unidos, y van poniéndose las bases de los principios esenciales configuradores del núcleo esencial del derecho a la privacidad. Como se ha señalado, de los *privacy principles* se pasa a las *privacy laws*[93]. Veremos que tales principios fueron en parte el embrión de los que más tarde se recogerían en textos internacionales y en normas europeas y nacionales[94].

El 8 de mayo de 1979 el Parlamento Europeo aprueba una Resolución sobre *"La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática*". En los años ochenta, desde el Consejo de Europa se dará un respaldo definitivo a la protección de la intimidad frente a la informática mediante el Convenio nº 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal (1.981). Este Convenio establece los principios y Derechos que cualquier legislación estatal debe recoger a la hora proteger los datos de carácter personal e intenta conciliar el Derecho al respeto de la vida privada de las personas con la libertad de información, facilitando la cooperación internacional en el ámbito de la protección de datos y limitando los riesgos de desviaciones en las legislaciones nacionales.

En fin, también la OCDE publica en 1980 dos importantes Recomendaciones en esta materia: la Recomendación sobre *"Circulación internacional de datos personales para la protección de la intimidad"* y la Recomendación relativa a la *"Seguridad de los sistemas de información",* y unos años más tarde, el 15 de diciembre 1983, el Tribunal Constitucional Alemán dicta su capital Sentencia sobre el Censo en el que, como ya he apuntado más atrás, se reflejan las aportaciones que desde la doctrina (principalmente norteamericana y en particular de la mano de WESTIN) se habían producido en orden a destacar el papel capital que tiene el control sobre la propia información en la configuración del derecho a la privacidad y a la protección de datos. El Tribunal Constitucional Alemán completó los derechos constitucionales de la personalidad a pesar de la inexistencia en la Ley Fundamental de 1.949 de un derecho específico. Sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad el Tribunal garantizó la continuidad de las libertades básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa. En la clave de bóveda del ordenamiento de la Ley Fundamental, dice el Tribunal, se encuentra la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. El derecho general de la personalidad abarca la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, protegiéndole contra la recogida,

el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona. Se garantiza así la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales. El tratamiento automatizado de datos ha incrementado en una medida hasta ahora desconocida las posibilidades de incidir sobre la conducta del individuo. El que no pueda percibir con seguridad suficiente qué informaciones relativas a su persona son conocidas en determinados sectores de su entorno social y no pueda saber en consecuencia qué se sabe de él, puede coartar substancialmente su libertad de planificar o decidir. Por ejemplo, quien sepa de antemano que su participación en una reunión o iniciativa ciudadana va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de sus derechos fundamentales. De modo que un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, concluye el Tribunal que ya no existe, desde la perspectiva del tratamiento automatizado de datos, ninguno "sin interés".

A partir de esta sentencia, que incorpora a los principios esenciales del derecho a la privacidad el del consentimiento, tal derecho y el derecho a la protección de datos ya no fueron lo mismo en Europa. Aunque todavía faltaba mucho por andar.

En la década de los noventa se incorpora un elemento fundamental al debate. La construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una economía cada vez más globalizada y transfronteriza. En este escenario se mueve la Directiva 95/46/CE[95] sobre protección de datos, que es sin duda la pieza jurídica más importante que sobre protección de datos existe[96]. Norma que, junto con la jurisprudencia del Tribunal de Justicia dictada sobre la materia[97], ha influido decisivamente en el desarrollo no ya a nivel europeo sino mundial (sin exageración alguna) del derecho a la privacidad y en particular del derecho a la protección de datos[98].

En el año 2000 la situación experimenta un giro copernicano tanto en Europa como en España. Se abre una nueva etapa, en la que ahora nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad. Tan radical innovación deriva fundamentalmente de la Jurisprudencia del Tribunal Europeo de Derechos Humanos[99] y de la Carta de los Derechos Fundamentales de la Unión Europea, que consolida definitivamente la diferencia entre el derecho a la privacidad y el derecho a la protección de datos. Al primero dedica un artículo, el 7º[100], mientras que el 8º reconoce de forma expresa y diferenciada el derecho fundamental a la protección de datos de carácter personal[101]. El carácter autónomo del derecho a la protección de datos[102] adquiere así carta de naturaleza al más alto nivel normativo. Privacidad, intimidad

y protección de datos no son conceptos equivalentes. Como ha señalado RODOTA, el reconocimiento de la protección de datos como derecho independiente contribuye a la "constitucionalización" de la persona, que el Preámbulo de la Carta sitúa en el centro de la acción de la Unión Europea[103].

Hay que decir, por cierto, que en virtud del artículo 2º de la Ley Orgánica 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta[104].

En España, ese 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[105].

La segunda de ellas, en particular, reconoce que el Derecho fundamental a la protección de datos personales deriva directamente de la Constitución y debe considerarse como un Derecho autónomo e independiente. El Fundamento Jurídico Séptimo es sin duda esencial, por lo que creo oportuno transcribirlo:

> 7. De todo lo dicho resulta que el contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.
>
> Y ese Derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.
>
> En fin, son elementos característicos de la definición constitucional del Derecho fundamental a la protección de datos personales los Derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.
>
> Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del Derecho a ser informado de quién posee sus datos personales y con qué fin, y el Derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del

> fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele[106].

Reconocida ya de forma indudable la existencia de un nuevo derecho, el de la protección de datos, cuya efectividad es esencial para la existencia misma de la privacidad, hay que definir los principios que lo configuran[107]. Tales principios pueden reconducirse a los que quizá son más nucleares en la configuración del derecho: Consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad. Principios todos ellos recogidos en la Ley Orgánica de Protección de Datos, artículos 4 y ss., a los que puede añadirse el de utilización leal de los datos y el de minimización en el uso de los datos (éste, por cierto, reconducible, también, en mi opinión, al de proporcionalidad). Principios que para ser efectivos requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición (regulados, en nuestro caso, en los artículos 15 y ss. de la LOPD).

Los anteriores principios alcanzan pleno significado desde el reconocimiento de que el derecho a la protección de datos se fundamenta en el poder de disposición de los datos personales por su titular, y en que tales datos son sometidos a tratamiento. Lo que se traduce en que por definición quien trata datos personales trata datos ajenos, no propios, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto a la dignidad de la persona, base fundamental de la protección de datos. Y explica perfectamente los principios que antes he mencionado.

En efecto, si los datos sometidos a tratamiento son datos ajenos y su utilización ha de hacerse en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre los datos, es lógico que cuando se recaben datos deba informarse al interesado (arts. 10 y 11 de la Directiva 95/46/CE; art. 5º de la LOPD y arts. 18 y 19 del Reglamento). Que el tratamiento deba estar amparado en un título que habilite su utilización, siendo esencial el consentimiento del titular de los datos (art. 7 de la Directiva y art. 8 de la Carta Europea de Derechos Fundamentales; arts. 6, 7 y 11 de la LOPD; arts. 12 a 17 del Reglamento). Que los datos sólo puedan utilizarse para la o las finalidades legítimas para las que fueron recabados (art. 6.1.a de la Directiva; art. 4 de la LOPD; arts. 8º y 9º del Reglamento), y que ha de respetarse el principio de proporcionalidad y mínima ingerencia en su tratamiento, así como uso leal y lícito (art. 6 de la Directiva; y, de nuevo, art. 4 de la LOPD y arts. 8º y 9º del Reglamento). Y que deben tratarse con seguridad (arts. 16 y 17 de la Directiva; art. 9 de la LOPD; arts. 79 y ss. del Reglamento). Todo ello, además, como he señalado, garantizado a su vez por el reconocimiento a los titulares de los datos de los derechos de acceso, rectificación, cancelación y oposición (arts. 12 y sigs. de la Directiva; arts. 15 y ss. de la LOPD; arts. 23 y ss. del Reglamento),

imprescindibles para garantizar ese derecho de disposición de los datos que está en la base misma del sistema.

Además, la Carta Europea de Derechos Humanos, siguiendo ya la tónica de textos anteriores, da un paso capital a favor de otro de los principios que ya son inherentes a la protección de datos: el principio que podría denominarse de control independiente. En efecto, al disponer que "*El respeto de estas normas [de protección de datos] quedará sujeto al control de una autoridad independiente"* está exigiendo la existencia de tal autoridad como requisito para considerar que el derecho a la protección de datos está suficientemente garantizado. De modo que se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho. Precisamente uno de los puntos esenciales de las decisiones de adecuación que hasta ahora ha aprobado la Comisión Europea en relación con la protección ofrecida por terceros países es la de la existencia de una autoridad independiente de control.

En cuanto a la privacidad propiamente dicha, se ha dejado firmemente sentado que es un derecho que ha de reconocerse a todas las personas. El Tribunal Constitucional, así lo ha recordado, por ejemplo, en relación con los presos. En las Sentencias 89/2006, de 27 de marzo, y 89/1987, de 3 de junio ha señalado que "una de las consecuencias más dolorosas de la pérdida de la libertad es la reducción de lo íntimo casi al ámbito de la vida interior, quedando, por el contrario, expuestas al público e incluso necesitadas de autorización muchas actuaciones que normalmente se consideran privadas e íntimas", lo que exige preservar especialmente los ámbitos de intimidad no concernidos por la pena o la medida y por su ejecución, y de declarar "ilegítimas, como violación de la intimidad y por eso también degradantes, aquellas medidas que la reduzcan más allá de lo que la ordenada vida de la prisión requiere"[108].

También ha subrayado el Tribunal (Sentencia 233/05, F.J. 4, último párrafo) que "para que la afectación del ámbito de intimidad constitucionalmente protegido resulte conforme con el art. 18.1 CE, es preciso que concurran cuatro requisitos: en primer lugar, que exista un fin constitucionalmente legítimo; en segundo lugar, que la intromisión en el derecho esté prevista en la ley; en tercer lugar (sólo como regla general), que la injerencia en la esfera de privacidad constitucionalmente protegida se acuerde mediante una resolución judicial motivada; y, finalmente, que se observe el principio de proporcionalidad, esto es, que la medida adoptada sea idónea para alcanzar el fin constitucionalmente legítimo perseguido con ella, que sea necesaria o imprescindible al efecto (que no existan otras medidas más moderadas o menos agresivas para la consecución de tal propósito con igual eficacia) y, finalmente, que sea proporcionada en sentido estricto (ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto) [SSTC 207/1996, de 16 de diciembre, FJ 4; y 70/2002, de 3 de abril, FJ 10 a)]". En la Sentencia 89/2006, de 27

de marzo, el Tribunal ha señalado: "En este sentido, hemos destacado (SSTC 66/1995 y 55/1996) que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"" (STC 207/1996, de 16 de diciembre, FJ 4.e)".

Vemos por tanto que el artículo 18 de la Constitución de 1978, en sus cuatro apartados, es el punto de referencia entre nosotros[109]. Y con él, las leyes que lo han desarrollado, de entre las que me permitiría destacar la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen, con sus modificaciones[110], los diversos preceptos del Código Penal referentes al tema, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, complementada por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la misma[111]. Además, son múltiples las leyes que directa o indirectamente regulan aspectos relacionados con la privacidad[112].

Desde el Derecho, pues, se articulan instrumentos de reacción frente a las constantes amenazas a que está sometida nuestra privacidad, sobre todo, como vengo insistiendo, frente al uso de las nuevas tecnologías. No en vano las primeras leyes sobre protección de datos nacen precisamente en los años setenta del sigo XX, cuando comienza a implantarse el uso de los primeros computadores o cerebros electrónicos, que ahora nos parecen absolutamente rudimentarios. El legislador supo reaccionar a tiempo y, a través de textos internacionales, leyes nacionales, y de la jurisprudencia se han ido fijando las reglas del juego que, con el valor de lo jurídico –no siempre suficientemente efectivo, hay que decir- pretenden evitar la desaparición de la privacidad y la protección de datos.

Pero, ¿es suficiente la respuesta del derecho tal como acabo de exponerla? BENNETT y RAAB consideran que las leyes de protección de la privacidad y de protección de datos sólo pueden tener un "impacto marginal" en el desarrollo de la sociedad de la vigilancia[113]. HOLTZMAN considera que las leyes de protección de datos "no funcionan particularmente bien"[114]. RULE considera incluso que en no pocas ocasiones las leyes que regulan el derecho a la privacidad son utilizadas para legitimar la introducción de nuevos sistemas de vigilancia[115]. LAPERRIÈRE ha señalado que la legislación de protección de datos parece una solución del pasado[116]. GELLMAN se ha preguntado directamente si el derecho a la privacidad realmente funciona[117].

Tales críticas provienen del otro lado del Atlántico, de la doctrina Norteamericana. Pero no cabe duda de que algo de verdad hay en lo que dicen. Porque parece evidente que el recurso a la ley, a la heterorregulación no es quizá por sí sólo remedio suficiente para garantizar de forma efectiva nuestro derecho a la privacidad y, más en particular, a la protección de datos de carácter personal.

Lo anterior en absoluto debe interpretarse en el sentido de que la ley es un instrumento ineficaz. En Europa, en los sistemas del *Civil Law*, seguimos creyendo en la bondad de la ley. Sobre todo si consideramos que estamos ante derechos fundamentales cuya regulación debe reservarse precisamente a la ley. Además, la interpretación que de la ley hacen los jueces y tribunales permite avanzar en el reconocimiento de los derechos y en una nueva configuración de los mismos adaptada a la nueva realidad social y, también, tecnológica. El Derecho, ante los avances tecnológicos, sigue evolucionando para hacer frente a nuevos y sofisticados ataques que pueden amenazar su contenido y razón de ser. En este sentido, y vuelvo al Tribunal Constitucional Alemán, tan importante como ejemplar es su Sentencia de 27 de febrero de 2008[118]. La sentencia es fruto del recurso interpuesto contra la reforma de la ley de los servicios de inteligencia del Estado de Renania del Norte Westfalia, en virtud de la cual se permitía expresamente que tales servicios pudiesen utilizar de forma secreta *spywares* troyanos para espiar los ordenadores de cualquier sospechoso: penetran en los ordenadores y captan todo tipo de información, que luego puede ser analizada. El Tribunal declara inconstitucional la reforma y configura, por primera vez, lo que se ha considerado ya como un nuevo derecho fundamental a la protección de la confidencialidad e integridad de los sistemas tecnológicos de información. El Tribunal de Karlsruhe da así un paso más en el reconocimiento, primero, del derecho a la autodeterminación informativa (en 1983 como ya sabemos) y más tarde del derecho a la protección absoluta de la zona nuclear ("core area") del comportamiento privado ("private conduct of life"). El Tribunal llega al siguiente razonamiento: "De la relevancia del uso de los sistemas tecnológicos de información para expresar la personalidad y de los peligros que para la personalidad representa tal uso, deriva una necesidad de protección que es significativa para los derechos fundamentales. El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la irrestricta expresión de su personalidad"[119]. Los sistemas de información protegidos por este nuevo derecho son todos aquellos (ordenadores personales, PDAs, teléfonos móviles…) que solos o interconectados con otros pueden contener datos personales del afectado de modo que el acceso al sistema permite hacerse una idea sobre aspectos relevantes del comportamiento vital de una persona o incluso obtener una imagen representativa de su personalidad[120]. Este derecho a la integridad y confidencialidad de los sistemas tecnológicos de información, que tendría la consideración de verdadero derecho constitucional, sólo puede ser restringido en casos muy limitados.

Sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro online. Técnicas que, en consecuencia, no pueden ser utilizadas en las investigaciones relacionadas con delitos "normales" ni en la actividad genérica de los servicios de inteligencia. Y que en cualquier caso requieren la adopción de medidas para proteger el núcleo central de la vida privada ("core area of private conduct of life"), que incluye la información relativa a las relaciones y los sentimientos personales. Por ello, el Tribunal señala que en caso de que de forma accidental se recabasen datos referidos a esa área vital, deben ser suprimidos de inmediato sin que puedan ser utilizados en ningún caso.

Es decir, el derecho a la privacidad alcanza también a los dispositivos informáticos que utilizamos y que forman parte ya de nuestra propia vida, que contienen información que nos identifica y que puede dar una imagen de nuestra personalidad.

Es éste, pues, un paso de gigante en la evolución del derecho a la privacidad y a la protección de datos. Pero los problemas siguen siendo muchos y las herramientas con que contamos no siempre son eficaces. Por eso es necesario buscar nuevas soluciones complementarias.

En este sentido la autorregulación es un instrumento que parece extraordinariamente útil y oportuno. De hecho el modelo norteamericano pivota en gran medida en torno a la autorregulación, a los códigos de conducta, a las políticas de privacidad[121]. Y también en Europa se ha apostado decididamente por esta vía. Así lo hace la Directiva 95/46/CE; así lo hacen las leyes de los Estados miembros de la Unión Europea; y así lo hace la Ley Orgánica de Protección de Datos de 1999, sobre todo tras la aprobación del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, cuyos artículos 71 a 78 contienen una muy razonable regulación de los llamados códigos tipo[122].

También resulta imprescindible reforzar la posición de las autoridades independientes de protección de datos. Ya hemos visto cómo el de control independiente es uno de los principios configuradores del contenido esencial del derecho a la protección de datos[123]. La existencia de tales entidades es requisito imprescindible para que la Unión Europea reconozca respecto de un tercer país que cuenta con un nivel adecuado de protección lo que facilita sobremanera la transferencia internacional de datos. No hace mucho las autoridades de Reino Unido, Alemania y Francia han reclamado mayores competencias y un sistema más riguroso de control y tratamiento de la información.

Por otra parte, la privacidad y el derecho a la protección de datos han de enfrentarse a procesos de globalización y de construcción de instrumentos que permitan garantizar al máximo su eficacia frente a ataques que no saben de límites fronterizos y que provienen en innumerables ocasiones de países en los que no hay en absoluto un marco jurídico de

la protección de la intimidad y en los que por tanto es imposible intentar siquiera poner en marcha mecanismo efectivos de *enforcement*[124]. Uno de los mayores obstáculos que hoy se presentan para conseguir una efectiva garantía y tutela de la privacidad es la falta de instrumentos jurídicos que afirmen la extraterritorialidad de las conductas ilícitas de tratamiento informatizado de la información, en relación con las cuales el territorio físico no tiene, sencillamente, trascendencia alguna.

Así mismo es muy necesario tener en cuenta que numerosas normas y actividades, públicas y privadas, tienen un considerable impacto sobre la privacidad y el derecho a la protección de datos, que no siempre es identificado por quines elaboran unas o llevan a cabo las otras. Es más, me atrevería a afirmar que la gran mayoría de las disposiciones que se adoptan, legales o reglamentarias, tienen una repercusión directa o indirecta sobre los derechos que ahora analizamos. Por ello creo que sería imprescindible introducir mecanismos y/o procedimientos de evaluación de impacto sobre la privacidad[125]. En el ámbito de las nuevas tecnologías cada vez se habla con más frecuencia de la *Privacy Impact Assessment* (*"PIA"*) como metodología que identifica las cuestiones relativas a la privacidad y los potenciales riesgos que para la misma pueden venir asociados con la implantación de nuevas tecnologías[126]. Se trata, pues, de integrar la protección de datos y la privacidad en la actuación de las organizaciones y en el proceso normativo.

En fin, se habla ya de un nuevo principio de la privacidad, el llamado "*Privacy by Design*"[127] en virtud del cual las consideraciones sobre privacidad deben ser incorporadas previamente al diseño de los sistemas informáticos, incluyendo medidas de seguridad para los componentes físicos, así como políticas y protocolos sobre privacidad. Tal modo de actuar, además, ahorrará tiempo y esfuerzos a largo plazo[128]. Principio que en realidad pone en relación el derecho y la técnica, algo esencial en el desarrollo de la privacidad y la protección de datos[129].

IV. Conclusion

En efecto, y ya concluyo, cuando hablamos de la necesidad de contar con un marco jurídico de garantía de la privacidad y de la protección de datos es imprescindible partir de un diálogo constructivo entre el derecho y la técnica. Se ha dicho que las leyes sólo son posibles si van de la mano de la realidad social y tecnológica, no contra ellas[130].

En un apasionante diálogo entre Natalino IRTI y Emmanuele SEVERINO[131] el primero mantiene que la técnica puede ser capaz de condicionar el derecho, pero no es capaz de hacer desaparecer la diferencia entre "la regla y el regulado", es decir, entre derecho y técnica[132]. El Derecho "actúa siempre como principio ordenador respecto a la materia regulada"[133]. SEVERINO, sin embargo va mucho más allá. A partir de su tesis

de la "inevitabilidad del dominio de la técnica", mantiene que "el hombre está destinado a abandonar la ilusión de servirse de la técnica para ser feliz y está destinado a cumplir la voluntad de la técnica, que se aprovecha, para mayor gloria de su propia fuerza, de la vida y de la felicidad humana"[134]. En este escenario, las relaciones entre derecho y técnica se traducen en el hecho de que el primero se convierte en "medio de la técnica". "No será ya la voluntad jurídica la que se sirva de la técnica para elaborar un cierto ordenamiento jurídico, sino que será la técnica la que se sirva del afán de lucro y de la voluntad jurídica para poder incrementar hasta el infinito su fuerza… La técnica está destinada a convertirse en la regla y todo el resto en lo regulado"[135]. ¿Qué podemos hacer los juristas ante tan espectacular como inevitable reto? No hay más alternativa que reivindicar de nuevo el valor de los derechos fundamentales, y muy en particular de la dignidad y libertad del ser humano. En el diálogo, además, hay que dar entrada a un interlocutor más, la ética. Pero sin perder de vista que los avances tecnológicos son imparables y que tienen a su alcance obviar (torear, en términos taurinos y más gráficos aunque menos eruditos) las herramientas de que hoy dispone el derecho para luchar contra la invasión de nuestra privacidad. Pensemos solo, por ejemplo, que la lucha contra el *spam* es prácticamente imposible dado que la gran mayoría de los correos basura que recibimos provienen de países en los que no hay legislación garantizadora de la protección de datos, y eso cuando se acierta a identificar la fuente originaria del *spam*, algo casi siempre imposible[136]. Por ello es imprescindible establecer mecanismo internacionales eficaces contra los ataque a la privacidad; ataques que, como ya he dicho, no saben de fronteras. La era de la información, la era digital, insisto, ha superado hace ya mucho la división territorial de los viejos Estados.

También es imprescindible que todos estemos concienciados sobre los riesgos a que nuestra privacidad está sometida. Concienciados no es agobiados, desde luego, pero tampoco debemos resignarnos a carecer de privacidad o asumirlo como algo inevitable en la sociedad moderna.

Imaginemos que estamos tranquilamente en nuestras casas. Alguien entra y tras decirnos que no nos preocupemos y que sigamos con lo que estamos haciendo, van tomando nota del programa de televisión que estamos viendo, de la página web que estamos visitando y de las que hemos visitado, de la llamada telefónica que estamos haciendo y de las que hemos hecho y recibido en el último año. Por encima de nuestro hombro cotillean el texto del correo electrónico que estamos escribiendo y a quién se lo enviamos. Abren nuestra cartera y toman nota de los números de nuestras tarjetas de crédito, de nuestro DNI. Con parsimonia escrutan todos los movimientos de nuestras cuentas corrientes, las revistas a las que estamos suscritos, las estancias en hoteles que hemos efectuado, los viajes realizados. Van al cajón donde tenemos nuestros papeles de los médicos, nuestras radiografías, análisis de sangre; escanean todo y lo guardan. Salimos de

casa y nos siguen, a nuestro lado, sin dejarnos. Recibimos una llamada en nuestro móvil y colocan un dispositivo para escuchar y grabar la conversación. Decimos a nuestro vigilante que nos deje en paz, que nos deje sólo, y nos contesta que lo siente, que no está en nuestras manos consentir o no su presencia. Que él siempre estará.

No es ciencia ficción. No es una pesadilla. Es una realidad. Virtual, de vigilancia invisible, pero real. Nuestra vida, queramos o no, es o puede ser así.

Marlon BRANDO reclamaba la privacidad no como un mero derecho, sino como una absoluta necesidad[137]. De Greta GARBO son estas palabras: "nunca he dicho que quiero estar sola. Sólo he dicho que quiero poder estar sola. Esta es la diferencia"[138].

Quizá todavía estemos a tiempo de preservar nuestra privacidad. La solución no está ni sólo ni siempre en nuestras manos. Agudicemos el ingenio jurídico para, de la mano de la técnica pero no bajo su dictadura, encontrar soluciones ingeniosas y eficaces que nos permitan seguir siendo libres con dignidad.

Notas

1 El presente trabajo tiene su origen en la Lección Magistral que fui invitado a impartir con motivo de la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid en septiembre de 2008. Lo he revisado y actualizado para esta ocasión.

2 Planeta de Agostini, Barcelona, 2005. Pág. 187.

3 Ver Daniel J. SOLOVE, The Digital Person. Technology and Privacy in the Information Age, New York University Press, 2004, pág. 224. Se ha señalado que la fuente original de tal cita se desconoce dadas las fuertes críticas que por ella recibió McNealy: vid. Colin J. BENNETT y Charles D. RAAB, The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press, Cambridge-Londres, 2006, págs. 8 y 298.

4 Frase tomada de la Conferencia pronunciada en el marco de la IAPP Privacy Summit, 2007, Washington, 7 de marzo de 2007.

5 Ver José Antonio DIAZ ROJO, "Privacidad, ¿Neologismo o barbarismo?", en Espéculo. Revista de Estudios Literarios, nº 21, 2002. También en http://www.ucm.es/info/especulo/numero21/privaci.html.

6 Ver por ejemplo la STS, Sala 3ª, de 28 de mayo de 2008, donde el término privacidad se utiliza como sinónimo de carácter privado de una actividad en contraposición a su carácter público.

7 Véase la importante obra en cinco volúmenes dirigida por Philippe ARIÈS y George DUBY, Historia de la vida privada, Taurus, Madrid, 1987 a 1989.

8 "Does privacy Law work?", en Philip E. AGREE y Marc ROTENBERG (Eds.), Technology and Privacy: The new Landscape, The MIT Press, 1998, pág. 193.

9 "Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is", en "The Right to Privacy", recogido en Ferdinand David SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007), pág. 272. Citado

también por James Q. WHITMAN, "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

10 Sentencia del TEDH de 28 de enero de 2003, asunto Peck contra Reino Unido, epígrafe 57. El Tribunal añade: "The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. That Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see P.G. and J.H. v. the United Kingdom, no. 44787/98, § 56, ECHR 2001-IX...)".

11 Un buen resumen de las diferentes definiciones de privacidad en la doctina norteamericana puede verse en Markku LAUKKA, Criteria for Privacy Supporing System, http://www.tml.hut.fi/Research/TeSSA/Papers/Laukka/Laukka_nordsec2000.pdf.

12 Irwin ALTMAN, The Environment and Social Behavior. Privacy, Personal Space, Territory, Crowding, Brooks/Cole, Monterey, CA,1975.

13 Darhl M. PEDERSEN, "Psychological Functions of Privacy", en Journal of Environmental Psychology, nº 17, 1997, págs. 147-156.

14 Patricia Brierley NEWELL, "A Cross-Cultural Comparison of Privacy Definitions and Functions: a System Approach", en Journal of Environemntal Psychology, Volumen 18, nº 4, Diciembre 1998, páginas 351-371.

15 Una interesante exposición de algunos intentos de definir la privacidad puede consultarse en Daniel J. SOLOVE, Marc ROTEMBERG y Paul M. SCHWARTZ, Information Privacy Law, Aspen, New York, 2ª ed., 2006, págs. 40 y ss.

16 A Treatise on the Law of Torts or the Wrongs which arise independent of contract, Callaghan 2ª ed., Chicago, 1888, p. 29.

17 Harvard Law Review, Vol IV, 15 de diciembre de 1890, nº 5. El título completo del artículo es "The Right to Privacy (The implicit made explicit)". También se recoge en Ferdinand D. SCHOEMAN, Philosophical dimensions…., op. cit., págs. 75 y ss.. Hay edición bilingüe, italiano e inglés, editada por el Garante per la Protezione dei Dati Personali: Il Diritto alla Privacy. The Right to Privacy, Roma, 2005. Contiene una muy interesante "Introduzione". A tan importante artículo volvía a referirse no hace mucho Stefano RODOTA: Intervista su Privacy e Libertà, a cargo de Paolo CONTI, Editori Laterza, Roma-Bari, 2005, pp. 7 y ss.

18 Véase Stefano RODOTA, La vita e le regole. Tra diritto e non diritto, Feltrinelli, Milán, 2006, pág. 100.

19 Alan F. WESTIN, Privacy and Freedom, Atheneum, New York, 1967. Hay edición de 1970.

20 Como ha recordado Jan HOLVAST, "History of privacy", en Karl DE LEEUW y Jan BERGSTRA (eds.), The History of Information Security. A Comprehensive Handbook, Elsevier, Amsterdam, 2007, págs. 737 y ss.

21 Sobre el concepto, vid., por todos, Pablo LUCAS MURILLO DE LA CUEVA, El derecho a la autodeterminación informativa, Tecnos, Madrid, 1990 y, más recientemente, "La Constitución y el derecho a la autodeterminación informativa", en Cuadernos de Derecho Público, nº 19-20 (2003), monográfico sobre

Protección de Datos, págs. 27 y ss. También Ricard MARTINEZ, Una aproximación crítica a la autodeterminación informativa, Civitas, Madrid, 2004.

22 Lo íntimo, lo privado, lo público, Cuadernos de Transparencia, nº 6, IFAI, México D.F., 5ª ed., octubre 2008. También publicado en la Revista Claves de Razón Práctica, número 137, Madrid, noviembre 2003.

23 Privacy and Freedom, op. cit.

24 Hal ABELSON, Ken LEDDEN y Harry LEWIS, Blown to Bits. Your Life, Liberty and Happines after the Digital Explosion, Addison-Wesley, 2008, pág. 68.

25 Vid. M. LAUKKA, "Criteria for Privacy….", op. cit. Se basa en estudios de FUSILIER y HOYER, en TOLCHINSKY y otros, "Employee perception of invasion of Privacy", Journal of Applied Psychology, nº 66 (1981), págs. 308 y ss.

26 En el momento de escribir estas líneas no he podido comprobar la fecha exacta de la sentencia. Tomo la información del Diario EL PAIS, 3 de septiembre de 2008, pág. 27.

27 En particular, en su relación con la libertad de expresión e información. Sobre la diferencia entre libertad de expresión y libertad de información es sumamente clara la STS de 25 de febrero de 2008, cuyo fundamento jurídico cuarto merece la pena transcribir:

"CUARTO. - El derecho al honor y la libertad de expresión e información.

El art. 20.1 d) CE , en relación con el artículo 53.2 CE, reconoce como derecho fundamental especialmente protegido mediante los recursos de amparo constitucional y judicial el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión y el art. 18.1 CE reconoce con igual grado de protección el derecho al honor.

Cuando se produce una colisión entre ambos derechos debe prevalecer la protección del derecho a la información siempre que su objeto tenga interés general, es decir, verse sobre asunto de relevancia pública por la materia y por las personas y la información sea veraz (SSTS, entre otras, de 19 de julio de 2006, rec. 2448/2002, y 18 de julio de 2007, rec. 5623/2000, y SSTC 54/2004, de 15 de abril, ciento 58/2003, de 15 de septiembre y 61/2004, de 19 de abril).

La libertad de expresión, igualmente reconocida en el art. 20 CE, tiene un campo de acción más amplio que la libertad de información (SSTC 104/1986, de 17 de julio y 139/2007, de 4 de junio), porque en tanto ésta se refiere a la narración de hechos, la de expresión alude a la emisión de juicios personales y subjetivos, creencias, pensamientos y opiniones. Comprende la crítica de la conducta de otro, aun cuando sea desabrida y pueda molestar, inquietar o disgustar a aquel contra quien se dirige (SSTC 6/2000, de 17 de enero, F. 5; 49/2001, de 26 de febrero, F. 4; y 204/2001, de 15 de octubre, F. 4), pues así lo requieren el pluralismo, la tolerancia y el espíritu de apertura, sin los cuales no existe «sociedad democrática» (SSTEDH de 23 de abril de 1992, Castells c. España, § 42, y de 29 de febrero de 2000, Fuentes Bobo c. España, § 43). Fuera del ámbito de protección de dicho derecho se sitúan las frases y expresiones ultrajantes u ofensivas, sin relación con las ideas u opiniones que se expongan, y por tanto, innecesarias a este propósito, dado que el art. 20.1 a) CE no reconoce un pretendido derecho al insulto, que sería, por lo demás, incompatible con la norma fundamental (SSTC 204/1997, de 25 de noviembre, F. 2; 134/1999, de 15 de julio, F. 3; 6/2000, de 17 de enero, F. 5; 11/2000, de 17 de enero, F. 7; 110/2000, de 5 de mayo, F. 8; 297/2000, de 11 de diciembre, F. 7; 49/2001, de 26 de febrero, F. 5; y 148/2001, de 15 de octubre, F. 4, SSTC 127/2004, de 19 de julio, 198/2004, de 15 de noviembre, y 39/2005, de 28 de febrero).

Con carácter general, los requisitos que debe reunir la información para que la libertad inherente a ella deba ser considerada prevalente respecto al derecho al honor son, en suma, los de interés general, veracidad y exposición no injuriosa o insultante".

28 S.M. JOURARD, "Some Psychological aspects of Privacy", Law and Contemporary Problems, nº 31 (1966), págs. 307 y ss. P. B. NEWELL, "A Systems Model of Privacy", Journal of Environmental Psichology, nº 14 (1994), págs. 65 y ss. A ellos se refiere LAUKKA, "Criteria....", op. cit.

29 "On Privacy (The American Dream: what happened to it?)", edición bilingüe en ingles e italiano, editado por el Garante per la protezione dei dati personali, en el Volumen Privacy, Roma, 2001. Incluye tambíen un interesante Ensayo de Piero BOITANI, "Il Paradiso perduto della Privacy", págs. 58 y ss.

30 LAUKKA, op. ult. cit, en base a las opiniones de PEDERSEN, NEWELL y KELVIN.

31 http://blog.wired.com/27bstroke6/surveillance/index.html

32 Vid sobre todo "La defensa frente al ruido ante el Tribunal Constitucional", en Revista de Administración Pública, nº 115, págs. 214 y ss., y "Medio ambiente sonoro", en ESTEVE PARDO (Coord.), Derecho del medio ambiente y Administración Local, Civitas-Diputación de Barcelona, 1996, págs. 227 y ss. Véanse asimismo Alberto DIAZ-ROMERAL, "La protección del medio ambiente urbano: la contaminación por el ruido en las ciudades y la sostenibilidad en el desarrollo urbano"; Patrica VALCARCEL, "Contaminación acústica y desarrollo sostenible en el marco de la actividad aeroportuaria. Algunas soluciones. En particular: ¿Servidumbres acústicas en la lucah contra el ruido?", ambos trabajos en PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 255 y ss., y 207 y ss., respectivamente.

33 "Il corpo e il post-umano", texto original amablemente cedido por el autor, pág. 5.

34 The Republic of Choice. Law, Authority and Culture, Harvard University Press, Cambridge, Mass., 1990, pág. 184.

35 La protection de la vie privée et des autres biens de la personnalité, Bruylant, Bruselas-Paris, 1990, pág. 167.

36 LAUKKA, "Criteria…", op. cit.

37 A la íntima relación entre dignidad y privacidad se ha referido ESCALANTE GONZALBO, El derecho a la privacidad, Cuadernos de Transparencia, nº 2, IFAI, México D.F., 6ª ed., octubre 2008.

38 "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

39 "The two Western Cultures of Privacy....", op cit., págs. 10 a 13 del texto disponible en http://papers.ssrn.com/abstract=476041.

40 Entre la doctrina norteamericana ha resaltado la estrecha relación entre privacidad y dignidad Edgard J. BLOUSTEIN: "Privacy as an aspect of human dignity. An Answer to Dean Prosser", *New York University Law Review*, nº 39 (1964), págs. 962 y ss., también recogido en SCHOEMAN, *Philosophical Dimensions.…*, op. cit., págs. 156 y ss.

41 Recientemente en *La vita e le regole.…*, op. cit., págs. 103 y ss.

42 Me he referido a tales tensiones en relación con la protección de datos, recientemente en "El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos", en PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, Madrid, 2008, págs. 91 y ss.

43 RODOTA se ha referido hace poco también a los riesgos que para la privacidad supone el mercado y la lucha por la seguridad: "Innovación, nuevas tecnologías, participación política y protección de datos. Un equilibrio para mejorar la democracia", conferencia impartida en los Cursos de Verano de la Universidad

del País Vasco, en el marco del Seminario *El acceso a la Información Parlamentaria*, impartida el 28 de julio de 2008. Utilizo el texto original que amablemente me ha facilitado el autor.

[44] Recientemente en "Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Boletín del Ilustre Colegio de Abogados de Madrid*, monográfico sobre *La Protección de Datos (I)*, núm. 36, 3ª época, abril 2007, págs. 13 y ss.

[45] Sobre ello vid. N. IRTI y E. SEVERINO *Dialogo su Diritto e Tecnica*, Editori Laterza, Roma-Bari, 2001; S. RODOTA *Tecnologie e diritti*, Il Mulino, Bari, 1995; *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información,* Losada, Buenos Aires, 2000; J.L. PIÑAR MAÑAS, "Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una Reflexión", en T.R. FERNANDEZ y otros, *La Autorización administrativa. La Administración Electrónica. La Enseñanza del Derecho Administrativo*, Aranzadi, 2007.

[46] Los llamados RFID, "identificadores por radiofrecuencia"

[47] El coste económico de los avances tecnológicos y de nuevos dispositivos es cada vez menor, lo que facilita aún más su uso e implantación. Gordon MOORE expuso su visión del futuro de las tecnologías en un breve artículo, de apenas cuatro páginas, publicado en 1965, en términos que más adelante se conocerían (y así se conocen hoy) como la "Ley de Moore". Avanzó entonces que "The complexity for minimum component costs has increased at a rate of roughly a factor of two per year ..... Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years": "Cramming more components onto integrated circuits", *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

[48] Vid. CASTELLS, Manuel, *La era de la información. Vol. 1, La sociedad red*, Alianza Editorial, Madrid, 3ª ed., 2005, pág. 70.

[49] El incremento de las cámaras de vigilancia en las calles es ya tan alarmante como algo desgraciadamente normal. Plantea problemas de gran importancia sobre la privacidad y la protección de datos. Vid. el *Dictamen de la Comisión de Venecia sobre la videovigilancia en lugares públicos por parte de las autoridades públicas y la protección de los derechos humanos*, en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 427 y ss. La Agencia Española de Protección de Datos ha dictado la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o de videocámaras (*BOE* de 12 de diciembre de 2006). La Conferencia Internacional de Autoridades de Protección de Datos celebrada en Londres durante los días 1 a 3 de noviembre de 2006 tuvo por tema precisamente la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos.

[50] Las siguientes reflexiones están tomadas de mi trabajo "Seguridad, Transparencia y Protección de Datos: el futuro de un necesario e incierto equilibrio", 2008.

51 Isaac ASIMOV, Los Límites de la Fundación, pág. 64 de la edición disponible en www.eBooket.com.

52 Así nos lo ha recordado RODOTA, "Il corpo…", op. cit., pág. 10.

53 Sobre ello recientemente vid. S. RODOTA La vita e le regole..... op. cit., págs. 174 y ss. Ellen ALDERMAN y Caroline KENNEDY consideraban ya hace más de diez años que la protección de la información genética era sin duda el tema más importante en el futuro de la protección de datos: The Right to

Privacy, Vintage Books, New York, 1997, pág. 336.

54 Véase Michael KINSLEY, "Inherited Properties. The U.S. Congress voted to ban genetic discrimination. But how much equality do Americans Really want?", en Time, 19 de mayo de 2008, pág. 60.

55 Sobre ello vid. Andrea KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001. Es esclarecedor el trabajo en este libro de James A. GOLDSTON, "Race and Ethnic Data: a Missing Resource in the Fight against Discrimination", págs. 19 y ss.

56 http://technology.timesonline.co.uk/tol/news/tech_and_web/article3193223.ece. The Times, 16 de enero de 2008.

57 Ver por ejemplo K.W. BOWYER, "Face recognition technology: security versus privacy", Technology and Society Magazine, IEEE, Primavera de 2004, Volumen 23, páginas 9 y ss. Jay STANLEY y Barry STEINHARDT. "Face-Recognition Technology Threatens Individual Privacy." Opposing Viewpoints: Civil Liberties. Ed. Tamara L. Roleff. San Diego: Greenhaven Press, 2004. Ver http://www.enotes.com/civil-liberties-article/41394. Ver un ejemplo de tal sistema en HOLTZMAN, Privacy lost. How Technology is endangering your Privacy, Jossey-Bass, San Francisco, 2006, pág. 6.

58 Ver Tim KINDBERG y Timothy JONES "Merolyn the Phone":A Study of bluetooth Naming Practices, en http://www.cs.bath.ac.uk/pervasive/publications/ubicomp07.pdf.

59 El término se utilizó por primera vez en torno a 1988 por Mark WEISER. Ver su trabajo The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html. Ver Reijo AARNIO, "Data Protection and New Technologies: "Ubiquitous Computing"", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss. Asimismo Marc LANGHEINRICH, "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems", 2001, en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf

60 CLIPPINGER, *A Crowd of one. . The Future of Individual Identity*, Public Affaires, New York, 2007, págs. 28 y 32.

61 http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP. Información sobre los fallos de seguridad producidos en Estados Unidos puede también obtenerse en www.attrition.org/security/dataloss.html y en la web de la National Association of Information Destruction -- NAIDDirect, www.naidonline.org

62 El escándalo de la venta ilegal de datos en Alemana ha puesto en marcha una propuesta para reformar la ley de protección de datos para hacerla más exigente y garantista. Con la nueva ley, cuyo primer texto quiere tenerse para el próximo mes de noviembre, se exigiirá el consentimiento expreso de los interesados para la cesión de sus datos con fines comerciales. Hasta ahora, los datos personales de clientes pueden ser cedidos con tales fines si el afectado no se ha opuesto expresamente: http://www.dw-world.de/dw/article/0,2144,3576639,00.html

63 *Vigilar y castigar*, Ed. Siglo XXI, México, 1976. A ello se ha referido también Daniel J. SOLOVE, *The Digital Person. op. cit.*, págs. 30-31.

64 Vid. BENNETT y RAAB, *The Governance*…., op. cit., págs. 16 y ss.

65 Reg WHITAKER, *The End of Privacy: how Total Surveillance is Becoming a Reality*, New Press, New York, 1999. Cit. por BENNETT y RAAB, op. ult. cit, pág. 338. Existe traducción al español de la obra de WHITAKER: *El fin de la privacidad. Como la vigilancia total se está convirtiendo en realidad*, Paidos, 1999.

66 Vid. David. H. HOLTZMAN, *Privacy lost. ….. op. cit.,* págs. 265 y ss.

[67] J. ROSEN, *The Unwanted Gaze. The Destruction of Privacy in America*, Vintage Books, New York, 2000.

[68] Vid. R. SMITH, *War Stories: Accounts of Persons Victimized by Invasions of Privacy*, Privacy Journal, 1993. Cit. por BENNETT y RABB, *Governance of Privacy...*, op. cit., pág. 7.

[69] *Blown to Bits….. op. cit.* Se trata de un muy interesante libro con reveladoras reflexiones acerca del futuro que pueden depararnos las nuevas tecnologías.

[70] Simson GARFINKEL, *Database Nation: the Death of Privacy in 21st Century*, O'Reilly Media, Sebastopol, California, 2001.

[71] *The limits of Privacy*, Basic Books, New York, 1999. A lo largo de toda la obra se exponen los *detrimental effects* de un exceso de privacidad y se proponen soluciones alternativas que pasan, como digo en el texto, por una definición de la privacidad en términos "comunitarios", dando mayor importancia al interés general.

[72] Vid. David. H. HOLTZMAN, *Privacy lost. .....* Op. cit.

[73] *El miedo a la libertad*, utilizo la edición de Paidos, Buenos Aires, 4ª ed., 1978, pág. 308.

[74] Op. Ult. Cit., pág. 302.

[75] "Il corpo...", op. Cit., pág. 9.

[76] *La vita e le regole…*, op. cit., pág. 114. Y advierte RODOTA: "Se libertá e spontaneità si rifugeranno soltanto nei nostri spazi rigorosamente intimi e privati, saremo portati a considerare lontano e ostile tutto quello che stá nel mondo esterno. Qui può essere il germe di nuovi conflitti, e dunque di una permanente e pi`radicale insicurezza".

[77] LANGHEINRICH, "Privacy by Design….", op. cit., pág. 7.

[78] Al que sigue LAUKKA, op. ult. cit.

[79] El concepto de "information privacy" se acerca mucho, en su contenido, al de protección de datos. Véase por todos SOLOVE, ROTEMBERG y SCHWARTZ, *Information Privacy Law*, op. cit. Como señalan los autores, "Information Privacy concerns the collection, use, and disclosure of personal information" (pág. 1). Como señalan BENNETT y RAAB, los concpetos de "information privacy" y "protección de datos" surgieron casi al mismo tiempo en los años sesenta y setenta: *The Governance….*, op. cit., pág. 8.

[80] Así lo ha apuntado Markku LAUKKA "Criteria for privacy…", op. cit.

[81] *A Treatise on the Law of Torts ….."*, *op. cit.* p. 29.

[82] Vol IV, 15 de diciembre de 1890, nº 5, op. cit.

[83] Lo cual es importante, pues el artículo de WARREN y BRANDEIS llama la atención acerca de la necesidad de que el derecho reaccione frente a los ataques a la privacidad no sólo por parte del Gobierno, sino también desde sujetos privados. E. ALDERMAN y C. KENNEDY han llamado la atención acerca de ello, señalando que la Constitución americana sólo protege a los individuos frente a la acción del Gobierno, lo que refuerza el alcance novedoso de la aportación hecha por aquéllos: *The Right to Privacy,* op. cit., pág. 155.

[84] Ver Amitai ETZIONI, *The limits of Privacy*, op. cit, pág. 190.

[85] Ya incluso en 1890, es decir el mismo año en que se publicó el repetido artículo, como recuerda PROSSER en "Privacy (A legal Analysis)", *California Law Review*, nº 48 (1960), págs. 338 y ss., también recogido en Ferdinand D. SCHOEMAN, *Philosophical dimensions….*, op. cit., págs. 104 y ss, y en par-

ticular, pág. 105. Puede consultarse una amplia selección de casos a lo largo de toda la obra de SOLOVE, ROTENBERG y SCWARTZ, *Information Privacy Law,* op. cit., y en ALDERMAN y KENNEDY, *The Right to Privacy*, op. cit., *in toto*.

[86] William PROSSER, que es muy crítico con el artículo de WARREN y BRANDEIS, distingue hasta cuatro diferentes daños derivados del ataque a la privacidad: la intrusión en los asuntos privados del afectado; revelar información privada referente al mismo; la posibilidad de ofrecer al público una falsa imagen del afectado ("false light in the public eye"); y la apropiación de información de aquél: "Privacy (A legal Analysis)", op. cit. Vid. ALDERMAN y KENNEDY, *The Right to Privacy*, op. cit., págs. 155-156; BENNETT y RAAB, *The Governance...*, op. cit., pág. 126. HOLTZMAN analiza "the four torts" propuestos por PROSSER en *Privacy Lost*…., op. cit., págs. 94 y ss., así como SOLOVE en *The Digital Person*…., op. cit., págs. 57 y ss. Edgard J. BLOUSTEIN ha sido, por su parte, crítico con las posiciones de PROSSER: "Privacy as an aspect of human dignity ….", op. cit.

[87] "*Artículo 12.* Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

[88] "*Artículo 11.* Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. 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. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

89 Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques.

90 "Artículo 8. Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[91] *DOCE* C 364-1, de 18 de diciembre de 2000.

[92] U.S. Department of Health , Education & Welfare, *Records, Computeres and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data System*. Vid. SOLOVE, ROTENBERG y SCHWARTZ, *Information Privacy Law*, op. cit., págs. 35-36 y 577-578.

[93] BENNETT y RAAB, *The Governance…*, op. cit., pág. 121.

[94] En la XXVII Conferencia Internacional de Autoridades de Protección de Datos celebrada en Montreux, Suiza, los días 13 a 15 de septiembre de 2005 se aprobó una Declaración Final sobre « *The protection of personal data and privacy in a globalised world : a universal right respecting diversities* », en la que se hace una referencia expresa a los principios del derecho a al protección de datos:

Recognising that the principles of data protection derive from international legal binding and non binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal

Data Files, the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data and the Asia Pacific Economic Cooperation Privacy Framework,

17. Recalling that these principles are in particular the following:

- Principle of lawful and fair data collection and processing,
- Principle of accuracy,
- Principle of purpose-specification and -limitation,
- Principle of proportionality,
- Principle of transparency,
- Principle of individual participation and in particular the guarantee of the right of access of the person concerned,
- Principle of non-discrimination,
- Principle of data security,
- Principle of responsibility,
- Principle of independent supervision and legal sanction,
- Principle of adequate level of protection in case of transborder flows of personal data.

95 Directiva 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

96 La bibliografía sobre la Directiva es abundantísima. Vid., recientemente, Christopher KUNNER, *European Data Protection Law: Corporate Compliance and Regulation*, Oxford University Press, 2ª ed., 2007.

97 Vid. PIÑAR MAÑAS "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre *Protección de Datos*, págs. 45 y ss. Ha sido traducido al inglés: "ECJ Case Law on the Right to Protection of Personal Data. Part. 1", *BNA International. World Data Protection Report*, Volumen 6, Nº 1, enero 2006. Págs. 3-11; La segunda parte, en la misma Revista, Volumen 6, Nº 2. Febrero, 2006. Págs. 23-32.

98 En la interpretación y desarrollo de la Directiva ha tenido y tiene un protagonismo esencial la labor del llamado Grupo del Artículo 29 de la Directiva, *"Art. 29 Working Party"*, así denominado por haber sido creado por el artículo 29 de la Directiva. Según el nº 1 de este precepto, "Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, …. que tendrá carácter consultivo e independiente". En el repetido artículo 29 y en el 30 se establece su naturaleza, régimen y funciones. Sobre el Grupo del Artrículo 29 vid. Peter SCHAAR, "The Work of the Article 29 Working Party", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 107 y ss. También desarrolla un importante cometido en lo que se refiere al tratamiento de datos por parte de las Instituciones europeas, el Supervisor Europeo de Protección de Datos. Sobre esta figura vid. Peter J. HUSTINX, "Data Protection in the European Institutions", en VARIOS AUTORES, *Proccedings of the First European Congress…., op. cit.,* págs. 113 y ss; HIJMANS, Hielke, "The European data protection supervisor: the institutions of the EC controlled by and independent authority", *Common Market Law Review*. Vol. 43 (2006), nº. 5, págs. 1313-1342.

99 De aquél año son las importantes sentencias dictadas en los asuntos Amann contra Suiza, de 16 de febrero de 2000 y Rotaru contra Rumania, de 4 de mayo de 2000.

100 "Artículo 7. Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

[101] "Artículo 8. Protección de datos de carácter personal.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[102] A ello me he referido en "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea. Revista Parlamentaria de la Asamblea de Madrid*, nº 13, dic. 2005, pág. 21 y ss.

[103] "Privacy and the Future: Some Opening Reflections", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, pág. 20.

[104] LEY ORGÁNICA 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, firmado en la capital portuguesa el 13 de diciembre de 2007.

El artículo 2º es del siguiente tenor: "Artículo 2. Carta de los Derechos Fundamentales de la Unión Europea.

A tenor de lo dispuesto en el párrafo segundo del artículo 10 de la Constitución española y en el apartado 8 del artículo 1 del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta de los Derechos Fundamentales publicada en el «Diario Oficial de la Unión Europea» de 14 de diciembre de 2007, cuyo texto íntegro se reproduce a continuación: (a continuación el texto íntegro de la Carta).

[105] 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). 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. Merece la pena recordar también las Sentencias constitucionales 110/84, 254/93, 143/94, 94/98, 11/98, 144/99 y 202/99 que resuelven básicamente recursos de Amparo, frente a tratamientos ilícitos, contrarios al principio de "autodeterminación informativa", que se traduce en el Derecho de control sobre los datos relativos a la propia persona o, lo que es lo mismo, el Derecho a controlar el uso de los mismos datos personales por parte de su titular. Así las sentencias 144/99 y 202/1999, dictadas frente a la utilización por RENFE de los datos de diversos trabajadores relativos a su afiliación sindical. Resoluciones anteriores relacionan el Derecho a la protección de datos de carácter personal con el Derecho a la intimidad (SSTC 143/1994, 254/1993 y 110/1984), proclamando con carácter general *"El reconocimiento global de un Derecho a la intimidad o a la vida privada que abarque su defensa frente las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida"*. En particular, la STC 254/1993 señala que la Constitución de 1978 ha incorporado el "Derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos". Añade que no es posible aceptar que "el Derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados.... son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución, y que dan vida al Derecho fundamental a la intimidad, resulten real y

efectivamente protegidos". Para un análisis de la jurisprudencia del Tribunal Constitucional en la materia, vid. E. GUICHOT, *Datos personales y Administración Pública*, Thomson-Civitas, 2005, págs. 68 y ss.

[106] La doctrina del Tribunal Constitucional ha sido asumida totalmente por los Tribunales. Véase la magnífica obra coordinada por Carlos LESMES SERRANO, *La ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008. Como ejemplo de tal asunción, he aquí un párrafo de la reciente Sentencia del Tribunal Supremo de 26 de junio de 2008, en el que además se distingue una vez más entre intimidad y protección de datos: "En nuestra Sentencia de 13 de Septiembre de 2.002 (Rec.92/1999) nos fijamos en que el *art. 18* de la Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen en su párrafo 1º y en su apartado 4º consagra lo que: "la jurisprudencia constitucional ha denominado el "derecho fundamental a la protección de datos personales", derecho fundamental estrechamente conectado con el reconocido en el apartado 1º del mismo precepto, aunque con un contenido propio y diferenciado, que –en palabras de la STC 292/2000, de 30 de noviembre - "impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información", habiéndose de tener en cuenta que, como dice esta misma sentencia constitucional, "el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el *art. 18.1 CE* otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"; de forma que, en conclusión, "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

[107] Las siguientes consideraciones ya las he expuesto en "El derecho fundamental a la protección de dastos. Contenido esencial….", op. cit., págs. 26 y ss.

[108] Fundamentos Jurídicos segundos de ambas Sentencias.

[109] Sobre la importancia del artículo 18.4 en relación con el derecho a la protección de datos, vid recientemente el "Prólogo" de Tomás DE LA QUADRA SALCEDO, al libro coordinado por Juan ZABIA DE LA MATA, *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008, págs. 7 y ss.

[110] Ley Orgánica 3/1985, de 29 de mayo, Ley Orgánica 5/1992, de 29 de octubre, y Ley Orgánica 10/1995, de 23 de noviembre.

[111] Sobre el Reglamento vid Juan ZABIA DE LA MATA (Coord.), *Protección de Datos. Comentarios al Reglamento*, op. cit. PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, op. cit. PIÑAR MAÑAS, "El porqué de un reglamento de desarrollo de la Ley Orgánica de Protección de Datos", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 9 y ss.; PIÑAR MAÑAS, "Strengthen-

ing Legal Certainty: New Regulations Developing the LOPD (Organic Data Protection Act)", en VARIOS AUTORES, *Proccedings of the First European Congress…,* págs. 33 y ss.; Antonio TRONCOSO, "Regulatory Development of the LOPD", en VARIOS AUTORES, *Proccedings…., op. cit,* págs. 51 y ss.; Belén VELEIRO, "Regulatory Development of the LOPD from a Business Perspective", en VARIOS AUTORES, *Proccedings ….op. cit.*, págs. 81 y ss. Juan Manuel FERNANDEZ LOPEZ, "Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007), págs. 35 y ss.

[112] Gran parte de ellas pueden consultarse en el *Código de Protección de Datos*, edición preparada por la Agencia Española de Protección de Datos, Ed. La Ley, Madrid, 2005. Deben tenerse especialmente en cuenta la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales; la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos; la Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos; la Ley Orgánica 10/2007, de 8 de octubre, reguladora de bases de datos policiales sobre identificadores obtenidos a partir del ADN; la Ley 30/2007, de contratos del sector público; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, o la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

[113] *The Governance of Privacy….*, op. cit., pág. 19.

[114] "The good news is that there is legal protection for privacy. The bad news is that it doesn't work particularly well": *Privacy Lost…*, op. cit., pág. 119.

[115] James RULE y otros, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, New York, 1980, págs. 68 y ss.

[116] Cit. por BENNETT y RAAB, *The Governance….*, op. cit., pág. 147.

[117] "Does Privacy Law work?", op. cit., págs. 193 y ss.

[118] A esta Sentencia se ha referido también recientemente RODOTA, "Innovación, nuevas tecnologías, ….", op. cit.

[119] Epígrafe 181 de la Sentencia.

[120] Epígrafe 203.

[121] Sobre los instrumentos de autorregulación, vid., entre otros, BENNETT y RAAB, *The Governance….*, op. cit., págs. 151 y ss.

[122] Vid los comentarios de María José BLANCO ANTON a los artículos citados en Juan ZABIA DE LA MATA (Coord.), *Protección de Datos. Comentarios al Reglamento*, op. cit., págs. 635 y ss.

[123] A ello me he referido con cierta extensión en "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", op. cit.

[124] A ello me he referido ya en "El derecho fundamental a la protección de datos. Contenido esencial…", op. cit., pág. 91.

[125] Sobre la "evaluation of impact" vid. BENNETT y RAAB, *Governance of Privacy…."*, op. cit., págs. 235 y ss. A la evaluación del impacto se ha referido también RODOTA, en "Innovación, nuevas tecnologías, ….", op. cit.

[126] WHITE, "The use of Privacy Impacts Assessments in Canada", *Privacy Files*, nº 4, 2001, pág. 2.

127 Vid. Marc LANGHEINRICH, Privacy by Design -Principles of Privacy- Aware Ubiquitous Systems, op. cit. El Supervisor Europeo de Protección de Datos ha resaltado la necesidad de reforzar ese principio en su Documento de 28 de abril de 2008 "The EDPS and EU Research and Technological Development", que puede consultarse en la dirección http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf.

128 Marit HANSEN, Ari SCHWARTZAND y Alissa COOPER, "Privacy and Identity Management", *IEEE Security & Privacy*, Marzo-abril, 2008, pág. 39.

129 Sobre la necesidad de que los soportes y sistemas de información tengan en cuenta las medidas de seguridad necesarias para garantizar la protección de datos, véanse los artículos 5.2 y 79 y ss. del Reglamento de Desarrollo de la LOPD, aprobado por Real Decreto 1720/2007. Asimismo, la Disposición Adicional única del Reglamento, en virtud de la cual "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 de acuerdo con lo establecido en el título VIII de este Reglamento".

130 M. LANGHEINRICH, *Privacy by Design….*, op. cit., pág. 16. Y afirma: "Si ciertas previsiones legales no pueden imponerse , es necesario encontrar soluciones tecnológicas o procedimentales alternativas, o la ley deberá cambiarse"

131 IRTI, Natalino, y SEVERINO, Emanuele, *Dialogo su Diritto e Tecnica*, Editori Laterza, Roma-Bari, 2001

132 Op. cit., pág. 14.

133 "Si pone sempre come principio ordinatore rispetto alla materia regolata". Op. cit., pág. 15.

134 "L'uomo è destinato ad abbandonare l'illusione di servirsi della técnica per essere felice, ed è destinato a fare la volontà della técnica, che si serve, per la gloria della propria potenza, della vita e della felicità umane". Op. cit., pág. 39.

135 "Non sará più la volontà giuridica a servirsi della técnica per realizzare un certo ordinamento giuridico, ma sará la técnica a servirsi della volontà di profitto e della volontà giuridica per incrementare all'infinito la propria potenza... La técnica è destinata a diventare al regola e tutto il resto il regolato". Id. Pág. 80.

136 Para luchar contra el spam y otras amenazas internacionales para la privacidad se constituyó en Londres, el 11 de octubre de 2004 el llamado London Action Plan, integrado por representantes de más de 27 países. Vid. http://www.londonactionplan.org/

137 "Privacy is not something that I'm merely entitled to; it's an absolute prerequisite". Cit. Por David H. HOLTZMAN, Privacy lost: How Technology….., pág. 3.

138 "I never said, "I want to be alone". I only said "I want to be left alone". There is all the difference". Cit. Por David H. HOLTZMAN, *Privacy lost....*, pág. 211. La cita original está tomada de la película Gran Hotel. También citada por RODOTA, *La vita e le regole….*, op. cit., pág. 99.

Bibliografia utilizada y citada

AARNIO, "Data Protection and New Technologies: "Ubiquitous Computing"", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss.

ABELSON, LEDDEN y LEWIS, Blown to Bits. Your Life, Liberty and Happines after the Digital Explosion, Addison-Wesley, 2008.

Agencia Española de Protección de Datos, Código de Protección de Datos, Ed. La Ley, Madrid, 2005.

ALDERMAN y KENNEDY, The Right to Privacy, Vintage Books, New York, 1997.

ALTMAN, The Environment and Social Behavior. Privacy, Personal Space, Territory, Crowding, Brooks/Cole, Monterrey, CA,1975.

ARIÈS y DUBY, Historia de la vida privada, Taurus, Madrid, 1987 a 1989.

ASIMOV, Los Límites de la Fundación, edición disponible en www.eBooket.com.

BENNETT y RAAB, The Governance of Privacy. Policy Instruments in Global Perspective, The MIT Press, Cambridge-Londres, 2006.

BLANCO ANTON, Comentarios a los artículos 71 a 78 en ZABIA DE LA MATA (Coord.), Protección de Datos. Comentarios al Reglamento, Lex Nova, Valladolid, 2008., págs. 635 y ss.

BLOUSTEIN: "Privacy as an aspect of human dignity. An Answer to Dean Prosser", New York University Law Review, nº 39 (1964), págs. 962 y ss. También recogido en SCHOEMAN, Philosophical Dimensions…., págs. 156 y ss.

BOITANI, "Il Paradiso perduto della Privacy", en Garante per la protezione dei dati personali, Privacy, Roma, 2001págs. 58 y ss.

BOWYER, "Face Recognition Technology: Security Versus Privacy", Technology and Society Magazine, IEEE, Primavera de 2004, Volumen 23, páginas 9 y ss.

CASTELLS, La era de la información. Vol. 1, La sociedad red, Alianza Editorial, Madrid, 3ª ed., 2005.

CLIPPINGER, A Crowd of one. The Future of Individual Identity, Public Affaires, New York, 2007

COOLEY, A Treatise on the Law of Torts or the Wrongs which arise independent of contract, Callaghan 2ª ed., Chicago, 1888.

DE LA QUADRA SALCEDO, "Prólogo" al libro coordinado ZABIA DE LA MATA, Protección de datos. Comentarios al Reglamento, Lex Nova, págs. 7 y ss.

DE LEEUW y BERGSTRA (eds.), *The History of Information Security. A Comprehensive Handbook*, Elsevier, Amsterdam, 2007

DIAZ ROJO, "Privacidad, ¿Neologismo o barbarismo?", en Espéculo. Revista de Estudios Literarios, nº 21, 2002. También en http://www.ucm.es/info/especulo/numero21/privaci.html.

DIAZ-ROMERAL, "La protección del medio ambiente urbano: la contaminación por el ruido en las ciudades y la sostenibilidad en el desarrollo urbano"; PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 255 y ss.

ESCALANTE GONZALBO, El derecho a la privacidad, Cuadernos de Transparencia, nº 2, IFAI, México D.F., 6ª ed., octubre 2008.

ETZIONI, The limits of Privacy, Basic Books, New York, 1999.

FAULKNER, "On Privacy (The American Dream: what happened to it?)", edición bilingüe en ingles e italiano, editado por el Garante per la protezione dei dati personali, en el Volumen Privacy, Roma, 2001.

FERNANDEZ LOPEZ, "Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", en Revista Española de Protección de Datos, nº 3 (julio-diciembre 2007), págs. 35 y ss.

FOUCAULT, Vigilar y castigar, Ed. Siglo XXI, México, 1976.

FRIEDMAN, The Republic of Choice. Law, Authority and Culture, Harvard University Press, Cambridge, Mass., 1990.

FROMM, El miedo a la libertad, he utilizado la edición de Paidos, Buenos Aires, 4ª ed., 1978

Garante per la Protezione dei Dati Personali: Privacy, Roma, 2001.

Il Diritto alla Privacy. The Right to Privacy, Roma, 2005.

GARFINKEL, Database Nation: the Death of Privacy in 21st Century, O'Reilly Media, Sebastopol, California, 2001.

GARZON VALDES, Lo íntimo, lo privado, lo público, Cuadernos de Transparencia, nº 6, IFAI, México D.F., 5ª ed., octubre 2008. También publicado en la Revista Claves de Razón Práctica, número 137, Madrid, noviembre 2003.

GELLMAN, "Does privacy Law work?", en Philip E. AGREE y Marc ROTENBERG (Eds.), Technology and Privacy: The new Landscape, The MIT Press, 1998, pág. 193.

GOLDSTON, "Race and Ethnic Data: a Missing Resource in the Fight against Discrimination", en Andrea KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001págs. 19 y ss.

GUICHOT, Datos personales y Administración Pública, Thomson-Civitas, 2005.

HANSEN, SCHWARTZAND y COOPER, "Privacy and Identity Management", IEEE Security & Privacy, Marzo-abril, 2008, págs. 38 y ss.

HIJMANS, "The European data protection supervisor: the institutions of the EC controlled by and independent authority", Common market law review. Vol. 43 (2006), nº. 5, págs. 1313-1342.

HOLTZMAN, Privacy lost. How Technology is endangering your Privacy, Jossey-Bass, San Francisco, 2006.

HOLVAST, "History of privacy", en Karl DE LEEUW y Jan BERGSTRA (eds.), The History of Information Security. A Comprehensive Handbook, Elsevier, Amsterdam, 2007

HUSTINX, "Data Protection in the European Institutions", VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 113 y ss

IRTI y SEVERINO Dialogo su Diritto e Tecnica, Editori Laterza, Roma-Bari, 2001.

JOURARD, "Some Psychological aspects of Privacy", Law and Contemporary Problems, nº 31 (1966), págs. 307 y ss.

KINDBERG y JONES "Merolyn the Phone":A Study of bluetooth Naming Practices, en http://www.cs.bath.ac.uk/pervasive/publications/ubicomp07.pdf

KINSLEY, "Inherited Properties. The U.S. Congress voted to ban genetic discrimination. But how much equality do Americans Really want?", en Time, 19 de mayo de 2008, pág. 60.

KRIZSÁN (Ed.), Ethnic Monitoring and Data Protection. The European Context, CPS Books, Budapest, 2001.

KUNNER, European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, 2ª ed., 2007.

LANGHEINRICH, "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems", 2001, en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf

LAUKKA, Criteria for Privacy Supporing System, http://www.tml.hut.fi/Research/TeSSA/Papers/Laukka/Laukka_nordsec2000.pdf

LUCAS MURILLO DE LA CUEVA:

El derecho a la autodeterminación informativa, Tecnos, Madrid, 1990

"La construcción del derecho a la autodeterminación informativa", *Revista de Estudios Políticos*, nº 104, 1999.

"La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, nº 19-20 (2003), monográfico sobre *Protección de Datos*, págs. 27 y ss.

MARTIN-RETORTILLO:

"La defensa frente al ruido ante el Tribunal Constitucional", en *Revista de Administración Pública*, nº 115, págs. 214 y ss.,

"Medio ambiente sonoro", en ESTEVE PARDO (Coord.), *Derecho del medio ambiente y Administración Local*, Civitas-Diputación de Barcelona, 1996, págs. 227 y ss

MARTINEZ, *Una aproximación crítica a la autodeterminación informativa*, Civitas, Madrid, 2004.

McNEALY, Conferencia pronunciada en el marco de la *IAPP Privacy Summit, 2007*, Washington, 7 de marzo de 2007.

MOORE "Cramming more components onto integrated circuits", *Electronics*, Volumen 38, Número 8, 19 de Abril de 1965.

NEWELL:

- "A Cross-Cultural Comparison of Privacy Definitions and Functions: a System Approach", en *Journal of Environemntal Psychology*, Volumen 18, nº 4, Diciembre 1998, páginas 351-371.

- "A Systems Model of Privacy", *Journal of Environmental Psichology*, nº 14 (1994), págs. 65 y ss.

PEDERSEN, "Psychological Functions of Privacy", en *Journal of Environmental Psychology*, nº 17, 1997, págs. 147-156.

PIÑAR MAÑAS:

(Dir.) *Desarrollo Sostenible y Protección del Medio Ambiente*, Civitas-Universidad San Pablo CEU, Madrid, 2001

"El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, nº 19-20, Monográfico sobre *Protección de Datos*, págs. 45 y ss. Ha sido traducido al inglés: "ECJ Case Law on the Right to Protection of Personal Data. Part. 1", *BNA International. World Data Protection Report*, Volumen 6, Nº 1, enero 2006. Págs. 3-11; La segunda parte, en la misma Revista, Volumen 6, Nº 2. Febrero, 2006. Págs. 23-32.

"El porqué de un reglamento de desarrollo de la Ley Orgánica de Protección de Datos", en *Revista Española de Protección de Datos*, nº 3 (julio-diciembre 2007)

"Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", *Boletín del Ilustre Colegio de Abogados de Madrid*, monográfico sobre *La Protección de Datos (I)*, núm. 36, 3ª época, abril 2007, págs. 13 y ss.

"Revolución tecnológica, Derecho Administrativo y Administración Pública. Notas provisionales para una Reflexión", en T.R. FERNANDEZ y otros, *La Autorización administrativa. La Administración Electrónica. La Enseñanza del Derecho Administrativo*, Aranzadi, 2007.

"El derecho fundamental a la protección de datos. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos", en PIÑA MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, Madrid, 2008.

"Seguridad, Transparencia y Protección de Datos: el futuro de un necesario e incierto equilibrio", 2008.

"Strengthening Legal Certainty: New Regulations Developing the LOPD (Organic Data Protection Act)", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 33 y ss

PIÑAR MAÑAS y CANALES GIL, *Legislación de Protección de Datos*, Iustel, 2008

PROSSER, "Privacy (A legal Analysis)", *California Law Review*, nº 48 (1960), págs. 338 y ss., también recogido en SCHOEMAN, *Philosophical dimensions.…*, op. cit., págs. 104 y ss

RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruylant, Bruselas-Paris, 1990.

RODOTA:

Tecnologie e diritti, Il Mulino, Bari, 1995;

Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione, Editori Laterza, Roma-Bari, 1997. Hay traducción al español: *Tecnopolítica. La democracia y las nuevas tecnologías de la información,* Losada, Buenos Aires, 2000

Intervista su Privacy e Libertà, a cargo de Paolo CONTI, Editori Laterza, Roma-Bari, 2005.

La vita e le regole. Tra diritto e non diritto, Feltrinelli, Milán, 2006.

"Il corpo e il post-umano", texto original amablemente cedido por el autor, 2008.

"Privacy and the Future: Some Opening Reflections", en VARIOS AUTORES, *Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006*, Fundación BBVA, Madrid, 2008, págs. 19 y ss.

"Innovación, nuevas tecnologías, participación política y protección de datos. Un equilibrio para mejorar la democracia", conferencia impartida en los Cursos de Verano de la Universidad del País Vasco, en el marco del Seminario *El acceso a la Información Parlamentaria*, impartida el 28 de julio de 2008. He utilizado el texto original que amablemente me ha facilitado el autor

ROSEN, The Unwanted Gaze. The Destruction of Privacy in America, Vintage Books, New York, 2000.

RULE y otros, The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies, Elsevier, New York, 1980.

SCHAAR, "The Work of the Article 29 Working Party", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 107 y ss.

SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007),

SMITH, War Stories: Accounts of Persons Victimized by Invasions of Privacy, Privacy Journal, 1993.

SOLOVE, The Digital Person. Technology and Privacy in the Information Age, New York University Press, 2004

SOLOVE, ROTEMBERG y SCHWARTZ, *Information Privacy Law*, Aspen, New York, 2ª ed., 2006.

STANLEY y STEINHARDT. "Face-Recognition Technology Threatens Individual Privacy." Opposing Viewpoints: Civil Liberties. Ed. Tamara L. Roleff. San Diego: Greenhaven Press, 2004

THOMSON, "The Right to Privacy", recogido en Ferdinand David SCHOEMAN, Philosophical Dimensions of Privacy: An Anthology, Cambridge University Press, 1984 (reedición de 2007), pág. 272.

TOLCHINSKY y otros, "Employee perception of invasion of Privacy", Journal of Applied Psychology, nº

66 (1981), págs. 308 y ss.

TRONCOSO, "Regulatory Development of the LOPD", en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 51 y ss

U.S. Department of Health , Education & Welfare, Records, Computeres and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data System, Washington, 1973.

VALCARCEL, "Contaminación acústica y desarrollo sostenible en el marco de la actividad aeroportuaria. Algunas soluciones. En particular: ¿Servidumbres acústicas en la lucah contra el ruido?", en PIÑAR MAÑAS (Dir.) Desarrollo Sostenible y Protección del Medio Ambiente, Civitas-Universidad San Pablo CEU, Madrid, 2002, págs. 207 y ss.

VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008.

VELEIRO, Regulatory Development of the LOPD from a Business Perspective, en VARIOS AUTORES, Proccedings of the First European Congress on Data Protection. Madrid, 29-31 March 2006, Fundación BBVA, Madrid, 2008, págs. 81 y ss.

WARREN y BRANDEIS, "The Right to Privacy (The implicit made explicit)". Harvard Law Review, Vol IV, 15 de diciembre de 1890, nº 5.

WEISER The Computer for the 21st Century, http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

WESTIN, Privacy and Freedom, Atheneum, New York, 1967.

WHITAKER, The End of Privacy: how Total Surveillance is Becoming a Reality, New Press, New York, 1999. Existe traducción al español de la obra de WHITAKER: El fin de la privacidad. Como la vigilancia total se está convirtiendo en realidad, Paidos, 1999.

WHITE, "The use of Privacy Impacts Assessments in Canada", Privacy Files, nº 4, 2001, págs. 2 y ss.

WHITMAN, "The two Western Cultures of Privacy: Dignity versus Liberty", en Yale Law Journal, Vol. 113, Abril 2004, pags. 1151 y ss. También puede consultarse en http://papers.ssrn.com/abstract=476041.

ZABIA DE LA MATA (Coord.), Protección de datos. Comentarios al Reglamento, Lex Nova, Valladolid, 2008.

La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo[1]

Lina Ornelas Núñez[*]
y Sergio López Ayllón

I. Introducción

John Rawls señala que una sociedad puede definirse como una asociación más o menos autosuficiente de personas que reconocen ciertas reglas de conducta como obligatorias en sus relaciones, y que en su mayoría actúan de acuerdo con ellas. En ese sentido, la sociedad se caracteriza típicamente tanto por un conflicto como por una identidad de intereses. Esta doble faceta en la caracterización de la sociedad surge debido a que, si bien es cierto que la cooperación social hace posible para todos una vida mejor de la que cada uno tendría viviendo en el aislamiento, también lo es que las personas no son indiferentes respecto a cómo han de distribuirse los mayores beneficios producidos por la colaboración.[2]

A lo largo de los estadios por los que ha pasado la historia de la humanidad, ésta se ha agrupado y gobernado bajo regímenes normativos muy diversos, creando importantes cuerpos normativos[3], no obstante lo cual hasta antes del siglo XVIII, no era posible aludir a la existencia de un conjunto de valores (listado de derechos) respecto de los cuales se tuviera la certeza histórica que el ser humano compartía en común. En ese sentido, la Ilustración señala el momento a partir del cual dio inicio la evolución de las instituciones que han forjado al Estado Moderno, entre cuyos productos se encuentran las declaraciones de derechos y las constituciones políticas.

Con las ideas de la Ilustración, comenzó una revolución normativa irreversible de la que derivarían, 200 años más tarde, instrumentos como la Declaración Universal de los Derechos Humanos, en la que se contiene en "germen" la síntesis de un movimiento

---

[*] Lina Ornelas es directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública (IFAI). Las opiniones aquí vertidas no representan necesariamente las institucionales. Por su parte, Sergio López Ayllón es profesor investigador del Centro de Investigación y Docencia Económicas (CIDE).

dialéctico que comenzó con la universalidad abstracta de los derechos naturales, pasó por la particularidad concreta de los derechos positivos nacionales y terminó con la universalidad ya no abstracta sino concreta de los derechos positivos universales, dando inicio a un largo proceso cuya realización última no podemos aún ver[4].

Constata lo anterior, la existencia de las distintas fases por las que han pasado los derechos humanos. En un primer tiempo se afirmaron los derechos de libertad, es decir, todos aquellos derechos que tienden a limitar el poder del Estado y a reservar al individuo o a grupos particulares una esfera de libertad frente al mismo. En un segundo momento se proclamaron los derechos políticos, al concebirse la libertad no sólo como el "no impedimento", sino positivamente como autonomía, teniendo por consecuencia una participación cada vez más amplia, difundida y frecuente de los miembros de una comunidad por el poder político (es decir, libertad dentro del Estado). Por último, se reconocieron los derechos sociales, que expresan la maduración de nuevas exigencias, de nuevos valores, como los del bienestar y de la igualdad no solamente formal, derechos a los que se podría llamar libertad a través o por medio del Estado.[5]

En prospectiva, y simplemente a manera de referencia, si a Locke, campeón de los derechos de libertad, alguien le hubiera dicho que todos los ciudadanos habrían debido participar en el poder político y peor aún obtener un trabajo remunerado, habría respondido que eran locuras. Lo anterior es así, toda vez que la persona respecto de la que Locke realizó estudios para definir la naturaleza humana, era únicamente el burgués o el comerciante del siglo XVIII, razón por la cual no pudo advertir las exigencias y reclamos de quien se ubicaba en otro estrato de la sociedad, lo cual le impidió abarcar el espectro completo de la naturaleza humana y con ello determinar los sujetos a quienes debía alcanzar la protección de los derechos humanos.[6]

Parafraseando a Bobbio, la Declaración Universal de los Derechos Humanos, representa la conciencia histórica que la humanidad tiene de sus propios valores fundamentales en la segunda mitad del siglo XX, es una síntesis del pasado y una inspiración para el porvenir, pero sus tablas no han sido esculpidas de una vez y para siempre[7].

El siglo XXI comienza con un despliegue tecnológico estelar. No puede concebirse más la vida de los seres humanos ni su interacción, sin el uso de tecnologías *urbi et orbi.* Dicha expansión conlleva el intercambio de flujos de información incluida la relativa a las personas. Ahora es posible a través de distintos medios acceder a la información de millones de seres humanos y sus actividades en cualquier parte del planeta. Sin embargo, frente al terreno ganado en materia de libertad de información y expresión, se ha irrumpido silenciosamente en el ámbito de lo privado, ya que la sencilla obtención de cualquier tipo de dato sobre una persona física posibilita la generación de perfiles sobre ella y afectar la esfera de sus derechos y libertades. Por ello puede afirmarse que los horizontes para la privacidad se están transformando en *terra incognita* debido a que sin que el propio titular del dato se entere, terceros -sean entes públicos o privados- tratan

su información a través de la utilización de todo tipo de tecnologías como la minería de datos, la geo-localización, la detección remota o la videovigilancia, todo lo anterior conectado a la w*orld wide web,* tecnologías que hoy en día ya han madurado y están plenamente disponibles en cualquier lugar del mundo.

Los avances tecnológicos repercuten generalmente de forma positiva en la calidad de vida del ser humano, mas sería ingenuo desconocer que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho, en su objetivo último de ordenar la convivencia social, debe dar respuesta. La tecnología no ha de permanecer ajena al Derecho, ni evidentemente, a la Constitución, por más que la incesante innovación les obligue a ser objeto de continuas relecturas y adaptaciones, so riesgo de caer en la obsolescencia.[8]

Por esa razón y desde hace décadas, cada vez más países aprueban nuevas leyes sobre privacidad o protección de datos[9], esto en atención al menor o mayor grado de importancia que a la privacidad se le asigne, ya que está ligada al pasado cultural e histórico de cada sociedad.[10]

Recientemente la Cumbre Mundial de la Sociedad de la Información ha hecho un llamamiento para pedir normas "mundiales" para la privacidad en el sentido siguiente: *"Hacemos un llamamiento a todas las partes interesadas para garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislación, la aplicación de marcos de colaboración, mejores practicas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios".*[11]

Los párrafos precedentes sirven de preámbulo para abordar el estado de la cuestión en México, lo cual nos lleva a describir los alcances de este artículo.

A efecto de lo anterior, se narran los antecedentes del derecho a la protección de datos, desde los instrumentos internacionales de derechos humanos, hasta la regulación formulada por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas.

Posteriormente se abordan las decisiones de la Comisión Europea sobre el nivel de adecuación que deben tener terceros países para la circulación de datos personales ya que arroja luz sobre algunos elementos indispensables a incluir en una regulación en la materia. Asimismo, se resaltan los aspectos esenciales de los apartados que contienen las directrices para la armonización del derecho a la protección de datos en Iberomérica como un insumo a considerar en la confección de una ley por su clara estructuración a manera de lista de verificación.

Posteriormente, se abordan las recientes reformas a los artículos 6, 16 y 73 de la Constitución Federal, estos últimos aún en ciernes, en cuanto al derecho a la protección de datos se refiere.

Finalmente en las conclusiones intentamos llevar a cabo un primer acercamiento en cuanto a los elementos mínimos o ejes fundamentales a partir de los cuales se debiera erigir la futura legislación en la materia para el caso mexicano, sobre todo abrevando de las experiencias internacionales y la propia realidad del país.

II. Antecedentes

1. Instrumentos internacionales

En los instrumentos internacionales, el artículo 12 de la Declaración Universal de los Derechos del Hombre[12] (10 de diciembre de 1948) 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.

En el mismo sentido, el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales[13] (14 de noviembre de 1950), reconoce el derecho de la persona al respeto de su vida privada y familiar de su domicilio y correspondencia.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[14] (16 de diciembre de 1966), 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.

En el mismo tenor, la Convención Americana[15] sobre derechos humanos (22 de noviembre de 1969) en su artículo 11 apartado 2, establece 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.

2. Unión Europea

2.1 Los orígenes del derecho a la protección de datos

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los "derechos humanos y nuevos logros científicos y técnicos[16]".

En un momento posterior, surgen diversas leyes nacionales, en 1977 era aprobada la Ley de Protección de Datos de la República Federal Alemana, mucho más ambiciosa

que su predecesora del *Land* de *Hesse*, en 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979)[17].

Hacia la década de los años ochenta surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.[18]

2.2. Convenio 108 del Consejo de Europa

El Convenio 108 sobre protección de datos personales (en adelante el Convenio 108) entró en vigor el 1 de octubre de 1985 y es creado con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades, en particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los Estados.

De esta forma el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

Hay que decir que el Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto debido esencialmente a la naturaleza del Convenio: el mismo a pesar de ser vinculante, establecía únicamente unos principios mínimos, permitiendo que posteriormente fueran los estados firmantes los que los desarrollaran.[19]

2.3 Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

La Directiva 95/46, fue aprobada con un doble objetivo: por un lado garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.[20]

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizan, dado que diversos estados consideran que no es posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.[21]

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido exclusivamente a la protección de datos de carácter personal como fundamento no a la protección de un derecho fundamental, sino la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.[22] La Directiva 95/46, finalmente, es aprobada el 24 de octubre de 1995.

2.4 Carta de Derechos Fundamentales de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea fue aprobada por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza el 7 de diciembre de 2000, reconociendo entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8.

De esta forma, a partir de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y como un derecho autónomo del derecho a la intimidad y a la privacidad de las personas.

3. Recomendaciones de la Organización para la Cooperación y el Desarrollo Económico

La recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en la que se contienen las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, adoptada el 23 de septiembre de 1980 (Recomendaciones de la OCDE), constituye el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.[23]

Su adopción se funda en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos..[24]

La primera parte de la Recomendación, establece las definiciones aplicables, la parte segunda establece los principios básicos aplicables al tratamiento de los datos personales, la tercera está dedicada a las transferencias internacionales de datos, la cuarta trata, en

términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores y la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembro.

4. Foro de Cooperación Economía Asia Pacífico.

Uno de los grupos formados por el Foro de Cooperación Economía Asia Pacífico (APEC), es el Grupo de Manejo del Comercio Electrónico (ECSG) establecido en febrero de 1999, y que dentro de sus principales actividades esta el desarrollo de legislaciones y políticas compatibles entre las Economías en el campo de la Privacidad, para lo cual ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguro y sin obstáculos.

Los principios desarrollados para el Marco de Privacidad de APEC se basan en las Recomendaciones de la OCDE. Estos principios tienen como fin los siguientes aspectos: Proteger la Privacidad de información personal; prevenir la creación de barreras innecesarias al flujo transfronterizo de datos; fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección, uso y procesamiento de datos personales; fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de datos personales.

La protección de la privacidad está diseñada para prevenir a los individuos a efecto de que sus datos no se recolecten erróneamente o bien se haga un mal uso de ellos, estableciendo medidas de resarcimiento proporcionales, en los casos que así proceda. Entre los principios que se reconocen encontramos el de aviso, limitación de la recolección, el de integridad de la información personal y el de salvaguardias a la seguridad, entre otros.

5. Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

La Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas (Resolución 45/95 de la ONU) de 14 de diciembre de 1990, contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial, entre otros, los de licitud, exactitud, finalidad, acceso y no discriminación.

III. Orígenes del derecho a la protección de datos en México

1. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y el derecho a la protección de datos personales

Con fecha 11 de julio de 2002, fue publicada en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Ley Federal de Transparencia)[25], la cual tiene por objeto regular el derecho a la información en una de sus vertientes, la del acceso a la información.

Considerando lo anterior, conviene cuestionarse en qué punto se conectan el derecho de acceso y el derecho a la protección de datos, la respuesta está en los límites del derecho de acceso a la información.

En el caso mexicano los límites al derecho de acceso están señalados de manera expresa en la propia Ley Federal de Transparencia en los artículos 13 y 14 y en el artículo 18. Entre las hipótesis normativas previstas en el artículo 18 de la Ley Federal de Transparencia, se establece que como información confidencial serán considerados los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos señalados en la misma.

Los datos personales se definen como aquella información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad[26].

Aunado a lo hasta ahora descrito, en el capítulo IV de la Ley Federal de Transparencia se establecen una serie de disposiciones dirigidas a garantizar el derecho a la protección de datos personales, tales como principios, derechos de los interesados, la existencia de un registro de protección de datos, así como las algunas reglas en torno a los procedimientos de acceso y corrección de datos personales.

2. El Instituto Federal de Acceso a la Información Pública y la protección de los datos personales

Entre las funciones a destacar del Instituto Federal de Acceso a la Información (IFAI), para efectos de este estudio, se encuentran dos aspectos, en primer lugar el relativo al conocimiento y resolución de los recursos de revisión derivado de solicitudes de acceso y en segundo el relacionado con la expedición de disposiciones administrativas de carácter

general (Lineamientos) para la mejor aplicación de la Ley Federal de Transparencia.

El primero de los aspectos señalados cobra especial importancia en el desarrollo del derecho a la protección de datos en México, ya que es a través de las resoluciones emitidas por el Pleno del IFAI, que se establecen una serie de criterios relevantes respecto al acceso y corrección de datos personales, principalmente en los casos denominados de "tensión de derechos" (fotografías de servidores públicos, expediente clínico del entonces Presidente de la República, entre otros.)

En cuanto al segundo de los aspectos indicados, con fecha 30 de septiembre de 2005, el IFAI publicó en el Diario Oficial de la Federación los Lineamientos de Protección de Datos Personales[27], los cuales tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal, para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Derivado de los citados lineamientos, con fecha 23 de agosto de 2006, se publicaron las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales, con el objetivo de constituirse en propuestas y sugerencias específicas que le permitiera a la Administración Pública Federal lograr una eficaz protección de los datos personales contenidos en sus sistemas de datos, según se desprende del último de sus considerandos[28].

Como se puede observar, la intervención del IFAI en esta materia es de la mayor relevancia ya que puede llegar constituirse en el factor que, por una parte, permita que el derecho a la protección de datos personales, dentro de los límites de la legalidad, responda a las exigencias a las que la realidad nos enfrenta, y por la otra facilite elementos orientadores que conduzcan al mejor entendimiento y aplicación de la norma jurídica a los casos que se les presenten.

3. El derecho a la protección de datos en la Constitución Política de los Estados Unidos Mexicanos

3.1 Artículo 6 de la Constitución Federal

Con fecha 20 de julio de 2007, fue publicada en el Diario Oficial de la Federación, la reforma al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, fundamentalmente, con el objeto de homologar el derecho de acceso a la información pública gubernamental, en cualquier punto del territorio nacional y en los tres niveles de gobierno. Al respeto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados se señaló lo siguiente:

> La iniciativa que se dictamina, surge de un análisis pormenorizado y exhaustivo de una problemática nacional que no debemos aceptar: luego de cuatro años de marcha

> de las leyes de transparencia y acceso a la información, se ha cristalizado una heterogeneidad manifiesta y perjudicial de los cimientos para el ejercicio del derecho, que contienen diversas leyes, tanto federal como estatales.

La reforma al artículo 6 de la Constitución Federal plantea diversos nuevos retos a la transparencia gubernamental en nuestro país que se materializaron en siete fracciones. En las tres primeras se establecieron los principios fundamentales que dan contenido básico al derecho, mientras que en las fracciones cuarta, quinta y sexta se plantearon las bases operativas que deberán contener las leyes en la materia para hacer del derecho una realidad viable, efectiva y vigente, según señala el ya citado dictamen de la Cámara de Diputados.

El reformado artículo 6, fracción II, establece como parte de los principios en materia de acceso, que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Al respecto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados, en el apartado en el que se hace el análisis de la iniciativa, se indicó lo siguiente:

> En ella se establece una segunda limitación al derecho de acceso a la información, misma que se refiere a la protección de la vida privada y de los datos personales. Esta información no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental, que es el de la intimidad y la vida privada.
>
> Es fundamental esclarecer que aunque íntimamente vinculados, no debe confundirse la vida privada con los datos personales…
>
> La fracción segunda establece también una reserva de ley en el sentido que corresponderá a ésta, determinar los términos de la protección y las excepciones a este derecho…

El mencionado artículo 6, fracción II, tiene la virtud de ser la primera disposición en la historia de nuestro país que hace un reconocimiento expreso al derecho a la protección de datos personales en la cúspide normativa, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

3.2 Artículo 16 de la Constitución Federal

Del año 2000 al 2005 se promueven diversos proyectos legislativos en torno al tema en el Congreso de la Unión, sin que ninguno de ellos fructifique dada la ausencia de disposición constitucional que las sustente, hasta que en el mes de abril de 2006 se aprobó

en la Cámara de Senadores el Decreto por el que se adicionan dos párrafos al artículo 16 de la Constitución Federal para reconocer el derecho a la protección de datos personales, enviándose a la Cámara de Diputados para los efectos constitucionales conducentes.

Derivado de lo anterior, con fecha 20 de septiembre de 2007, se vota, con un par de modificaciones mínimas, la propuesta enviada en su momento por la Cámara de Senadores para reconocer el derecho a la protección de datos personales como derecho fundamental autónomo. En este momento la iniciativa regresó a la Cámara de su Origen (la de Senadores) en virtud de las pequeñas modificaciones efectuadas por la Revisora.

El Proyecto de Decreto por el que se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento.
>
> 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.
>
> No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado.

Con la reforma al artículo 16 constitucional finalmente se reconoce y da contenido al derecho a la protección de datos personales. En ese sentido, en la reforma se plasman los derechos con los que cuentan los titulares de los datos personales como lo son los de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO).

Por otra parte, se hace referencia a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios.

Conviene destacar que inclusive antes de la reforma al artículo 6º constitucional y de la propuesta de reforma al 16, se venían haciendo esfuerzos muy loables en torno al derecho a la protección de datos personales, no obstante lo cual la dimensión de este derecho seguía sin tener la profundidad requerida para dotar al gobernado de un herramienta efectiva que le permitiera equilibrar su situación jurídica frente al vertiginoso desarrollo tecnológico y el pujante comercio internacional que al mismo acompaña.

A mayor abundamiento, conviene citar algunas de las razones que se plasman en la valoración de la minuta aprobada por la Cámara de Diputados (en su carácter de cámara revisora) en relación con la propuesta de reforma al mencionado artículo 16:

> Esta Comisión revisora resalta la relevancia de emitir un dictamen en el que por primera vez en la historia de México, se reconozca al máximo nivel de nuestra pirámide normativa la existencia de un nuevo derecho distinto y fundamental a la protección de datos personales, dentro del catálogo de garantías. Lo anterior, en razón de la evolución normativa experimentada en nuestro país, a partir de la regulación de la protección de datos personales en posesión del Estado regulada por la fracción II del artículo 6 constitucional. La intención de reformar el artículo 16 para incluir la protección de los datos personales, es un camino que desde hace algún tiempo inició el legislador mexicano.
>
> Derivado de lo anterior, la propuesta que se presenta ante esta Cámara Revisora, tiene como propósito consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, apuntalando, por una parte, la estructura edificada a través del artículo 6 fracción II de la Constitución Federal y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder del sector privado.

Hasta aquí en cuanto a las razones y alcances, en lo general, que produciría la reforma al artículo 16 constitucional de aprobarse por el Senado[29], y en su momento por las legislaturas estatales.

3.3 Artículo 73 de la Constitución Federal

De acuerdo con el proyecto de Decreto aprobado en la Cámara de Diputados (en su carácter de cámara de origen), la propuesta tiene por objeto dotar de facultades al Congreso Federal para que legisle en materia de protección de datos en posesión de los particulares, la cual es la siguiente:

> Artículo Único. Se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
>
> Artículo 73. El Congreso tiene facultad:
>
> I. a XXIX-N. ...
>
> XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de particulares.

Entre las materias con las que se encuentra íntimamente vinculado el derecho a la protección de datos se encuentra el comercio internacional. Dentro de las razones históricas

que justificaron la creación de este derecho y sus consecuentes instrumentos regulatorios, está el impedir la restricción de la libre circulación de los datos personales entre Estados.

El mejor ejemplo de la situación previamente descrita es la Unión Europea, en la que se garantiza la libre circulación de personas, bienes y datos personales entre los países miembros, lo que desde luego no representa ningún contrasentido, considerando que los Estados miembros cuentan con regulaciones homogéneas a partir de las cuales los datos se encuentran igualmente protegidos en un país u otro de la Unión.

Existen dos razones que sustentan que la ley que regule los datos personales en posesión de los particulares sea federal: por una parte, el comercio internacional, en virtud de que el Estado Mexicano hacia el exterior es uno y como tal debe contar con una legislación uniforme en sus relaciones internacionales, independientemente del área del territorio nacional donde materialmente se estén tratando los datos personales, y por la otra, que la materia de comercio es federal, de conformidad con nuestra Ley Fundamental.

Respecto de los datos personales en posesión de los entes públicos estatales y municipales, corresponderá a las legislaturas estatales trazar el camino por el que encauzarán el derecho a la protección de datos personales, sobre la base constitucional que en su momento se apruebe.

De concretarse estas reformas, México se ubicaría entre la élite de países que cuentan con un derecho a la protección de datos personales a nivel constitucional, con lo que se contribuye a la consolidación democrática y económica de este país desde el terreno de los derechos humanos.

IV. Aspectos relevantes de la actualidad del derecho a la protección de datos que debieran tenerse como referente para la legislación mexicana

1. Nivel de adecuación de países terceros conforme a la Directiva 95/46/CE

Los artículos 25 y 26 de la Directiva 95/46/CE, establecen un régimen específico para los flujos transfronterizos de datos personales hacia países distintos de los estados miembros en los cuales se exige, como punto de partida, que el Estado al que se destinen los datos ofrezca un nivel adecuado de protección.

A efecto de lo anterior, la Comisión Europea decide si un país tercero se adecua al nivel de protección de datos establecido en la citada Directiva 95/46/CE, teniendo en cuenta el dictamen que para el caso elabore Grupo de trabajo de protección de las per-

sonas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la mencionada Directiva teniendo como base el documento de trabajo del Grupo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado el 24 de julio de 1998, cuyo Capítulo 1 analiza qué debe entenderse por "protección adecuada".

Dicho documento delimita dos tipos de análisis que habrían de efectuarse sobre la legislación del Estado de destino de los datos, a fin de poder delimitar si la misma resulta adecuada: el relativo a su contenido sustantivo y el relacionado con los mecanismos y procedimientos de aplicación de la legislación sustantiva.

En cuanto al contenido sustantivo, la legislación del Estado de destino habría de contener los principios básicos de protección de datos que tradicionalmente son reconocidos por los acuerdos y directrices internacionales adoptados en este ámbito, considerándose como tales los siguientes: 1. Limitación de la finalidad; 2. Calidad y proporcionalidad de los datos; 3. Transparencia; 4. Seguridad y confidencialidad; 5. Derechos de acceso, rectificación, supresión y bloqueo de los datos; 6. Restricciones a la transferencia ulterior; 7. Categorías especiales de datos; 8. Marketing directo; 9. Decisión individual automatizada.

Aunado a lo anterior, la Comisión Europea verifica que el ámbito de aplicación de la regulación de un tercer estado contemple a los sectores público y privado, que exista una autoridad independiente, dotada con facultades de inspección y sanción ante la cual puedan acudir los interesados para hacer efectivos sus derechos frente a los responsables de los tratamientos de datos.[30]

2. Directrices para la armonización de la protección de datos en la comunidad Iberoamericana, el cual constituye un modelo acerca de lo que debe contener una legislación en los estados miembros.

Los días 13 y 14 de noviembre de 2003, en la ciudad de Santa Cruz de la Sierra, Bolivia, se llevó a cabo la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, de la que derivó la Declaración de Santa Cruz de la Sierra, la cual fue suscrita por el Presidente de la República.[31]

Es a partir de la integración de México en la Red Iberoamericana de Protección de Datos, que se ha cobrado conciencia plena sobre el tema gracias al acercamiento con otros países en los que ya se cuenta con una legislación integral y vigente, a través de los cuales fue posible conocer los efectos positivos que produce el contar con instrumentos normativos en la materia de protección de datos personales.

En el V Encuentro Iberoamericano de Protección de Datos[32], se aprobó por los miembros de la Red, el documento que contiene "Las directrices para la armonización

de la protección de datos en la comunidad Iberoamericana, el cual constituye un modelo acerca de lo que debe contener una legislación en los estados miembros"

Entre los elementos que debe contener una ley de protección de datos de acuerdo con las directrices de referencia podemos destacar los siguientes aspectos:

- En cuanto al ámbito de aplicación, la necesidad de dirigir la legislación a todo tipo de tratamiento de datos sea manual o automatizado llevados a cabo por las entidades de los sectores público y privado.
- En relación con el régimen de excepciones al ámbito de aplicación el sustraer o modular, según el caso, cuestiones relativas a seguridad nacional, el orden público, la salud pública o la moralidad y dicha medida resulte estrictamente necesaria y no excesiva en el ámbito de una sociedad democrática.
- Respecto a las disposiciones generales fijar los principios de calidad de los datos (lealtad, licitud, proporcionalidad, exactitud y conservación), legitimación del tratamiento, transparencia e información al interesado, entre otros.
- En torno a los derechos que se reconozcan los de acceso, rectificación, cancelación y oposición respecto de los cuales se establezcan, procedimientos claros, expeditos y gratuitos o sin gastos excesivos.
- En cuanto a la seguridad y confidencialidad en el tratamiento que se adopten de medidas técnicas y organizativas necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.
- Respecto del régimen de transferencias internacionales de datos como regla general que éstas se efectúen únicamente al territorio de Estados cuya legislación recoja los mínimos requeridos para tales efectos, en una situación similar a la que ocurre en el caso de las autorizaciones que realiza la Comisión Europea en la Unión Europea.
- En relación con la autoridad de control que está se diseñe de tal manera que pueda actuar con plena independencia e imparcialidad, con mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.

Asimismo se sugiere que la autoridad de control cuente como mínimo con competencias para conocer de las reclamaciones que les sean dirigidas por los ciudadanos, en particular en cuanto al ejercicio de sus derechos, para realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de la regulación, así como para imponer sanciones, en los casos que así lo amerite

- También deberá establece la necesidad de contar con un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer sus derechos.

V. Conclusiones:

El derecho a la protección de datos personales ha experimentado un desarrollo muy basto a nivel europeo extendiéndose a otras latitudes sobre todo en razón del avance tecnológico, la ubicuidad de la computación y los intercambios globales.

Del análisis efectuado podemos decir que este nuevo derecho sitúa a la persona como el centro de la protección, mas que al dato *per se*. Dado que la norma secundaria derivara de un derecho fundamental reconocido al más alto nivel de la pirámide normativa será necesario esperar la aprobación definitiva de las reformas constitucionales a los artículos 16 y 73, para conocer los alcances que a este derecho quiso dar el constituyente.

Una mirada crítica a los modelos existentes de protección de datos personales puede permitirnos el diseño de una ley moderna que recoja las mejores prácticas, los mecanismos mas adecuados de tutela y modelar instituciones eficaces. Los retos no son pocos en este tema. Por su complejidad y múltiples conexiones con otros derechos, el de la protección de datos se antoja laberíntico.

Derivado de los desarrollos normativos descritos en este artículo, a continuación y solo a modo indicativo, consideramos que los ejes fundamentales de una ley de protección de datos personales pueden ser los siguientes:

a) En primer lugar el objeto de la norma debería ser garantizar la protección de los datos de carácter personal reconociendo los derechos y principios que rigen la materia. En ese sentido, la ley debe posibilitar de manera equilibrada por una parte, la legítima y controlada transferencia y utilización de datos genéricos con el consentimiento tácito de los titulares y cuando se trate de datos sensibles solo mediante el consentimiento expreso e informado. Una regulación demasiado estricta sería de difícil cumplimiento, sobre todo en una era donde la tecnología avanza con tal rapidez.

b) El ámbito de aplicación de la Ley podría abarcar tanto la regulación para aquellos sistemas (bases) de datos personales públicos como privados, o bien sólo para éstos últimos, dejando a las leyes de transparencia o especiales, la regulación para los públicos (en armonía con lo dispuesto por la fracción II del recién reformado artículo 6 constitucional).

c) Debieran preverse los principios de protección de datos personales reconocidos a nivel internacional, tales como el de licitud, calidad, proporcionalidad, consentimiento, finalidad, información y seguridad. De la claridad en las definiciones y alcances de dichos principios, dependerá la operatividad y efectividad de la ley. Tal es el caso del consentimiento del titular de los datos, el cual se erige como la columna vertebral de este nuevo derecho. Las reglas para otorgarlo, obtenerlo o revocarlo en razón de la naturaleza del dato deben ser claras e incluir todos los supuestos.[33]

d) Los Derechos de los titulares de los datos personales deben incluirse de manera contundente y clara como lo son, el de acceso, corrección, cancelación y oposición, así como al recurso ante una autoridad independiente que los tutele de manera eficaz. Como todo derecho encontrará sus límites en la propia norma.
e) La existencia de una autoridad independiente y especializada que garantice la tutela del derecho a la protección de datos, con facultades para sancionar. En este punto puede explorarse la conveniencia de que un mismo órgano se encargue de garantizar el derecho de acceso a la información así como el de protección de datos a nivel nacional, o bien se cree una autoridad distinta e independiente. [34]
f) Por su parte, la ley deberá prever disposiciones para el adecuado tratamiento, confidencialidad y custodia de los datos personales sensibles por los efectos socioeconómicos negativos en el corto y mediano plazo que su liberación no controlada puede ocasionar, por lo que la Ley deberá contemplar el tratamiento diferenciado de datos de acuerdo con su naturaleza y grado de protección que ésta conlleva.
g) Se estima que debiera valorarse la utilidad de la existencia de un Registro de Protección de Datos, ya que con ello se dota al gobernado y a la autoridad de un instrumento general de consulta y control respecto de los datos que los sujetos obligados poseen. Sus requisitos deben ser sencillos para permitir su operatividad.
h) Asimismo, debe preverse un apartado de transferencias internacionales de datos, a efecto de que la protección alcance dentro y fuera del territorio nacional, sin que con ello se vulneren las reglas del derecho internacional,[35] así como mecanismos de cooperación internacional en la materia.

Este trabajo intenta poner sobre la mesa que no estamos frente a un debate cerrado y propone nuevas ópticas de análisis a la problemática de ingeniería jurídica que ocupará un lugar central en la agenda legislativa de nuestro país y sobre todo, en el devenir de la sociedad que se avecina en materia de privacidZad.

Notas

[1] *Memorias del II Congreso Mexicano de Derecho Procesal Constitucional*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, 2007.

[2] *Vid*. RAWLS, John. *Teoría de la Justicia*, México, Fondo de Cultura Económica 1979, p. 1.

[3] El Código de Hammurabi en la antigua Mesopotamia, las XII Tablas y el denominado *Corpus Iuris Civilis* en Roma, así como el derecho común europeo en la Alta Edad Media, entre otros.

[4] *Vid*. PECES- BARBA, Gregorio. *Derecho positivo de los derechos humanos*, Madrid, Debate, 1987,

[5] *Vid.* BOBBIO, Norberto. *El tiempo de los derechos*, Madrid, Sistema, 1991, p 109.

[6] *Vid*. PECES- BARBA, Gregorio. *Op.cit.*, p 139.

[7] BOBBIO, Norberto. *La herencia de la gran revolución*, Madrid, Sistema, 1991, p.172.

[8] GUERRERO PICÓ, María del Carmen. El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal. Estudios de Protección de Datos. Agencia de Protección de Datos de la Comunidad de Madrid. Thomson Civitas, 2006.

[9] El último reporte sobre Privacidad y Derechos Humanos 2006 del E*lectronic Privacy Information Center (EPIC*), da cuenta de los desarrollos constitucionales, legales y del marco regulatorio en materia de protección a la privacidad en mas de 75 países alrededor del mundo. Ver www.epic.or

[10] Esta afirmación corresponde, entre otros a J. DHONT y M. V. PEREZ ASINARI, *"New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation, looking for Adequate protection"* en Flujos transfronterizos y extraterritorialidad: La postura europea, PUOLET, Ives, Revista Española de Protección de Datos p.112. Julio-Diciembre 2006. Thomson Civitas.

[11]Idem.

[12] http://www.un.org/spanish/aboutun/hrights.htm.

[13] http://www.derechos.org/nizkor/espana/doc/conveudh50.html.

[14] http://www.derechos.org/nizkor/ley/pdcp.html.

[15] http://www.oas.org/juridico/spanish/Tratados/b-32.html.

[16] *Vid.* Piñar Mañas, José Luis. El derecho fundamental a la protección de datos personales, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005, p 20.

[17] *Ibidem*.

[18] *Idem*, pp. 20-21.

19 Vid. ARENAS RAMIRO, Mónica. El derecho fundamental a la protección de datos personales en Europa, Valencia, Tirant lo Blanch, p. 156.

20 ARENAS RAMIRO, Mónica. op. cit., pp. 277-278.

21 PUENTE ESCOBAR, Agustín. Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005,, p. 43.

22 Idem.

23 Vid. PUENTE ESCOBAR, Agustín. op. cit., p 51.

24 Ibidem.

25 http://www.diputados.gob.mx/LeyesBiblio/decre/LFTAIPG_06jun06.doc.

[26] Artículo 3 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

27http://www.ifai.org.mx/pdf/ciudadanos/cumplimiento_normativo/datos_personales/lineamientos_protdaper.pdf.

[28]http://portaltransparencia.gob.mx/pot/marcoNormativo/consultar.do?method=consultar&idMarcoNormativo=39&idDependencia=06738&_idDependencia=06738

[29] Los cambios realizados por la Cámara de Diputados que motivaron el envío del proyecto de decreto de regreso a la Cámara de origen (Senado) son los siguientes: en el primer párrafo de la propuesta se omitió la palabra destrucción y se sustituyó por la expresión "manifestar su oposición". En el segundo párrafo se cambió de posición la palabra público, que anteriormente sólo calificaba a la palabra "interés" para adjetivar las palabras "interés, seguridad y salud" con el calificativo "públicos".

[30] La Comisión Europea ha emitido a la fecha 6 decisiones de nivel adecuado de protección de datos a los siguientes países en orden cronológico: Suiza, Estados Unidos de América (Acuerdos de Safe Harbour), Canadá, Argentina, Guernesy e Isla de Mann.

[31] Entre los puntos a resaltar en la citada Declaración se destaca el identificado con el número 45, que señala lo siguiente: "45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra comunidad. "

[32] Celebrado en noviembre de 2007 en la ciudad de Lisboa, Portugal.

[33] Así por ejemplo, debiera incluirse un doble esquema conocido como el enfoque *opt in- opt out*, por el cual, en el primer supuesto, necesariamente debe obtenerse el consentimiento previo, libre, expreso e informado de su titular para el tratamiento de lo**s** datos especialmente protegidos o sensibles como lo son los relativos a la salud, la preferencia sexual, la religión u opiniones políticas; mientras que en el segundo, los datos no sensibles pueden transmitirse con un consentimiento tácito y solo mediante la oposición expresa a que los datos sean utilizados, los usuarios de los mismos estarían impedidos de tratarlos. Lo anterior podría generar beneficios al propio titular como consumidor, así como a la economía en general permitiendo que varios agentes económicos utilicen la información con fines de mercadeo de bienes o servicios.

[34] El primer modelo funciona en países como Reino Unido donde el *Infomation Commissioner* es la misma autoridad para resolver sobre las negativas de acceso a la información así como para velar por la protección de datos personales. Ello tiene la complejidad que conlleva el administrar dos piezas legislativas distintas, pero también puede tener ventajas como el hecho de que una sola autoridad concentre los criterios de apertura y protección evitando posibles conflictos como en el caso francés en el cual, la Comisión de Acceso a Documentos Administrativos (CADA) no en pocas ocasiones se encuentra contrapuesta con la Comisión Nacional de Libertades Informáticas (CNIL). Otra ventaja puede ser el ahorro en los costos de creación institucionales.

[35] En ese sentido, siguiendo la tendencia global de negocios debe preverse la posibilidad de utilizar mecanismos alternativos como los contractuales, así como incluir mecanismos de autorregulación o códigos de conducta de sectores involucrados como las denominadas *"Cross Border Privacy Rules"* entre empresas de la misma familia que llevan a cabo transferencias internacionales de datos, códigos de ética o sellos de confianza que aseguren el adecuado tratamiento de los datos.

Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual

Isabel Davara F. de Marcos

I. Planteamiento

Últimamente todos hablan de la protección de datos de carácter personal y su posible y futura legislación en México.

Lo cierto es que actualmente no existe actividad, pública o privada, comercial o no, que pueda sobrevivir sin tratamiento de datos de carácter personal (administrados, clientes, personal, etc.).

Es más, en nuestra opinión, el único valor añadido que la industrializada producción tiene hoy es el conocimiento de los destinatarios de sus productos y servicios, fabricados todos de manera muy similar, y la difícil competencia sólo encuentra dicha diferenciación en tanto en cuanto se conoce al consumidor final.

Y, dando un paso más allá, consideramos que hoy en día en realidad nuestra "identidad virtual" es incluso más importante, al menos cuantitativamente hablando, que nuestra única hasta el momento identidad física.

Y así dice Rodotà: "Las tecnologías de la información y de la comunicación están rediseñando el mundo, las relaciones personales, sociales, políticas y económicas. Pero esta transformación tiene un precio. (…) es justamente la información la que viene a constituir ahora la materia prima más importante y que, dentro de la información, los datos personales son especialmente preciados. (…) nuestra propia vida está volviéndose hoy en día un intercambio continuo de informaciones (…) la protección de datos asume una importancia creciente, que la conduce cada vez más hacia el centro del sistema político-institucional1".

Por otro lado, podría parecer que en esta cuestión existen posiciones extremistas, o, más bien diríamos, que hay quien puede estar interesado en hablar de posturas radicales, y fomentar así incertidumbre y prejuicios, sin contar con quienes pretenden reducir su importancia a las usuales quejas de los particulares en temas de publicidad y marketing no consentidos2.

Es en consecuencia nuestra intención plantear aquí un enfoque general de la materia, para lo que partiremos en primer lugar de algunas consideraciones preliminares que intentarán clarificar algunos extremos confusos. Continuaremos adentrándonos en la historia de este derecho a la protección de datos personales en el entorno internacional, siguiendo con el análisis de la situación nacional del mismo, para ya poder intentar analizar los elementos que componen este derecho, distinguiendo entre principios, derechos y procedimiento. Posteriormente trataremos algunas cuestiones específicas como la transferencia internacional de datos, para pasar al análisis de las reformas constitucionales, y así terminar finalmente con unas breves reflexiones a modo de conclusión.

II. Algunas consideraciones preliminares

Primera

La denominación de "protección de datos personales" ya conduce a confusión. El dato, en sí mismo, no necesita protección alguna. Sin embargo, cuando el dato se une a una persona, es algo distinto. Ya no protegemos, entonces, al dato, sino al titular del mismo, a la persona. Es más, cuando el dato se une a la persona se convierte en información personal3.

En este mismo sentido, las normativas en protección de datos persiguen proteger al individuo frente al ilícito tratamiento de la información personal que le concierne. Es decir, el individuo es el titular del derecho. Es un derecho subjetivo, no se trata de una protección de la información per se, sino de la protección del individuo a que dicha información concierne.

Y es precisamente la información la que tiene relevancia en la sociedad de hoy en día. Tanto así que se habla de Sociedad de la Información –distinta de la Sociedad del Conocimiento, pero éste es un tema en el que no podemos divagar en este momento- empujada por la inmensa magnitud de información a nuestro alcance en la actualidad, gracias en gran parte a la existencia y uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC).

El valor de los datos personales es absolutamente innegable. De un lado, en términos de derecho de la personalidad, del individuo, y, de otro, aunque no nos guste excesivamente el planteamiento, en claros términos económicos4.

Y decimos lo anterior porque, aunque preferimos plantear el derecho como un derecho subjetivo fundamental de tercera generación, como veremos después, no es menos cierta su relevancia en términos mercantiles.

Es más, es precisamente esta importancia la que lleva a que sean tan codiciados y a que su reglamentación, además de debida por su cualidad jurídica, sea más que deseable.

Por una parte, desde el enfoque del que trata esos datos, es decir, la empresa o dependencia, hablando coloquialmente, con unos fines y utilidades determinados, para los que, como decíamos, constituyen un activo fundamental en su operación.

Pero, por otra parte, es el propio titular de los datos el que debería ser consciente, o al menos empezar a serlo, de su valor, y comenzar a actuar en consecuencia diligentemente respecto del tratamiento de su información personal5, decidiendo cada uno personal y conscientemente qué tipo de cuidado y límites desea para su información personal.

Es difícil, y hasta cuestionable, reclamar cuidado y tutela de un tercero sobre algo propio que no se cuida. Si el mismo titular no tiene diligencia sobre el cuidado de sus datos, y los entrega sin ninguna cautela, incluso llegando a comerciar con ellos a cambio de meras baratijas, después no puede enfurecerse por un tratamiento posterior que incluso él ha podido propiciar y en ocasiones hasta consentir.

Segunda

En esta materia se interrelacionan y mezclan muchos conceptos, como intimidad, privacidad y datos personales.

En cuanto a la intimidad, siempre ha habido tratamiento de datos de carácter personal, pero, hasta la utilización masiva de la informática para dicho tratamiento, no se producía una intromisión tan importante y agresiva en la esfera personal e íntima de las personas6. Esta intromisión, que en algunos casos no tiene por qué ser negativa, ni mucho menos ilícita, se percibe como una amenaza potencial, desconocida.

Además, la importancia del tratamiento por medios informáticos ha tenido una especial incidencia, pues las fronteras de tiempo y espacio, que protegían en gran manera la intimidad del individuo, se han difuminado sustancialmente, haciendo que la información personal se pueda tratar, comunicar, conservar, manipular, etc., de muy diferentes maneras.

Es aquí donde esta inmensa transformación tecnológica hace que el Derecho tenga que reaccionar y proponer soluciones encaminadas a manejar este nuevo escenario en la protección no ya de la intimidad de las personas, sino de su derecho fundamental a la protección de datos de carácter personal, o, en términos más coloquiales, a su privacidad.

La concepción cerrada y estática del derecho a la intimidad pasa a una abierta y dinámica, que implica el reconocimiento no sólo de un derecho sino de nuevos mecanismos de protección.

En relación con la privacidad7, la privacidad es un término más profundo que la intimidad8, concepto más conocido y común en ordenamientos jurídicos de nuestro entorno, mientras que en el entorno anglosajón9 se usa indistintamente la palabra privacy entremezclada con la intimidad, y de ahí también que al castellanizar el término se fomente la confusión señalada.

Es un concepto más amplio porque está compuesta por diversas facetas del individuo, de su personalidad, que, tratadas de manera conjunta, máxime por medios informáticos, pueden llegar a constituir un perfil que el mismo individuo, titular de esos datos aislados, desconoce, y, por tanto, no controla.

Podemos afirmar, por tanto, que privacidad es un término que se utiliza para referirnos al perfil que se puede obtener de una persona con el tratamiento de sus datos de carácter personal y que el individuo tiene derecho a exigir que permanezca en su esfera interna, en su ámbito de privacidad10.

En definitiva, los conceptos, si bien entrelazados, e incluso a veces confusos y confundidos, son distintos.

Cada sujeto define la intimidad en función de sus preferencias, si bien, por supuesto, existen unas reglas en Derecho que impiden ciertas intrusiones abusivas, mientras que la privacidad, derivada del tratamiento de los datos, aunque pueda ser manejada en cierta medida por su titular, principalmente por medio del consentimiento, debe estar sujeta a unas normas establecidas para controlar el tratamiento de los mismos11.

En relación con la vida privada. El término vida privada, que aparece entre otros en la reforma constitucional al artículo Sexto, añade un concepto más a tener en cuenta.

La vida privada podría entenderse como vida familiar, y, en este sentido, el derecho es individualista, se manifiesta especialmente al excluir interferencias ajenas, y, por ende, la tutela es estática, negativa.

Por su parte, en la protección de datos, como hemos dicho al hablar de privacidad, la tutela es dinámica, sigue los datos en circulación, y, además, ya no es individualista sino que implica una específica responsabilidad pública. El concepto de privacidad evoluciona desde su definición original como "derecho a ser dejado solo" hasta el derecho de mantener control de la propia información y construir la propia esfera privada12.

Así, señala la Exposición de Motivos de los Lineamientos de protección de datos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LFTAIPG): "Atendiendo a la evolución que ha ocurrido de la noción tradicional de intimidad o vida privada limitada al derecho de impedir interferencias ajenas, o al derecho a ser dejado solo, hasta el derecho de mantener el control de la propia información y de determinar la forma de construcción de la propia esfera privada que el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la persona en las sociedades democráticas".

En cuanto a los datos personales, La relevante Sentencia del Tribunal Constitucional español 292/00, de 30 de noviembre, instaura jurisprudencialmente en España la autonomía e independencia del derecho fundamental a la protección de datos, diferenciándolo claramente de otros cercanos, como el de la intimidad13.

Y así señala en su Fundamento Jurídico Sexto: "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado(...) atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer."

Igualmente reconoce la Exposición de Motivos de los Lineamientos antes mencionados: "… a efectos de lograr un uso racional y ético de las tecnologías, en el concierto de las naciones se ha legislado en materia de protección de datos personales, por lo cual los individuos gozan de un nuevo derecho denominado a la autodeterminación informativa, como garantía del ciudadano en las modernas sociedades frente al desafío del tratamiento electrónico de sus datos, entendida la garantía como la facultad del individuo de decidir quién, cuándo y bajo qué circunstancias utiliza sus datos personales, tanto en el sector público como en el privado".

Tercera

¿Qué podemos entender, entonces, por protección de datos personales? Al intentar definir qué se puede entender por protección de datos, seguimos a Davara14, que entiende al respecto: "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

Hondius, por su parte, define el derecho a la protección de datos como "aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos15".

Pérez Luño señala que "la protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos16".

En otro orden de cosas, siguiendo igualmente el planteamiento de Davara, el análisis de la protección de datos puede estructurarse en un triángulo cuyos tres vértices se denominarían principios, derechos, y procedimiento respectivamente.

Así, diríamos que la protección de datos se compone de una serie de principios, que, a modo de declaraciones programáticas, establecen los pilares en los que se basa la protección de datos.

Los derechos, por su parte, representan la concreción subjetiva de ejercicio de esos principios, es decir, cómo el titular de los datos de carácter personal puede ejercer unos derechos que concretan los principios teóricos en los que se basa toda la normativa.

El procedimiento, finalmente, cerrando este triángulo ficticio, concreta la tutela pública a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de esos principios.

Por otro lado, en el tratamiento de datos de carácter personal podemos distinguir tres fases claramente diferenciadas: la obtención de los datos, el tratamiento de los mismos, y la utilización del resultado del tratamiento, y, en su caso, transmisión de datos a un tercero. En cada una de esas fases tenemos que atender al respeto de todos los principios y derechos prescritos en la normativa. De esta manera, si no se cumple con alguno, el tratamiento se convierte inmediatamente en ilícito.

Cuarta

¿De qué tipo de derecho hablamos? Es un derecho subjetivo, fundamental, y de tercera generación. Es un derecho subjetivo en tanto en cuanto es el titular de los datos, la persona, la que ostenta dicho derecho, a la que se protege.

Es un derecho fundamental, así reconocido internacionalmente. No obstante, en México, se le acaba de dar cabida hace apenas un año, el pasado 20 de julio de 2007, en el reformado artículo Sexto Constitucional, si bien podrían caber dudas y realizarse disquisiciones doctrinales acerca de su reconocimiento como derecho fundamental o como mera garantía "institucional" que debe desarrollarse para adquirir dicha categoría.

Es un derecho de tercera generación. Se puede hablar de una primera generación de derechos civiles y políticos, seguidos de la segunda generación de derechos sociales y culturales, para llegar a una tercera generación de derechos de los pueblos o la solidaridad. Son derechos colectivos o comunitarios (por ejemplo, derecho a la autodeterminación, a la paz, al desarrollo, a la democracia, a la integración, a recibir y producir información equitativamente, al medio ambiente sano y ecológicamente equilibrado, a beneficiarse del patrimonio común de la humanidad…) que se encuentran en distintas etapas de desarrollo internacionalmente. Son, además, derechos que por un lado implican una defensa frente al Estado y, por otro, se pueden demandar ante el mismo, que requieren de

todos los actores sociales para su cumplimiento, plantean exigencias en el plano nacional y en el internacional, y encajan en el concepto moderno de "calidad de vida" .

Quinta

Delimitación con otros derechos, en especial, el del acceso a la información pública. Ningún derecho es absoluto en un Estado de Derecho . Por lo tanto, tampoco lo es el derecho a la protección de datos de carácter personal.

Sentando lo anterior, parece que en México se ha pretendido optar por plantear el derecho a la protección de datos de carácter personal como un límite al acceso a la información pública, cuando, como hemos reiterado en multitud de ocasiones, si bien puede entrar en conflicto con la misma (y entonces habría que acudir a los conocidos instrumentos de prueba del daño e interés público para dilucidar la supremacía de alguno de los dos), como con muchos otros derechos, sería preferible, en todo caso, plantearlo como complemento.

Sin embargo, aún partiendo de la base de que la transparencia es un elemento fundamental de la democracia, como se plantea Rodotà: "¿debería eso ser un óbice para la igual defensa de la privacidad? ¿Es posible que la defensa de la privacidad conviva con esta idea de democracia? ¿Como se entrelazan, la esfera pública y la privada? ¿Cuál debería ser en esta materia la relación entre la libertad del individuo y las intervenciones del Estado?"

La privacidad, como dijimos, no puede ser ya hoy entendida como el derecho a ser dejado solo, sino que conlleva el poder de controlar la información personal , y, en concreto, el flujo de la misma.

La protección de datos cambia el paradigma, basándose ahora en la posibilidad del individuo a acceder a su información personal en posesión de cualesquiera terceros, ejerciendo éste un poder de control sobre los sujetos, públicos o privados, que disponen de sus datos personales.

Se crea así un nuevo modelo que, al reforzar la esfera privada, refuerza al mismo tiempo el peso del individuo en la esfera pública, constituyendo así un elemento básico de la que podemos denominar nueva ciudadanía electrónica, donde el test de "impacto privacidad" es imprescindible para juzgar el efectivo nivel de democracia del sistema político en cuestión.

Sexta

Y, finalmente, ¿qué implica la definición legal de dato personal? Siguiendo la máxima romana, toda definición en Derecho es peligrosa , luego los textos legales tienden a huir de las mismas. Pero, en esta supuestamente tecnificada materia sí se establecen, y,

además, la definición de dato de carácter personal es esencial, pues constituye el ámbito de aplicación objetivo de la normativa, es decir, en caso de que consideráramos que algo no es dato de carácter personal, la normativa no se aplicaría, por lo que pasamos a examinarla brevemente.

La LFTAIPG) en la fracción II del artículo 3 define datos personales como "la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten a su intimidad".

Como simple mención a los orígenes de la definición, expondremos un par de antecedentes en Derecho comparado.

Así, el Convenio (108) define en la letra a) de su artículo 2 el concepto de datos de carácter personal como: "cualquier información relativa a una persona física identificada o identificable ("persona concernida")".

Por su parte, la Directiva 95/46/CE, define en la letra a) del artículo 2 el concepto de datos personales de la siguiente manera: "toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Retomando la definición de la LFTAIPG, pasamos a analizar sus componentes.

Se trata de una definición amplia, al igual que los legisladores internacionales intentaron en sus propios textos, y así el mismo Parlamento Europeo decía que dicha definición debería ser tan amplia como fuera posible para incluir toda información referente a una persona identificable. Pero tampoco es un concepto ilimitado. El objetivo es proteger los derechos y libertades fundamentales individuales en lo que se refiere al tratamiento de datos personales. Así, el ámbito de aplicación de las normas no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de datos personales.

"La información": existen una serie de datos personales que todo el mundo identifica como tales, pero queda un gran espectro de información personal sobre la que no se tiene demasiado interés a menudo y que ni tan siquiera se considera como propia. No obstante, consideraciones sociológicas aparte, lo cierto es que la definición legal es, como dijimos, muy amplia, por lo que cabe toda información relacionada con una persona física, no sólo los datos ya comunes y habituales sino cualquier información que nos relacione con una persona física aunque ella misma lo desconozca.

Persona física: en la normativa mexicana sólo tiene sentido la protección de datos sobre los datos de las personas físicas . Podríamos hablar en este sentido de otras protecciones jurídicas, pero no de aplicación de la normativa en protección de datos de carácter personal..

Identificada o identificable: No sólo es que sepamos que cualquier información relacionada con una persona física es información de carácter personal, sino que, incluso cuando esa persona sólo pueda ser identificable , es decir, aunque no la tengamos identificada actualmente, eso sigue siendo información personal.

"Entre otra" y "otras análogas que afecten a su intimidad": en la definición se indican a modo de ejemplo algunos datos o clases de datos que entran dentro del concepto de dato personal y que por tanto tienen que ser protegidos por la LFTAIPG. Es decir, no se puede considerar, tal y como se deduce claramente de las expresiones "entre otra" y "otras análogas que afecten a su intimidad" utilizadas, que se trate de un numerus clausus, sino de una lista que queda abierta y en la que se proporcionan algunos ejemplos de lo que se considera dato de carácter personal.

Por otro lado, la LFTAIPG protege los datos personales bajo la figura de la información confidencial. No estamos de acuerdo con ello: no todos los datos personales son confidenciales, ni viceversa.

Un dato personal puede ser público o privado. No pierde su característica de dato personal por ser público, podría en algún caso tener que ceder algo de su protección, pero no pierde su esencia.

Finalmente, si los datos se someten a un procedimiento de disociación, que el lineamiento 20º define como "procedimiento por el cual los datos personales no pueden asociarse al titular de los datos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo", estos dejan de ser datos de carácter personal, porque pierden su característica más esencial, que es identificar o hacer identificable a una persona. En otras palabras, el dato deja de cumplir una función identificativa de la persona para convertirse en anónimo.

En conclusión, cualquier información, en cuanto asociada a un titular, es información de carácter personal, no por la información en sí, sino por su asociación con la persona física a la que se protege. Así, no se puede hablar de datos de carácter personal en sentido neutro, sino que tan sólo adquieren este carácter en cuanto se asocian a un titular.

III. Un poco de historia

Se suele decir que existen dos enfoques claramente diferenciados: el europeo y el estadounidense. Pero la normativa en protección de datos personales ha encontrado su

desarrollo en el continente europeo, y en la multitud de diferentes territorios que han adoptado su modelo, adecuándolo a su entorno socio jurídico (Japón, Australia, Canadá, Argentina, entre otros…) Por su parte, el denominado modelo estadounidense sólo se aplica en Estados Unidos.

Hay quien argumenta que esta preeminencia doctrinal y legislativa europea es la respuesta defensiva al injusto e ingente tratamiento y uso de la información personal por parte de los totalitarismos sufridos en diferentes países europeos durante el siglo XX, donde el control por parte del Estado de dicha información personal posibilitó en diversas ocasiones actos de barbarie. Sin embargo, esto no explicaría las también muy conocidas persecuciones sufridas en Estados Unidos y otros territorios .

Podríamos incluso intentar comparar las diferencias a grandes rasgos y decir que en Europa hay un enfoque social, los principios de protección se establecen en las leyes, el tratamiento de datos se da cuando es necesario, existen autoridades reguladoras independientes, y la protección se extiende a los no nacionales, mientras que en Estados Unidos el enfoque es individual, los alcances de la protección se delimitan ante los tribunales, el tratamiento de datos se realiza cuando es conveniente, el mercado es el regulador (con intervención de algún organismo sectorial como la Federal Trade Commission), y sólo se protege a los ciudadanos norteamericanos.

No obstante, a pesar de que muchos autores y políticos sostienen las grandes divergencias que entre los dos enfoques existen, no deja de haber voces que proclaman que las metas pueden ser idénticas, es decir, que se puede llegar al mismo punto aún partiendo de dos concepciones muy distintas .

Habiendo expuesto entonces la controversia entre los dos enfoques, pasamos a realizar un breve recorrido histórico internacional, europeo y estadounidense en la materia.

Ya la Declaración Universal de los Derechos Humanos, de 1948, establece en su artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Asimismo el artículo 8 del Convenio Europeo para la Protección de los Derechos y las Libertades Fundamentales, de 1950, reconoce bajo el derecho al respeto de la vida privada y familiar que : "1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2 No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, de

1966, afirma "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.".

La Convención Americana sobre derechos humanos de 1969 en su artículo 11, apartados 2 y 3, señala, bajo el epígrafe de "protección de la honra y de la dignidad" que "2. 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; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó en 1980 sus "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales", que constituyen el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos personales.

La Asamblea General de la Organización de las Naciones Unidas emitió la Resolución 45/95 en 1990 con una lista básica de principios como el de licitud, exactitud, finalidad, acceso, no discriminación, entre otros.

La Asociación para la cooperación económica Asia-Pacífico (APEC) enfocada en que la protección de datos acompañe el crecimiento económico emitió en 1998 su Marco de Privacidad, similar al de la OCDE, que establece los principios de prevención de daño, aviso, limitación a la recolección de información personal, usos de la información o datos personales, elección, integridad de la información personal, seguridad, acceso y corrección, y responsabilidad.

La Red Iberoamericana de Protección de Datos aprobó su Reglamento en Mayo de 2008 destacando su impulso e implantación del derecho fundamental a la protección de datos de carácter personal instando a los gobiernos a elaborar una normativa que logre la obtención de la declaración de adecuación por parte de la Comisión Europea.

En Europa, como sucinta mención normativa, podemos partir de la Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos de 1968, continuar con las Resoluciones del Comité de Ministros de 1973 y 1974, pasando por el Convenio 108 del Consejo de Europa , para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal y a la libre circulación de estos datos de 28 de enero de 1981; la Directiva 95/46/CE, por su parte, vino a asentar un régimen normativo específico, un marco definido para esta teoría, con el mandato consecuente de implantación para todos los Estados miembros, asimismo la Directiva 2002/58 hace lo propio en el sector de las comunicaciones electrónicas junto con la Directiva 2006/24/CE de retención de datos de comunicaciones electrónicas. Como logro especialmente importante, la Carta Europea de Derechos

Fundamentales, en su artículo 8, señala el derecho a la protección de datos de carácter personal como uno de los derechos fundamentales en el ámbito europeo. Finalmente, incluso, la polémica Constitución europea incorpora el artículo I-51 dedicado al derecho a la protección de datos personales.

Finalmente, el pasado 5 de noviembre de 2009 se aprobó y presentó la denominada Resolución de Madrid, que contiene los Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, en la sede de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada ese mismo día en Madrid .

Además del iter normativo (utilizando el adjetivo en sentido amplio), como hito histórico esencial, la conocida sentencia del Tribunal Federal Alemán de 1983, sobre la licitud del tratamiento de los datos por la Ley del censo de un ciudadano alemán, abrió un nuevo e importante camino en la protección de datos internacionalmente.

Podemos decir que en esta sentencia se asienta el conocido principio a la autodeterminación informativa -que la doctrina suele llamar, en un juego de palabras, "principio a la autodeterminación informátiCa" aludiendo al tratamiento automatizado de los mismos- que señala que el titular de los datos es el único que tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos, dando lugar a un importante desarrollo normativo internacionalmente.

En Estados Unidos tenemos que comenzar por el conocidísimo artículo de los Jueces del Tribunal Supremo, Samuel D. Warren y Louis D. Brandeis , de 1890, donde se explica la evolución de dicho derecho, apoyándose en un tratado muy renombrado sobre injurias de otro juez, llamado Cooley, donde defendía el derecho a "ser dejado en paz", y comienzan así a definir lo que se entiende por privacidad en la era moderna en dichos ordenamientos.

En Europa y Canadá, como decíamos, existen leyes nacionales comprehensivas que se aplican a través de diferentes categorías.

En Estados Unidos, existe un mosaico de leyes federales y estatales que protegen ciertos sectores , además de la denominada "autorregulación industrial" desarrollada esencialmente por el sector privado, y cuya efectividad depende, en gran parte, del poder de coacción de quien formula dichos códigos y de la aplicación de las sanciones previstas en ellos.

Como breve nota común a las mencionadas regulaciones podemos destacar los ampliamente aceptados fair information practice principles (Información (Notice), Elección (Choice), Acceso (Access) y Seguridad (Security)), que en 1973 desarrolló el Departamento de Sanidad, Educación y Bienestar de los Estados Unidos en su informe sobre la protección de la privacidad en la era de la recogida de datos.

IV. Escenario legal actual en México

El actual Plan Nacional de Desarrollo 2007-2012 plantea entre sus estrategias "Desarrollar el marco normativo que garantice que la información referente a la vida privada y a los datos personales estará protegida (…) es necesario el desarrollo de una Ley Federal (…) Dicha regulación deberá incluir los principios de protección de datos personales reconocidos por los tratados internacionales en la materia, que el Estado mexicano debe observar."

Así, antes de adentrarnos en el análisis de los principios, veamos brevemente en qué estado legislativo nos encontramos actualmente en México.

Lo anterior no es una misión sencilla, ya que el caos y la confusión parece prevalecer. Comencemos por lo relevante y medianamente claro.

De un lado, tenemos la reforma al artículo sexto de la Constitución incorpora un párrafo destinado a la protección de datos personales que después veremos. Aquí ya tenemos una pequeña "victoria" y reconocimiento al derecho -o mera garantía institucional, en su caso como dijimos antes-, aunque encuadrado dentro de la reforma al acceso a la información pública gubernamental.

De otro lado, actualmente están en discusión otras dos reformas constitucionales mucho más relevantes para la materia, la del artículo decimosexto, que estaría totalmente dedicada a la inclusión y protección de datos personales, y la del artículo Septuagésimo Tercero, para lograr una regulación a nivel federal del tema en el Sector Privado.

No obstante, como decíamos, en el entorno legislativo, la situación es sumamente confusa. El iter de iniciativas ha sido, como mínimo, desordenado. Se pueden encontrar unas cuantas generales, muchos incluso hablan de alguna "fantasma", e incluso algunas otras reformas de mayor o menor calado a diferentes cuerpos legislativos .

Como adelantábamos, la primera referencia a nivel constitucional que se encontraba, hasta el pasado 20 de julio de 2007, estaba en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos que establece que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones".

Sin embargo, con la publicación, el mencionado pasado 20 de Julio de 2007, en el Diario Oficial de la Federación, en sus páginas 2 y 3, del Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo Sexto de la Constitución, se hace una referencia explícita a la protección de datos personales, si bien dentro del artículo destinado al derecho de acceso a la información.

No obstante, en México, no existe aún una ley específica a nivel federal que regule específicamente la protección de datos personales, aunque sí existen referencias en diferentes cuerpos legislativos . Por su parte, a nivel estatal, el Estado de Colima sí cuenta con una regulación concreta desde el 2003, que sigue en gran medida la antigua y derogada

LORTAD española -tanto que, como mera curiosidad, habla de "ficheros" en lugar de "archivos"-, aunque sin que haya tenido aplicación en la práctica. Igualmente, por otro lado, Guanajuato, Jalisco y Sinaloa también han desarrollado previsiones legales al respecto, y la Ley de Protección de Datos del Distrito Federal se encuentra asimismo a punto de publicarse. Y, todo lo anterior sin olvidar que muchas de las reformadas leyes de transparencia dan un ámbito de actuación mayor a los Estados, por lo que habrá que esperar regulaciones cercanas y ambiciosas .

A pesar de lo anterior, la LFTAIPG, que, si bien es una norma cuyo objeto es, según dispone su artículo 1, "garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal", también destaca en su artículo 4 apartado III, como uno de los objetivos de la ley: "Garantizar la protección de los datos personales en posesión de los sujetos obligados", por lo que regula directamente la privacidad de los individuos cuyos datos personales son objeto de tratamiento por la Administración Pública Federal, planteándolo, al igual que la reforma constitucional, como un límite al acceso a la información, cuestión que entendemos desafortunada, pues, más que límite, es, en todo caso, complemento.

En el presente trabajo atenderemos, por razones de generalidad, a la regulación establecida por la LFTAIPG y a sus Lineamientos de protección de datos personales.

Es más, en realidad nos guiaremos fundamentalmente por los Lineamientos, porque desarrollan y profundizan en la regulación, pues, como dijimos, la LFTAIPG es claramente limitada a este respecto, entre otras cosas, porque no es una norma de protección de datos personales, sino de acceso a la información pública.

V. Los principios

Según los Lineamientos, los principios rectores de la protección de datos son la licitud, la calidad, el acceso y corrección, la información, la seguridad, la custodia y el consentimiento para la transmisión.

Dado que son, como apuntábamos, la referencia más clara de la doctrina del hasta ahora más general órgano de tutela seguiremos su agrupación en el análisis por cuestiones didácticas teniendo en cuenta la coyuntura regulatoria actual.

Sin embargo, queremos dejar claro desde el inicio igualmente que no estamos de acuerdo con no mencionar otros principios esenciales, especialmente el del consentimiento en origen, aunque sea aclarando que no se necesita por estar en una excepción al mismo, entre esos principios rectores de carácter general

Pasamos entonces a analizar muy sencillamente dichos Lineamientos evitando engorrosos reenvíos legales a otros textos para simplificar la exposición.

Licitud

El artículo 6º de los Lineamientos, bajo el epígrafe de "Licitud" dice que "la posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones"

Como decíamos, los Lineamientos, siguiendo su ámbito subjetivo particular, tan sólo establece el consentimiento en la fase de transmisión, sin tratarlo en origen.

En nuestra opinión, aunque en este artículo 6º.1 establece la licitud del tratamiento al reiterar que sólo será posible aquél que esté dentro de las atribuciones legales o reglamentarias de la dependencia, debería especificar que por tanto no es necesario dicho consentimiento, es decir, que se excepciona el mismo. Sin embargo, entendemos que no se haya hecho así, porque no podría irse vía Lineamientos contra la reglamentación de la LFTAIPG, que no trata tampoco el consentimiento en origen.

Es más, al establecer que el tratamiento sólo podrá hacerse dentro de dichas atribuciones, en realidad está supliendo, incluso de una manera muy magistral, la posible ilicitud ab initio de dicho tratamiento. Es decir, los Lineamientos, en este punto, parecen estar diseñados por alguien que ha tenido muy claro dicha deficiencia y la ha salvado con una excepción general al consentimiento, la atribución legal o reglamentaria, pero esto, en nuestro parecer, no tendría por qué haber impedido una referencia más general al consentimiento.

Y continúa el lineamiento entendiendo asimismo que la licitud también comprende que "los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos".

Sólo se podrá valorar la bondad de un tratamiento en cuanto a los fines del mismo, que deben de ser determinados y legítimos, por cuanto circunscriben las posibilidades de actuación sobre los datos objeto del mismo en relación, reiteramos, con la finalidad. Parece un círculo vicioso –o virtuoso- pero no hay tratamiento legítimo (ni lícito) si su finalidad no está determinada, y ésta no puede tampoco ser válida si no lo es a su vez.

Calidad

El artículo Séptimo de los Lineamientos, acerca de la Calidad de los datos, dice que "el tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo respecto de las atribuciones legales de la dependencia o entidad que los posea".

En nuestra opinión, estas cualidades deberían predicarse no respecto de las atribuciones de la dependencia, sino de la finalidad del tratamiento, que además debe de estar previsto dentro de dichas atribuciones, porque, si no, podría decirse que se cumple con la calidad porque la atribución legal lo permite cuando en realidad no se estaría cumpliendo por estar fuera de la finalidad del tratamiento en sí.

Es decir, las atribuciones legales de las dependencias son mucho más amplias que las finalidades de tratamientos concretos llevados a cabo por las mismas.

Además, al omitir la posibilidad de atribuciones reglamentarias previstas en el artículo anterior -por descuido, error o voluntad- circunscribe excesivamente dichas atribuciones.

Por otro lado, el lineamiento 14º obliga a los Responsables, Encargados o usuarios que detecten que hay datos inexactos a actualizarlos de oficio en cuanto tengan conocimiento de la inexactitud y siempre que posean los documentos justificativos que justifiquen la actualización. Si bien pudiera parecer que deja abierta la puerta a la indefinición temporal, no es muy sencillo que pueda concretarse más este extremo, y, al exigir contar con documentación acreditativa del hecho subsana posibles actualizaciones carentes de prueba justificativa posteriormente.

Acceso y corrección

El lineamiento 5º tan sólo señala que los sistemas deberán almacenarse para permitir el ejercicio de los derechos de acceso y corrección en los términos previstos en la Ley, el Reglamento y los Lineamientos.

Por lo tanto, el principio, aún denominado acceso y corrección, en realidad no desarrolla nada, y además, en nuestra opinión, no es la colocación adecuada sistemáticamente hablando, por lo que nos remitimos a su análisis en el apartado destinado a los derechos.

Información

Es otro principio general de protección de datos que todo ciudadano tiene derecho a ser informado de determinados extremos cuando se le solicitan datos de carácter personal con el fin de que conozca quién, cómo y para qué los va a tratar, así como poder ejercitar, en su caso, los derechos que la Ley le reconoce.

Así, el Lineamiento 9º dice que se debe hacer del conocimiento del titular de los datos al momento de recabarlos y de forma escrita el fundamento y motivo de ello, así como los propósitos para los que se tratarán dichos datos.

Seguridad

La implementación del principio de seguridad deviene esencial para impedir el acceso a los sistemas de datos personales, en particular, y a los datos en general, a personas no autorizadas, o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos, además de para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado, asegurando la confidencialidad y la integridad de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado.

El lineamiento 20º, al hablar de seguridad, dice que se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado y posteriormente el capítulo IV se dedica a ahondar detalladamente en dichas medidas de seguridad .

Custodia y cuidado de la información

El lineamiento 11º señala que los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento, sin que exista una obligación similar en la LFTAIPG.

Consentimiento para la transmisión

El eje central de las normativas en protección de datos es el principio del consentimiento, por el que el titular de los datos es el único que tiene derecho a decidir quién, cómo, cuándo y para qué se tratan sus datos, derivado claramente del derecho a la autodeterminación informativa comentado antes.

Es cierto que hay quienes defienden que el principio fundamental es el de calidad de los datos, argumentando que no tiene ninguna excepción, que siempre debe cumplirse, mientras que el de consentimiento, si bien también esencial en su opinión, sí cuenta con estas excepciones.

En nuestra opinión, lo anterior implica mezclar conceptos. El principio del consentimiento no es una cualidad o adjetivo del tratamiento, sino el eje del mismo. El hecho de que tenga excepciones no quiere decir que no sea la regla, sino más bien lo contrario.

La protección de datos gira en torno al individuo, a la persona, que es a quien se protege, no a los datos, ni al tratamiento de los mismos con una finalidad determinada.

Si bien es absolutamente imprescindible definir la finalidad del tratamiento, en tanto en cuanto sólo se pueden tratar datos con una finalidad explícita, legítima y determinada, lo que de verdad es irrenunciable es la característica subjetiva del derecho que va indisolublemente unido a la persona, cuyo consentimiento, aunque prescindible en algunos casos en pos del equilibrio de derechos fundamentales e intereses en conflicto, constituye la manifestación más relevante de dicha subjetividad.

El consentimiento se articula en cierta medida en el Lineamiento 12º, aunque no se contempla nada acerca de la necesidad del consentimiento para el tratamiento en origen o posterior de datos personales.

Sólo se exige, excepciones aparte, en la fase en la que los datos se transfieren a un tercero, es decir, cuando se produce la transmisión de datos a terceros, en la que el titular

pierde, en su caso, aún más el control sobre su información personal. No obstante, ya hemos dicho al hablar de la calidad que los lineamientos no podían señalar lo contrario ya que irían contra la regulación de la LFTAIPG.

El tratamiento de datos, según la propia definición de la LFTAIPG, no sólo se refiere a la transmisión -definida en el artículo 21 de la LFTAIPG como "difundir, distribuir o comercializar los datos personales"- sino que incluye la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y transmisión de datos personales, y, por lo tanto, todo tratamiento debería requerir del consentimiento, como regla general, y no únicamente en esa fase posterior de transmisión.

Además, el Lineamiento 23 va más allá y exige que cuando el consentimiento no esté excepcionado para la transmisión, entonces se necesitará que una disposición legal lo prevea de modo expreso y que medie el consentimiento expreso de los titulares. En nuestra opinión, al exigir los dos requisitos rompe de nuevo el principio vertebral, pues el consentimiento por sí solo no parece bastar para la transmisión.

El consentimiento deberá otorgarse en forma libre, expresa e informada. Además tendrá que darse por escrito incluyendo la firma autógrafa y la copia de la identificación oficial o bien mediante un medio de autenticación, debiendo en todo caso las dependencias cumplir con las disposiciones sobre firmas electrónicas.

En cuanto a la forma en la que se puede otorgar el consentimiento, con carácter general cabe distinguir entre consentimiento presunto, tácito, expreso y expreso por escrito .

En cualquiera de los casos señalados, la cuestión se centra en la prueba de la obtención del consentimiento, que recae en quien dice tenerlo.

Es decir, tanto en el consentimiento tácito, principalmente, como en el expreso que no sea escrito, parece que hay que implementar procedimientos estandarizados de obtención de dicho consentimiento a efectos de prueba posterior.

Otras obligaciones y materias relacionadas

A pesar de que las normas internacionales sobre protección de datos hacen referencia, de una u otra manera, a unas categorías especiales de datos, también denominados datos sensibles, que, por su especial naturaleza, requieren de un mayor grado o nivel de protección para garantizar la privacidad de los ciudadanos (entre los que podemos citar origen racial, vida sexual, salud, ideología, religión, creencias y afiliación sindical), la normativa mexicana no hace distinción alguna en lo que a estas distintas clases de datos de carácter personal se refiere.

En otro orden de cosas, la necesidad y utilización real de terceros que presten determinados servicios que implican acceso a los datos por los mismos, se recoge en las

distintas legislaciones internacionales en protección de datos como una figura distinta de la transmisión de datos ya comentada.

En la prestación de servicios, o acceso a los datos por terceros se establece un encargo por parte del responsable del sistema de datos a un tercero para que se le preste un servicio determinado.

En la transmisión se produce una transferencia de datos del responsable a otro responsable para que éste haga con los datos lo que considere pertinente en relación con la finalidad prevista, perdiendo el originario responsable el control sobre dichos datos, mientras que en la prestación de servicios el prestador sólo hace con los datos lo que el responsable originario le encargó que hiciera.

El lineamiento 21º dice que cuando se contrate a terceros para que realicen el tratamiento de datos personales deberá estipularse en el contrato respectivo la implementación de medidas de seguridad y custodia así como las penas convencionales por incumplimiento.

VI. Los derechos

Vistos los principios que rigen el tratamiento de datos, la normativa prevé la existencia de unos derechos de los titulares de dichos datos en los que se concretan los mencionados principios, como instrumento propicio para controlar el tratamiento que haga el responsable del sistema de datos personales.

En el entorno internacional hispanoparlante goza de cierta popularidad denominarlos como los derechos "ARCO", acrónimo que sintetiza el acceso, rectificación, cancelación y oposición.

El derecho de acceso (regulado en los arts. 20 y 24 LFTAIPG y en el artículo 47 de su Reglamento) faculta a los titulares de los datos para solicitar al responsable del sistema de datos personales información relativa al tratamiento de sus datos personales, pudiendo conocer qué datos tiene sobre él y a quiénes se van a comunicar.

Los derechos de rectificación y supresión (según el art. 25 de la LFTAIPG) permiten al titular de los datos, por un lado, solicitar la modificación, en los casos de que los datos sean inexactos, y cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados, requerir su cancelación.

Otro de los derechos previsto en la LFTAIPG (en su art. 23 y 48 del Reglamento) es el derecho de consulta por los interesados a un Registro público al que los responsables de los sistemas de datos personales notifiquen la existencia de los sistemas de datos de carácter personal, y que va a permitir a los interesados obtener información con el propósito de poder dirigirse a su responsable para ejercitar sus derechos.

Así, el "Sistema Persona" se crea en el Capítulo VI de los Lineamientos para facilitar el ejercicio de los derechos de acceso y corrección de los particulares, incluyendo asimismo el derecho de consulta a dicho Sistema.

Finalmente, como decíamos, en las legislaciones internacionales existen otros derechos, como el derecho de oposición recogido en la Directiva 95/46/CE europea, que consiste en que el titular, en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos, pero la breve normativa mexicana, repetimos, no específica en protección de datos, no lo contempla.

Asimismo, la norma europea mencionada también prevé otro derecho relativo a la posibilidad del titular de los datos de impugnar las valoraciones que de él se hagan como resultado del tratamiento de sus datos de carácter personal. Por último, en otras normativas nacionales se prevén otros derechos concretos, como el derecho de los interesados a recurrir a los Tribunales con objeto de obtener una compensación cuando se hayan vulnerado sus derechos, respecto a otros bienes jurídicos protegidos, como el derecho al honor y a la intimidad.

Por otro lado, nos parece importante asimismo volver a recalcar que no sólo se tienen derechos, pues, además de las limitaciones que los derechos de los demás imponen a los propios, que deben ceder, por ejemplo, ante un interés o bien público, el titular de los datos tiene un deber de diligencia o de cuidado sobre los mismos.

El individuo debe ser consciente del valor de sus datos y su posterior utilización, y actuar en consecuencia, para que si consiente a que se traten sus datos lo haga de una manera sensata y razonada, evitando comerciar con ellos a cambio de regalos, premios o invitaciones puntuales que en muchas ocasiones conllevan el consentimiento para su utilización con múltiples finalidades.

VII. El procedimiento y la Autoridad de Control

Para cerrar el triángulo del que hablábamos al principio, tenemos que tratar el vértice procedimental, al que puede recurrir el titular de los datos lesionado en sus derechos.

El histórico "habeas corpus" protegía la integridad corporal del sujeto. El "habeas data", como evidente desarrollo del anterior, protege la integridad corporal electrónica del sujeto, es decir, la información personal.

En el caso mexicano, al ser esta regulación muy escasa, lo cierto es que más que de procedimiento vamos a hablar de la necesaria existencia de una autoridad de tutela ante la que se gestionaría dicho procedimiento.

En el artículo 33 de la LFTAIPG se prevé que el Instituto Federal de Acceso a la Información Pública es "un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades."

En España, por poner un ejemplo de un país concreto de similar tradición jurídica y en este caso de más asentado respeto a la materia, en principio existen dos procedimientos diferenciados en materia de protección de datos: el denominado "tutela de derechos" y el "procedimiento sancionador". En realidad, para ser puristas, el único procedimiento que el titular de los datos puede originar es el de tutela de derechos, es decir, cuando se ve lesionado en sus derechos puede acudir ante el órgano competente, la Agencia Española de Protección de Datos en el ámbito nacional y las Agencias autonómicas (locales/"cuasi federales") existentes en el caso de los archivos públicos de las comunidades autónomas que cuenten con dicha Agencia. El procedimiento sancionador, por su parte, sólo puede ser instado por la Agencia, por su Director, aunque pueda traer causa, sin que esto sea muy formal decirlo, de una denuncia previa y un expediente de tutela de derechos.

El IFAI, por su parte, cumple con alguna de las funciones en materia de control y tutela de los derechos de la normativa en protección de datos, sin que pueda afirmarse que exista en México, en la actualidad, un verdadero procedimiento en la materia, al estilo de lo que se ha denominado el "habeas data" como mecanismo de protección y tutela del ciudadano que se ve lesionado en su derecho a la protección de datos, ni que el IFAI sea una autoridad o órgano de control en la materia, como en las normativas internacionales se configura.

El procedimiento ante el IFAI se regula en los artículos 49 a 60 de la LFTAIPG, pudiendo iniciarse en concreto ante la negación de acceso a la información o la inexistencia de los documentos solicitados.

Finalmente, la LFTAIPG prevé como causas de responsabilidad las acciones y omisiones que se indican en el artículo 63 y será exigida conforme a lo dispuesto en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, resaltando, de nuevo, que las sanciones se refieren a la "información", pues, de nuevo, tenemos que repetir que la LFTAIPG sólo destina un capítulo, de 7 artículos, y algunas referencias más dispersas, a la protección de datos.

VIII. Otras cuestiones

Dentro de la normativa de protección de datos de carácter personal hay muchos otros temas de especial relevancia, como la transferencia internacional de datos, o tratamien-

tos de datos específicos (como datos de salud, datos con fines de solvencia patrimonial y crédito o datos en el entorno de las telecomunicaciones), o, finalmente, la existencia y, en nuestra opinión, necesario fomento de la utilización de códigos de conducta, éticos o deontológicos.

Todos ellos son aspectos concretos de la regulación que sería imposible tratar en este trabajo por razones de espacio y metodología, pero entendemos especialmente interesante por diversas cuestiones detenernos brevemente en la problemática de la transferencia internacional de datos y la utilización de códigos de conducta.

La transferencia internacional de datos

La globalización del comercio, en el más amplio sentido de la palabra, conlleva en la mayoría de las ocasiones la necesidad de tratar datos de carácter personal, dando lugar a la Transferencia Internacional de Datos (TID) entre diversos países.

Estos tratamientos tienen que adecuarse a las previsiones legales establecidas en los diversos ordenamientos jurídicos en juego, que tienen como fin garantizar al individuo, cuyos datos son objeto de tratamiento, su derecho fundamental a la protección de datos , y así facilitar la realización de transacciones internacionales , comerciales y no comerciales.

La legislación europea exige para realizar cualquier transacción que involucre datos de carácter personal, es decir, casi todas, que el destinatario cuente con un nivel adecuado de protección, bien vía país de destino o vía contractual.

En este sentido, la legislación europea establece unas reglas muy delimitadas para que estas TID se puedan llevar a cabo. Así, los principios que rigen esta regulación son:

1. Prohibición de transferencias a un país tercero que no garantice un nivel de protección adecuado (art. 25.1 Directiva 95/46/CE).

   Lo que nos lleva inmediatamente a preguntarnos qué se entiende por nivel de protección adecuado. El artículo 25.2 de la Directiva dispone que dicho carácter adecuado se evalúa atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos, y, en particular: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. En definitiva, se busca que el sistema de protección proporcione un buen nivel de cumplimiento de las normas, apoyo y ayuda a los sujetos de datos individuales en el ejercicio de sus derechos y una reparación adecuada a las partes perjudicadas cuando no se cumplan las normas . La Comisión podrá adoptar una Decisión en la que establezca que un país tercero ga-

rantiza un nivel de protección adecuado, en cuyo caso los Estados miembros tendrán que adoptar las medidas necesarias para adecuarse a la misma (art. 25.6 Directiva 95/46/CE).

2. No obstante, la Directiva prevé a continuación una serie de excepciones a los principios en su artículo 26, como el consentimiento inequívoco del interesado, la ejecución de un contrato con determinados requisitos, o la salvaguardia de un interés público importante o para el reconocimiento de un derecho en un procedimiento judicial.

3. Finalmente, también se podrá autorizar esta TID cuando el responsable del tratamiento ofrezca garantías suficientes, pudiendo incluirse las mismas en cláusulas contractuales apropiadas, incluyendo la utilización de unas cláusulas contractuales predispuestas y redactadas por la Comisión.

En la actualidad, podemos decir que las TID en función del país destino se podrán realizar conforme a la legislación europea:

En caso de que el país tercero destinatario de los datos esté declarado como país que proporciona un nivel adecuado de protección. Aquí se encontrarían las siete Decisiones de la Comisión Europea declarando a Suiza, Hungría (aunque esta Decisión está ya un poco vacía de contenido porque Hungría ya pertenece a la Unión Europea), Canadá, Argentina, Guernsey, Isla de Man y Jersey, como terceros países que proporcionan un nivel adecuado de protección. En el caso de Estados Unidos se declara la adecuación mediante un sistema de adhesión voluntaria al programa de "Puerto Seguro". La sustancial diferencia entre estos dos grupos es que las primeras determinan que las legislaciones de dichos países garantizan un nivel adecuado de protección, mientras que en el caso de EE.UU. no se está reconociendo que proporcione un nivel de protección adecuado, sino que son las entidades que cumplen con el Acuerdo de Puerto Seguro las que obtienen la presunción de "adecuación".

En el caso de que el país de destino no proporcione un nivel adecuado de protección y no estemos en una de las excepciones del art. 26 de la Directiva se podrá optar por el contrato propuesto por la Comisión, cuyas cláusulas ofrecen las garantías respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas y el respeto al ejercicio de los respectivos derechos. Estas cláusulas contractuales tipo han sido aprobadas mediante las correspondientes Decisiones de la Comisión, en función de cuál sea la finalidad de la transferencia y se refieren únicamente a la protección de datos, pudiendo añadirse por las partes del contrato aquellas otras necesarias para el desarrollo de su negocio.

En definitiva, se puede realizar una TID a un país tercero, cuando se tenga el nivel adecuado de protección o se esté en una excepción, o, finalmente, se utilice un mecanismo de cláusulas contractuales .

Por su parte la normativa mexicana en el Lineamiento 24 dice: "En caso de que el o los destinatarios de los datos sean personas o instituciones de otros países, las dependencias y entidades deberán asegurarse que tales países garanticen que cuentan con niveles de protección semejantes o superiores a los establecidos en estos Lineamientos, y en la normatividad propia de la dependencia o entidad de que se trate."

El Acuerdo de Puerto Seguro

El denominado Acuerdo de "Puerto seguro" es una excepción a las demás Decisiones adoptadas por la Comisión, fruto de las intensas y no siempre exentas de polémica negociaciones mantenidas, durante más de dos años, entre el Departamento de Comercio de Estados Unidos y la Comisión Europea, partiendo de los diferentes enfoques que los EE.UU. y la UE dan a la protección de la vida privada de sus ciudadanos, basándose el planteamiento de los EE.UU. en una mezcla de normas legales y autorregulación por parte del sector privado.

Es un Acuerdo muy complicado, tanto que normalmente estas Decisiones sobre el nivel adecuado tienen una extensión de un par de hojas, y este Acuerdo es muy largo, precisamente por todas las complicaciones de gestión y de negociación que conllevó .

En el Acuerdo de Puerto Seguro la Comisión no declara, al contrario que en el resto, que Estados Unidos sea un país con un nivel de protección adecuado, o equiparable a la Unión Europea, sino que se acuerda que las entidades estadounidenses, que voluntariamente decidan adherirse a los principios contenidos en el mismo, podrán recibir datos personales de responsables establecidos en alguno de los Estados miembros de la UE al entenderse que las mismas proporcionan una protección suficiente.

El Acuerdo se compone de unos Principios -que, en opinión de la mayoría de las autoridades europeas, son muy laxos, máxime en comparación con sus legislaciones nacionales- y de unas Preguntas Más Frecuentes que explican dichos principios.

Las entidades que puedan y quieran adherirse a este Acuerdo tienen que adherirse a un programa de autorregulación que ya contenga dichos principios o bien por autorregulación de la entidad en cuestión si dicha autorregulación los respeta. El método de adhesión es por un sistema de autocertificación, mediante una carta firmada por uno de los responsables de la entidad, ante el Departamento de Comercio, y aplicándose sobre todos los datos personales recibidos desde la Unión Europea.

Las cláusulas contractuales tipo

Tal y como decíamos, existe una tercera vía disponible desde la norma comunitar-

ia que puede calificarse como una solución específica a la necesidad de garantizar el cumplimiento de las disposiciones en materia de protección de datos en el caso de aquellas transferencias de datos que se efectúan con destino a países que no proporcionan un nivel adecuado de protección, tanto si se trata de una transferencia que tenga por objeto la comunicación de los datos a un responsable del tratamiento establecido en un país tercero como si es a un encargado del tratamiento para la prestación de un servicio por cuenta del responsable del tratamiento.

Con este fin, la Comisión Europea ha aprobado dos Decisiones que tienen por objeto aprobar clausulados contractuales tipo que contemplan las transferencias efectuadas a países terceros que no otorguen un nivel de protección equivalente al que proporciona la Directiva.

Así, en concreto, la Comisión está trabajando en las conocidas "Binding Corporate Rules (BCR)" o Reglas Corporativas Vinculantes, que es un catálogo de medidas en protección de datos aplicables a las empresas multinacionales y demás grupos similares que garantizan un nivel adecuado de protección cuando la información es transferida fuera de la Unión Europea a un país que no tiene dicho nivel .

Pero evidentemente, dado que los modelos tipo que proporciona la Comisión son una guía orientativa, las partes también pueden diseñar su propia solución contractual, que deberá ser evaluada mediante los mismos criterios que para un sistema de protección de datos ya hemos mencionado.

Los Códigos Tipo

Los códigos tipo, o deontológicos, o de buena conducta o práctica profesional, son un elemento de autorregulación especialmente apropiado para el entorno del Derecho de las Nuevas Tecnologías , y, más en concreto, para la generación de la tan nombrada y necesitada confianza.

Cuando hablamos de autorregulación no queremos con ello decir que estos códigos puedan sustituir a la regulación clásica, y menos en los países de nuestro entorno, claramente guiados por el sistema regulatorio, en contra de otros ordenamientos que promulgan y fomentan mucho más la participación industrial en estos temas, como el estadounidense ya mencionado.

La autorregulación, plasmada en los códigos de conducta y en otras medidas que tienen por objeto garantizar la privacidad de los usuarios, se configura como una solución complementaria especialmente adecuada al esquema legislativo, y como un modo de hacer y dirigir los negocios, con respeto a la normativa.

Se debe prestar especial atención a las garantías de cumplimiento y respeto de estos códigos, como la obtención de una satisfacción en caso de incumplimiento de lo dis-

puesto, o, simplemente, el establecimiento de unos procedimientos serios y consistentes en relación con una posible reclamación.

Si no se establecen, y se cumplen, las mencionadas reglas, se puede caer fácilmente en una mera declaración de principios o intenciones que no justifique en realidad la existencia del código, es más, que ni tan siquiera sea un código como tal.

Las notas que caracterizan a la autorregulación frente a las normas emanadas de un poder público son las siguientes:

Derivan de la iniciativa de un sector concreto, público o privado, pero nunca del propio Estado que es el único órgano con el poder necesario para la elaboración de una norma legal.

Si bien pueden haber previsto un mecanismo de sanciones en caso de incumplimiento de las normas contenidas en el mismo, estas pueden ser insuficientes al no ser impuestas por un órgano superior, como es el caso del Estado.

Dan una respuesta mucho más rápida ante situaciones de vacío legal o cuestiones que requieren un tratamiento específico para su posterior regulación.

IX. La reforma al artículo 6 de la Constitución

Pasando al comentario de la inclusión en la Constitución, el pasado 20 de julio de 2007, de un nuevo artículo 6 que engloba a la protección de datos, si bien dentro del derecho al acceso a la información del ciudadano, nuestra opinión se podría resumir, con los riesgos que ello conlleva, en lo ya dicho anteriormente respecto del objeto de la LFTAIPG, es decir, que dicha colocación dentro del artículo del derecho de acceso puede llegar a dar a entender, a no ser que se profundice en la interpretación, que también la Constitución plantea a los datos personales como un límite al acceso a la información, cuestión que, como decíamos, entendemos desafortunada, pues, más que límite, es, en todo caso, complemento.

En lo que afecta a protección de datos personales la reforma ha sido la siguiente: "Artículo Único.- Se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 6o.- ... Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: (…) II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. 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 pro-

cedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión. VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes."

Como breves comentarios a esta reforma, podemos hacer los siguientes:

En todo caso, alabamos la inclusión en el texto constitucional del absolutamente ya reconocido y establecido internacionalmente derecho a la protección de datos. Pero no podemos dejar de preocuparnos, como decíamos, ante la colocación de la referencia, como un límite al derecho de acceso a la información aparentemente. Las interpretaciones siempre son peligrosas en Derecho, y nos inquieta que el legislador no profundice sobre el verdadero sentido de la protección de datos, de manera independiente.

El texto diferencia entre la vida privada y los datos personales. Como decíamos supra los conceptos se interrelacionan. No obstante, por supuesto que la vida privada y los datos personales son dos cosas diferentes . Lo que la normativa en protección de datos personales trata de proteger es el tratamiento de la información personal por terceros, máxime en un entorno automatizado. El concepto de vida privada es más subjetivo, y depende de parámetros personales e individuales . La normativa gira en torno a cuestiones objetivas, donde el tratamiento de los datos personales, públicos o privados, tiene que seguir unas ciertas reglas. Sin embargo, lo que sí resulta en todo caso resaltable, como decíamos, es que se exige la protección.

El párrafo III ordena: "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", puede parecer algo exagerado si no se analiza un poco más detenidamente. No se está otorgando nada que no se deba, salvo una precisión acerca de la gratuidad infinita que haremos a continuación. El titular tiene acceso a sus datos, porque son suyos. El hecho de que no tenga que acreditar interés o justificar nada es porque accede a algo que le concierne a él mismo. No obstante, en relación con la rectificación creemos que, de nuevo, el desarrollo legal posterior deberá concretar este extremo. Cuando se va a rectificar un dato se tiene que demostrar, en lo que esto signifique en cada caso, que es erróneo, pues, de otra manera el titular del archivo podría tener consecuencias no deseadas. Es decir, no se tendrá que justificar la rectificación, o, en su caso, en un paso más allá, la cancelación, si por justificar se refiere el texto a, coloquialmente, "dar explicaciones", pero sí tendrá el titular de los datos, aunque esta sutil diferenciación parezca contradictoria, que probar, en la mayoría de los casos, de alguna manera dicha rectificación, aportando los datos pertinentes, adecuados y exactos.

No obstante, continuando con el párrafo III, y a pesar de que alabamos la intención garantista del constituyente en relación con los derechos en que se concreta la protección de datos, es igualmente cierto que la excesiva apertura, especialmente en lo relacionado

a la obligatoria gratuidad (párrafo III) de dicho derecho puede ocasionar problemas indeseados en la práctica, ya sea por negligencia, o, incluso, aprovechamiento por parte del no siempre indefenso titular de los datos. No obstante, si en el desarrollo legal, o reglamentario, posterior, se circunscribe este extremo de una manera justa y equitativa que no impida el comercio preservando dichas garantías, diciendo, por ejemplo, que será gratuito en la primera ocasión y siempre que no se repita en un plazo adecuado, entonces no veríamos ningún problema.

Por su parte, y como ya hemos visto en la exposición teórica antecedente, la concreción del extremo procedimental (párrafo IV) resulta indispensable. El único problema es que el párrafo expresamente sólo se refiere al acceso a la información. No obstante, en una labor exegética lo cierto es que podríamos entender que también se tendría que hacer en las mismas condiciones para el acceso a datos personales. En todo caso, lo que queremos resaltar es que sin el establecimiento de un procedimiento adecuado y expedito el derecho se quedaría vacío de contenido, al menos en parte. Es fundamental que se prevea una autoridad independiente, con plena capacidad de obrar y de decisión propias, que no tenga que estar sujeto a ningún poder en concreto, por lo menos en términos de sumisión. Hay que resaltar que la protección de datos es una materia que se introduce en todos los ámbitos de la sociedad en general. En la actualidad no existe actividad alguna que no requiera en algún momento del tratamiento de la información personal, y, por ende, no puede haber ningún ámbito que se sustraiga a la debida tutela.

Finalmente, las sanciones son imprescindibles, máxime en una materia como la que nos ocupa, de nueva introducción y gran desconocimiento, inclusive para el titular del derecho en sí. Sin unas adecuadas sanciones, severas pero proporcionadas al caso y las circunstancias, y un procedimiento eficaz y eficiente con una autoridad de tutela garantista, el derecho, como ya habíamos dicho, queda vacío de contenido, de fuerza y eficacia en la práctica.

X. La reforma al artículo 16 Constitucional

La propuesta de la Comisión de Puntos Constitucionales de reforma del artículo 16 constitucional, fue aprobada por el Senado el 4 de diciembre de 2008 y por la Cámara de Diputados el 11 de diciembre de 2008.

Conceptualmente engloba mucho más coherentemente la materia tratada, como la misma reforma señala "el texto que se dictamina permitiría concluir el trabajo iniciado con la reciente reforma al artículo 6 de la CPEUM (…) y por su parte el artículo 16 establecerá el derecho a la protección de datos personales, que, aunque mencionado en la fracción II del 6° se estaría dotando finalmente de contenido a este derecho fundamental".

Asimismo señala como su propósito "consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, apuntalando, por una parte, la estructura edificada a través del artículo 6 fracción II de la Constitución Federal y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder del sector privado".

El texto de la reforma propuesta es el siguiente: "Artículo Único. Se adiciona un segundo y tercer párrafos recorriéndose los subsecuentes en su orden al artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: "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 terceros."

Como breves comentarios a esta iniciativa, podemos hacer los siguientes:

En primer lugar, como ya decíamos, la inclusión del reconocimiento independiente y autónomo del derecho en este artículo constitucional es mucho más pertinente y adecuada.

"toda persona": el término persona da cabida, a menos de que posteriormente se circunscribiera, lo que parece difícil al venir así dispuesto en la norma constitucional, a las personas morales.

"derecho a acceder a sus datos personales": el ejercicio de los derechos es personalísimo, sólo puede ser por su titular o el representante del mismo en caso de incapacidad legal.

"en su caso, obtener su rectificación, cancelación": la atención a los derechos de rectificación y cancelación no implica necesariamente la concesión de los mismos. El titular de los datos deberá justificar y probar con la documentación acreditativa pertinente dichos cambios, y, además, puede suceder que el responsable del archivo entienda que no procede dicha rectificación o cancelación.

"manifestar su oposición": la filosofía subyacente a este derecho, con claras aplicaciones al entorno publicitario, es, como dijimos, la posible negación del titular en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, cuando existan motivos fundados y legítimos, y el responsable del archivo tendrá que proceder a la exclusión de los mismos.

"Supuestos de excepción": tal y como señala la iniciativa, hay dos finalidades importantes al recalcar la existencia de las excepciones: "dar certidumbre al gobernado

respeto de los casos en los que será posible tratar sus datos sin que medie su consentimiento, desde el nivel constitucional" y "dejar claro que este derecho encuentra límites frente a otros, en los que previa valoración de las circunstancias particulares, el derecho a la protección de datos puede ceder frente a los mismos".

XI. La reforma al artículo 73 Constitucional

Por su parte, la Iniciativa de la Comisión de Puntos Constitucionales de reforma del artículo 73 constitucional, asimismo aprobada por unanimidad por el Pleno de la Cámara de Diputados el pasado 20 de septiembre de 2007, y por el Senado el 4 de diciembre de 2008, tiene como finalidad "otorgarle la facultad exclusiva al Congreso de la Unión de legislar en materia de protección de datos personales en posesión de los particulares".

El texto propuesto dice: "Artículo Único. Se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 73. El Congreso tiene facultad: XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de particulares."

La justificación de la reforma incide en que los datos se utilizan usualmente para llevar a cabo transacciones comerciales y dicha materia es competencia exclusiva federal.

Como ya hemos visto, en la actualidad el IFAI tiene competencia sobre los datos personales en poder de la Administración Pública Federal, pero lo que la Iniciativa persigue es que los datos en posesión de los particulares, es decir, del Sector Privado, no puedan ser sometidos a legislaciones estatales, ya que se podría dar de facto lugar a desigualdades y mercados territoriales de información personal.

XII. Algunas reflexiones finales

El derecho a la protección de datos de carácter personal se encuentra aún lejos de ser valorado en su magnitud. No sólo es generalmente desconocido, sino, lo que es peor, minusvalorado.

El individuo tiene derecho a decidir cuándo, cómo y quién va a tratar su información personal.

A pesar de ser un derecho elevado a la categoría de fundamental en muchos ordenamientos, aún no se puede decir que se encuentra en igualdad de condiciones en la práctica, al menos respecto de los demás derechos fundamentales.

En América Latina queda mucho trabajo por hacer en relación con la privacidad, pues la mayor parte de los países no tienen una regulación en la materia. México no

cuenta tampoco con una regulación federal específica, si bien se observan movimientos hacia ello, como la reforma del artículo sexto constitucional y la propuesta al artículo 16 del mismo texto, que confiemos den pronto los frutos esperados afirmando la necesaria independencia y autonomía del derecho a la protección de datos personales.

La privacidad es irrenunciable, inalienable, y, más aún en una sociedad en la que, como hemos dicho, el valor más importante es la información. En consecuencia, la información personal aún debería adquirir una relevancia mayor dentro de la escala de gradación.

En cuanto a su relación con otros derechos o intereses, en nuestra opinión, el justo medio, aún tan difícil de encontrar, parece la solución adecuada. Se debe garantizar la privacidad, y afirmamos al mismo tiempo que no tiene por qué ser un inhibidor del comercio, entendiendo el respeto a dicho derecho fundamental como un valor añadido en la gestión empresarial y pública.

Debe tenerse en cuenta, a este respecto, los principios y derechos que conforman la estructura de dichas leyes, procurando encontrar un equilibrio entre la protección individual y el desarrollo económico.

Finalmente, la existencia de un órgano de control deviene imprescindible, quedando su estructura y composición, así como su funcionamiento y facultades, necesitadas de concreción y ajuste al entorno socio cultural en concreto, siempre manteniéndose unos mínimos requisitos.

Las TIC no deben ser sólo una amenaza para esta privacidad, sino que incluso pueden ser utilizadas precisamente para ayudar en su preservación, fomentando la implementación de las tecnologías de protección de la privacidad, como complemento, que no sustituto, de la legislación adecuada.

Tampoco debe invocarse situaciones especiales, de riesgo o miedo ante posibles ataques, sacrificando la privacidad del individuo, sino llegarse al equilibrio entre los intereses en conflicto, sin dejar que pretendidas amenazas aniquilen el derecho fundamental de los seres humanos a controlar su información personal y el tratamiento de la misma.

Nos permitimos así abogar desde estas líneas por la información y la formación del usuario acerca sus derechos y obligaciones en el cuidado de su información personal, huyendo de los extremismos, con objetividad, así como por un asentamiento legal, jurisprudencial, social y cultural del derecho a la protección de datos personales en México.

Referencias normativas

Carta de los derechos fundamentales de la Unión Europea de 7 de diciembre de 2000 (2000/C 364/01).

Constitución europea incorpora el artículo I-51 dedicado al derecho a la protección de datos personales, http://es.constitutio.com/051.php, disponible a 25 de septiembre de 2008.

Convención Americana sobre derechos humanos de 1969, http://www.oas.org/juridico/spanish/Tratados/b-32.html, disponible a fecha de 19 de septiembre de 2008.

Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981.

.Convenio Europeo para la Protección de los Derechos y las Libertades Fundamentales, http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf, a fecha de 19 de septiembre de 2008.

Decisión 2001/497/CE de la Comisión, de 15 de junio, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a un tercer país previstas en la Directiva 95/46/CE (D.O. L 181, de 4 de julio)

Decisión 2002/16/CE de la Comisión, de 27 de diciembre, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a los encargados de tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (D.O. L 6, de 10 de enero de 2002).

Decisión 2000/520/CE de la Comisión, de 26 de julio (Diario Oficial de la Unión Europea serie L, núm. 215, de 25 de agosto).

Decisión 2002/518/CE de la Comisión, de 26 de julio (Diario Oficial de la Unión Europea serie L, núm. 215, de 25 de agosto)

Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001 (Diario Oficial de la Unión Europea serie L, núm. 2, de 4 de enero de 2002)

Decisión 2003/490/CE de la Comisión, de 30 de junio (Diario Oficial de la Unión Europea serie L, núm. 168, de 5 de julio)

Decisión 2003/821/CE de la Comisión, de 21 de noviembre (Diario Oficial de la Unión Europea, serie L, núm. 308, de 25 de noviembre)

Decisión 2004/411/CE de la Comisión, de 28 de abril (Diario Oficial de la Unión Europea serie L, núm. 151, de 30 de abril)

Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008 (Diario Oficial de la Unión Europea serie L, núm. 138, de 28 de mayo).

Declaración Universal de los Derechos Humanos, de 1948, http://www.un.org/spanish/aboutun/hrights.htm a fecha de 19 de septiembre de 2008

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (D.O. L 201, 31/7/2002).

.Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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 (D.O. L 281, 23/11/1995).

Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales (1980), Organización para la Cooperación y el Desarrollo Económicos.

Ley de protección de datos personales del Estado de Colima, aprobada por Decreto número 356 de 14 de junio de 2003.

Ley de protección de datos personales para el Estado y los Municipios de Guanajuato de 19 de mayo de 2006.

Ley federal de transparencia y acceso a la información pública gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002, reformada el 11 de mayo de 2004.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 298, de 14 de diciembre

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 262, de 31 de octubre (derogada por Ley Orgánica 15/1999).

Lineamientos de protección de datos personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares (DOF Martes 6 de abril de 2004)

Marco de Privacidad (1998) de la Asociación para la cooperación económica Asia-Pacífico.

Pacto Internacional de Derechos Civiles y Políticos, http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm, a fecha de 19 de septiembre de 2009.

Plan Nacional de Desarrollo 2007-2012 http://pnd.calderon.presidencia.gob.mx/index.php?page=transparencia-y-rendicion-de-cuentas, disponible a 11 de septiembre de 2009.

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el IFAI disponibles en http://www.ifai.org.mx/datos_personales/seguridad/Recomendaciones_SDP.pdf, a 20 de agosto de 2009.

Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee_on Automated Personal Data System, Julio, 1973. Disponible en http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm, disponible a 22 de septiembre de 2009.

Reforma propuesta al Artículo 16 Constitucional, Gaceta Parlamentaria, Cámara de Diputados, número 2343-II, martes 18 de septiembre de 2007. http://gaceta.diputados.gob.mx/Gaceta/60/2007/sep/20070918-II.html#Dicta20070918Art16Const

Reforma propuesta al Artículo 73 Constitucional, Gaceta Parlamentaria Congreso de Diputados número 2339, miércoles 12 de septiembre de 2007. http://gaceta.diputados.gob.mx/Gaceta/60/2007/sep/20070912-II.html#Dicta20070912Articulo73

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. (Primera Sección) (DOF Miércoles 11 de junio de 2003)

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

Resolución 509 (1968) de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos.

Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

Resolución R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público.

Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, Madrid: Boletín de Jurisprudencia Constitucional, año 1984, páginas 126 y ss.

Bibliografía recomendada

AGRE, PHILIP E. AND MARC ROTENBERG, editores, Technology and Privacy: The New Landscape, Cambridge, 1997, MA: MIT Press, 334 páginas.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Protección de la intimidad en el tráfico de datos en Internet (2001-2002)", Quince años de Encuentros sobre Informática y Derecho, Madrid: Ed. Universidad Pontificia Comillas, 2002, páginas 561-570.

BAYENS, S., The search and seizure of computers: are we sacrificing personal privacy for the advancement of technology?, Drake Law Review, 2000

CARBONELL, M. "La reforma constitucional en materia de acceso a la información: una aproximación general", en Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia, Instituto de Investigaciones Jurídicas, UNAM, Diciembre 2007.

COATS, W. The Practitioner's Guide to Biometrics. Ed. ABA Section of Science& Technology Law. 2007 Chicago, Illinois.

DAVARA FERNÁNDEZ DE MARCOS, I.:

Breve análisis de la reforma al artículo 6º constitucional en lo relativo a protección de datos personales, en Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia, Instituto de Investigaciones Jurídicas, UNAM, Diciembre 2007.

Protección de datos de carácter personal, Revista Abogado Corporativo, Asociación Nacional de Abogados de Empresa, nº 3, Enero - Febrero 2008

La protección de datos en España, en La protección de datos en el mundo, México D.F.: Senado de la República, México D.F., Septiembre 2006.

DAVARA RODRÍGUEZ, M.A.:

Guía Práctica de Protección de Datos para abogados, Madrid: Editorial DaFeMa, 2004.

Manual de Derecho Informático. 6ª edición, Pamplona: Editorial Aranzadi, 2004.

DE ASÍS ROIG, A. E., "Protección de datos y derecho de las telecomunicaciones", Régimen Jurídico de Internet, Madrid: Ed. La Ley , Enero 2002, páginas 201-228.

ESCALANTE GONZALBO, F., El derecho a la Privacidad, Cuadernos de transparencia nº 2, México: IFAI, Agosto 2004.

FERNÁNDEZ LÓPEZ, J. M., "El derecho fundamental a la protección de datos personales", OTROSÍ num. 25, Madrid: Ed. Colegio de Abogados de Madrid, 2001, páginas 56-60.

FROOMKIN, M., The Death of Privacy? Stanfrod Law Review , Vol. 52:1461, 2000.

FREIXES SANJUÁN, T.: Libertades informativas e integración europea, Madrid: Ed. Constitución y Leyes, 1996.

GARCÍA GONZÁLEZ, A., La protección de datos personales: derecho fundamental del Siglo XXI. Un estudio comparado. Boletín Mexicano de Derecho Comparado, Número 120, Septiembre-Diciembre 2007, Instituto de Investigaciones Jurídicas de la UNAM.

GARZÓN VALDÉS, E., Lo íntimo, lo privado y lo público, Cuadernos de transparencia nº 6, México: IFAI, Abril 2005.

GÓMEZ ROBLEDO y ORNELAS NUÑEZ, Protección de datos personales en México: el caso del Poder Ejecutivo Federal, México: UNAM, 2006.

HAGEL, J. y J.F. RAYPORT, The Coming Battle for Customer Information, Harvard Business review, vol 75 n 30, 1997.

HONDIUS, F. W., A decade of international data protection, "Netherlands of International Law Review", vol. 30, n° 2, 1983.

HUTCHINS, J.; U.S. Data Breach Notification Law: State by State. Ed. ABA Section of Science & Technology Law. 2007.

JAMES, MICHAEL, Privacy and human rights: An international and comparative study, with special reference to developments in information technology, Paris : UNESCO, 1994.

KANG, J., Information Privacy In Cyberspace Transactions, 50 Stanford Law Review 1193, Abril 1998.

LÓPEZ AYLLON, Sergio Derecho de la Información, Ed. McGraw-Hill/Interamericana Editores, S.A. de .C.V; 1997 México.

LÓPEZ-IBOR MAYOR, V., "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos", Actualidad Informática Aranzadi núm. 8, Pamplona: Ed. Aranzadi, 1993, páginas 1-3.

LUCAS DURÁN, M., El acceso a los datos en poder de la Administración Tributaria, Pamplona: Ed. Aranzadi, 1997, páginas 265 y ss.

LUCAS MURILLO DE LA CUEVA, P., "Las funciones de la Agencia de Protección de Datos", Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid: Ed. Agencia de Protección de Datos, 28, 29 y 30 de Octubre de 1996, páginas 276 y ss.

OLIVER LALANA, A. D., "Autorregulación, normas jurídicas y tecnológicas de privacidad. El lado virtual del derecho protección de datos", XVII Encuentros sobre Informática y Derecho, Madrid: Ed. Universidad Pontificia Comillas, 2002-2003, páginas 85-102.

PECES-BARBA, G., "Derechos Fundamentales", Madrid: Ed. Guadiana de Publicaciones, 1976, 318 páginas.

PÉREZ LUÑO, A. E., Cibernética, Informática y Derecho. (Un análisis metodológico), Bolonia: Ed. Real Colegio de España, 1976. 166 Páginas.

POSNER, RICHARD, The Economics of Privacy, The American Economic Review, Vol. 71, No. 2, Mayo 1981.

RODOTÀ, S.:

- "Democracia y protección de datos", Cuadernos de Derecho Público, Madrid: INAP, núms. 19-20, mayo-

diciembre de 2003.

- Tecnología y derechos fundamentales, Agència Catalana de Protecció de Dades, 2004, disponible en www.apd.cat a 25 de agosto de 2008.

RUBÍ NAVARRETE, J., "Los códigos tipo: la alternativa de la autorregulación", Actualidad Informática Aranzadi núm. 35, Pamplona: Ed. Aranzadi, 2000, páginas 1-5.

Rule, J, Privacy in Peril. Ed. Oxford University Press, 2007.

SANCHO VILLA, D., Transferencia Internacional de Datos Personales, Madrid: Ed. Agencia de Protección de Datos, 2003.

SOOKMAN, B., Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions. Ed. Thomson Carswell. 2002 Canadá.

SULLIVAN, J; HIPPA A Practical Guide to the Privacy and Security of Health Data. Ed. American Bar Association. Chicago, Illinois.

VV.AA., Privacy & Human Rights. Ed. Electronic Privacy Information Center and Privacy International. First edition 2007.

WESTBY, J. et al., International Guide to Privacy. Ed. Section of Sience &Technology Law, American Bar Association. 2004 Chicago, Illinois.

WESTIN, A., Privacy and Freedom, Nueva York: Ed. Atheneum, 1967.

WU, S., et al: A Guide to Hipaa Security and the Law. Ed: ABA Section of Science & Technology Law.2007 Chicago, Illinois.

ZÚÑIGA URBINA, F., El derecho a la intimidad y sus paradigmas, "Ius et praxis", Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, año 3, n° 1, 1997.

El Instituto Federal de Acceso a la Información Pública como órgano garante en materia de protección de los datos personales1

*Jacqueline Peschard Mariscal**

Introducción

En México, el Instituto Federal de Acceso a la Información Pública (en adelante IFAI)2, es la autoridad especializada en materia de acceso a la información pública gubernamental y garante de la protección de los datos personales en posesión de las dependencias y entidades de la Administración Pública Federal, en lo sucesivo, Poder Ejecutivo Federal.

La prioridad para los Comisionados del IFAI en el arranque de la Ley Federal de Trasparencia y Acceso a la Información Pública Gubernamental3 (la Ley) fue privilegiar la difusión del derecho a saber de todas las personas acerca de cómo hacen las cosas los órganos gubernamentales, cómo ejercen el gasto público, y cómo cumplen sus metas y los objetivos, entre otros muchos aspectos.4

Sin embargo, con el paso del tiempo y la especialización que fue dándose al interior de la Institución, la faceta de autoridad garante de la protección de los datos personales contenidos en los ficheros públicos (denominados por nuestra normativa como sistemas de datos personales) comenzó a desarrollarse, si bien, el ejercicio de los derechos de acceso y rectificación de datos fue plenamente observado desde el inicio por los entes gubernativos.

El presente artículo tiene como objetivo compartir las experiencias surgidas de las primeras verificaciones que se han efectuado a los sistemas de datos personales en posesión de la Administración Pública Federal, para conocer el grado de observancia del Capítulo IV, del Título Primero de la Ley de Transparencia, así como de los Lineamientos de protección de datos personales.5

---

*Doctora en Ciencias Sociales, por el Colegio de Michoacán. Miembro del Sistema Nacional de Investigadores y de la Academia Mexicana de Ciencias. Actualmente es Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública (IFAI).

Verificaciones a sistemas de datos personales.

El objetivo de las verificaciones es conocer el cumplimiento que el Ejecutivo Federal da a los principios de protección de datos personales y evaluar las acciones implementadas, así como el nivel de observancia de la normatividad aplicable en esta materia, para la posterior emisión de recomendaciones.

En este sentido, a partir de 2007 se dio inicio a los procedimientos de verificación de sistemas de datos personales, a través de la notificación de requerimientos de información a distintas dependencias y entidades (seleccionadas previamente en razón de la importancia de los sistemas o la sensibilidad de los datos, entre otros criterios).

Los cuestionamientos específicos a las distintas instituciones abarcan los siguientes aspectos:

Cumplimiento de los principios de protección relativos a licitud, calidad, información, custodia y cuidado y seguridad;

Los procedimientos implementados por parte de las dependencias y entidades de la Administración Pública Federal para garantizar el ejercicio de los derechos de acceso y corrección (rectificación);6

El tratamiento y acciones realizadas al efectuar transmisiones de datos personales con dependencias, entidades o entes públicos federales, ya sea estatales o municipales; o bien con gobiernos u organismos internacionales;

Las medidas de seguridad administrativa, física y técnica, implementadas por el Ejecutivo Federal para asegurar la integridad, disponibilidad y confidencialidad de los datos personales en su posesión;

El registro de los sistemas de datos (registro de ficheros) en la herramienta generada para tal efecto, y

Los mecanismos para la contratación de los servicios de un tercero para el tratamiento de los sistemas de datos personales.

Durante el proceso de respuesta y envío de información al IFAI, se sostienen reuniones de trabajo con las distintas dependencias y entidades verificadas, lo cual permite, por una parte, sensibilizar a los responsables de los sistemas en cuanto al tratamiento de los datos y, por otra, contar con mayores elementos para emitir recomendaciones específicas, en razón de las respuestas proporcionadas por las unidades administrativas responsables del sistema objeto de verificación.

Emisión de Recomendaciones a sistemas de datos personales.

La recomendaciones se emiten mediante acuerdos tomados por mayoría de votos de los 5 comisionados que integran el Pleno del IFAI, las cuales tienen por objeto indicar ac-

ciones concretas para la debida observancia de los principios y derechos en materia de protección de datos personales, a partir de la identificación de las condiciones o puntos críticos detectados en las verificaciones realizadas, tales como riesgos existentes o potenciales, a efecto de minimizarlos. También el Instituto reconoce los avances registrados en el cumplimiento de la legislación y regulación secundaria por parte del Ejecutivo Federal.

A la fecha, el IFAI han emitido 62 recomendaciones en materia de protección de datos personales. Así, la tarea del IFAI en materia de protección de datos personales se ha centrado en construir una política pública de respeto y adecuado tratamiento a la información de las personas, a partir de dar a conocer los criterios del Instituto en cada caso concreto.

Los sistemas de datos personales verificados refieren a diversas finalidades, las cuales se encuentran vinculadas con las facultades y atribuciones lícitas y legales que cada órgano gubernamental tiene conferidas; finalidades que pueden comprender, solo por mencionar algunas, el control de programas sociales; registros de población; actividades de control migratorio; atención médica (expedientes clínicos); líneas de atención telefónica a víctimas de violencia; sistemas o ficheros de datos de control de personal con fines puramente administrativos, tales como los expedientes de personal, entre otros.

De esta suerte, los aspectos de interés que destacaron en el desarrollo de las verificaciones, fueron tan bastos como los ficheros en sí. En este sentido, por obvio de espacio, nos centraremos en algunos aspectos relevantes de las recomendaciones emitidas, tomando en cuenta la finalidad del sistema y la dependencia o entidad que los posee.

En principio, vale la pena referirnos a los sistemas de datos en posesión del Instituto Nacional de Migración,7 órgano técnico desconcentrado de la Secretaría de Gobernación, el cual tiene por objeto la planeación, ejecución, control, supervisión y evaluación de los servicios migratorios en el país, así como el ejercicio de la coordinación con las diversas dependencias y entidades de la Administración Pública Federal que concurren en la atención y solución de los asuntos relacionados con la materia migratoria.

Del análisis realizado a los sistemas de datos, FM1 Delegaciones, FM1 Electrónica, Sistema Integral de Operación Migratoria SIOM y LASERFICHE (Digitalización del Archivo Migratorio Central), entre otros, respecto al tratamiento de los datos de carácter personal por parte de las unidades administrativas responsables, arrojó en su generalidad resultados favorables. Por lo anterior, el IFAI realizó una serie de recomendaciones tendientes a mejorar, y en su caso, reforzar las medidas implementadas por el Instituto Nacional de Migración, tales como:

Incorporar en sus mecanismos escritos de recolección de datos la leyenda de información -aviso de privacidad- a que hace alusión el Decimoctavo de los Lineamientos de Protección de Datos Personales;

Definir y delimitar las atribuciones, funciones y obligaciones de los servidores públicos que interactúan con los datos personales, en el ejercicio de sus funciones, con el carácter de encargados y usuarios, y

Diseñar e instrumentar planes de capacitación que estén enfocados a difundir la normatividad aplicable en materia de protección de datos personales y las medidas de seguridad de índole administrativa, física y técnica implementadas para la adecuada protección de los datos personales contenidos en los sistemas, entre otras.

Cabe señalar, que el estudio realizado fue respecto de los datos personales que recaba el órgano desconcentrado en ejercicio de sus facultades de carácter administrativo, y no así para aquella información que le es proporcionada por los órganos de inteligencia y procuración de justicia del país en términos de lo señalado en los artículos 72 y 73 de la Ley General de Población,8 y 202 de su Reglamento.9

Ahora bien, por lo que hace a los ficheros relacionados con asistencia social, el sistema de datos personales denominado "Sistema de Acreditación de Derechohabiente" en posesión del Instituto Mexicano del Seguro Social10, se considera de gran relevancia, al tener como finalidad el registrar los datos de identificación de los derechohabientes del Instituto Mexicano del Seguro Social, para la expedición de un medio de identificación que simplifique la entrega de las prestaciones en especie y en dinero, a través de medios electrónicos modernos, eficaces y seguros que vincule al derechohabiente de forma única, confiable e inequívoca a las prestaciones a que tiene derecho.

Uno de los aspectos que merece mención de la verificación a dicho sistema, refiere a la contratación de los servicios de un tercero para el tratamiento de datos personales. El IFAI, pudo constatar que el Instituto Mexicano del Seguro Social cumple adecuadamente respecto a este rubro, al establece mediante un instrumento jurídico adecuado -un contrato- las acciones sobre tratamiento y seguridad que debe adoptar el prestador del servicio, a través de un clausulado específico, en el cual se exigen los siguientes puntos:

Los criterios de seguridad de la información que debe cumplir el proveedor en los que se incluyen integridad, confidencialidad, autenticación, control de accesos, no repudio, disponibilidad, auditoría y monitoreo, y

El destino final de los datos obtenidos como parte del proceso de enrolamiento, en el cual se establece que son propiedad de Instituto, y el proveedor es responsable de brindar el servicio de generación y entrega del documento de acreditación, así como la inserción del registro a la base de datos.

Como se desprende, numerosos son los aspectos positivos resultado de las recomendaciones emitidas por el Pleno del IFAI en materia de protección de datos personales; en particular, el IFAI ha sido contundente al indicar el tipo de medidas de seguridad que

impidan que los datos recabados sean sustraídos y utilizados para otros fines.

En ese sentido, se han realizado sesiones informativas para que las dependencias y entidades conozcan el contenido y alcances de un documento de seguridad de sistemas de datos personales (el cual es obligatorio), a efecto de aclarar dudas concretas y acompañar a los servidores públicos responsables del tratamiento de datos y de áreas de tecnologías de la información, en la tarea de identificar sus riesgos para que, a partir de ellos, cada uno elaborare una política de gestión de la seguridad ad-hoc. El énfasis se ha puesto por tanto, en garantizar la integridad, confidencialidad y disponibilidad de la información personal, así como contar con planes para enfrentar contingencias concretas.

Finalmente, cuando los sistemas involucran el tratamiento de datos biométricos, cabe hacer mención, que el Instituto considera y ha citado, a manera de referencia, el documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003, por el Grupo del artículo 29,11 con relación al uso de huellas dactilares. Del mismo modo, se ha hecho mención al estudio Fingerprint Vendor Technology Evaluation, publicado por el National Institute of Standards and Technology.12

Nuevos retos a enfrentar

La actuación del IFAI como órgano garante en materia de protección de datos personales, comienza a implantarse cotidianamente en el quehacer de las oficinas gubernamentales.

Otra de las prioridades del IFAI en el mediano plazo, es efectuar evaluaciones del impacto a la privacidad (PIA) ex ante el lanzamiento de grandes proyectos que involucran la utilización de nuevas tecnologías e información de las personas.

En ese rubro, se contrató a través de una licitación pública internacional los servicios de un consultor especializado para llevar a cabo una PIA para un Anteproyecto de Norma Oficial Mexicana, que implementará un expediente clínico electrónico bajo un formato estándar para todos los mexicanos. A p

artir de los hallazgos del consultor, el IFAI emitió recomendaciones específicas a la Secretaría de Salud para su observancia, de modo que la información personal contenida en historias clínicas electrónicas, esté debidamente protegida.

Otra asignatura pendiente es efectuar, a su vez, un análisis de mitigación de los impactos a la privacidad del proyecto para la emisión de una cédula de identidad ciudadana. Sobre este proyecto me complacerá compartir nuestra experiencia en futuras publicaciones.

Notas

1 Peschard Mariscal, Jacqueline, "The Federal Institute of Access to Public Information as the Guarantor Entity for the Protection of Personal Data", dataprotectionreview.eu, número 10, Madrid, España, octubre, 2009. Versión en español.

2 El Instituto Federal de Acceso a la Información Pública es un organismo descentralizado, no sectorizado, con autonomía operativa, presupuestaria y de decisión, en términos de lo establecido en el su Decreto de Creación , publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002.

3 Ley Federal de Transparencia y Acceso a la Información Pública , publicada en el Diario Oficial de la Federación, el 11 de junio de 2002 y reformada mediante Decreto publicado en el citado órgano informativo el 6 de junio de 2006.

4 De junio de 2003 a septiembre de 2009, se cuenta con los siguientes datos:

- Total de solicitudes de acceso a la información presentadas: 456,335
- Total de recursos (quejas) ante el IFAI: 23,531

Para consultar mayores detalles ver:http://www.ifai.org.mx/descargar.php?r=/pdf/gobierno/&a=stats.pdf.

5 Lineamientos de protección de datos personales , publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

6 Con la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 1 de junio de 2009, se reconoce el derecho de toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición; no obstante, no se cuenta todavía con una ley reglamentaria que permita el ejercicio de los derechos de cancelación y oposición a nivel Federal, por lo que hasta en tanto no se legisle en consecuencia, el ejercicio de los derechos de protección de datos personales se encuentra limitando al de acceso y corrección (rectificación), en los términos que establece la Ley de Trasparencia. Respecto a las leyes reglamentarias, no se omite señalar que algunos estados de la República Mexicana, como Colima y el propio Distrito Federal ya cuentan con leyes específicas en materia de protección de datos personales.

7 Artículos 55 y 56 del Reglamento Interior de la Secretaría de Gobernación. Disponible en http://www.ordenjuridico.gob.mx/Federal/Combo/R-273.pdf.

8 Disponible para consulta en http://www.diputados.gob.mx/LeyesBiblio/doc/140.doc.

9 Disponible para consulta en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.doc.

10 En términos del artículo 251 de la Ley del Seguro Social, el Instituto Mexicano del Seguro Social, tiene dentro de sus atribuciones y facultades, administrar los seguros de riesgos de trabajo, enfermedades y maternidad, invalidez y vida, guarderías y prestaciones sociales, salud para la familia, adicionales y otros, así como prestar los servicios de beneficio colectivo que señala su propia ley, y en general los asuntos relacionados con la asistencia social de sus derechohabientes, entre otros. Ley del Seguro Social, disponible en: http://www.diputados.gob.mx/LeyesBiblio/doc/92.doc.

11Para consulta en: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/rules-art-29_en.pdf.

12 Es un organismo federal, dentro del Departamento de Comercio de los Estados Unidos de América, cuya misión es promover la innovación y la competitividad industrial mediante la promoción de la ciencia y la tecnología en formas que mejoren la seguridad económica, entre otras funciones. Fingerprint Vendor Technology Evaluation 2003. National Institute of Standards and Technology (NIST), pp. 14 y 15.

La protección de datos personales por el gobierno la actuación del Instituto Federal de Acceso a la Información Pública[1]

Alonso Lujambio Irazábal y*
Lina Ornelas Núñez

1. Introducción

Es un principio tan viejo como el common law que el individuo debe gozar de total protección en su persona y en sus bienes; 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. El derecho a la vida servía para proteger a los súbditos frente a las variadas formas de agresión violenta; libertad quería decir que se era libre, que no se estaba sometido; y el derecho a la propiedad garantizaba al hombre sus tierras y su ganado. Más tarde, vino el reconocimiento de otras posesiones del ser humano, más allá de las puramente materiales. 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.2

Según señala Luciano Vandelli, si se mira bien lo sucedido en las últimas décadas, se pondría de manifiesto cómo los nuevos valores -desde la tutela medioambiental hasta

---

*Alonso Lujambio Irazábal es licenciado en Ciencias Sociales por el Instituto Tecnológico Autónomo de México (ITAM), Maestro y Doctor por la Universidad de Yale, Consejero Electoral del Instituto Federal Electoral (1996-2003) y fungió como Comisionado Presidente del Instituto Federal de Acceso a la Información Pública. Lina Ornelas es abogada egresada de la Facultad de Derecho de la Universidad de Guadalajara. Maestra en Cooperación Legal Internacional por la Universidad Libre de Bruselas *(Vrije Universiteit Brussel).* Coordinadora de subgrupos de trabajo de la Red Iberoamericana de Protección de Datos. Actualmente es Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública (IFAI).

la protección de la vida privada y de la intimidad- han conducido a la expansión del derecho administrativo hacia campos inéditos. En concreto, la libertad informática constituye uno de los más claros exponentes de los llamados derechos fundamentales de tercera generación, muy alejados de los primeros derechos reconocidos en el ámbito de las revoluciones burguesas en el siglo XVIII, caracterizados por la defensa de la esfera privada ante la intromisión de los poderes públicos, o de los decimonónicos de segunda generación para la salvaguarda de los aspectos económicos, sociales y culturales. Estamos ante derechos humanos de tercera generación surgidos en respuesta a las amenazas de la modernidad.3

Es así que, resulta imprescindible poner de relieve el creciente protagonismo que durante las últimas décadas ha ido adquiriendo la protección de la información de carácter personal.

En el caso mexicano, a partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se ha dado inicio a un nutrido debate por la creciente demanda de información desde las más diversas ópticas.

Tal diversidad ha llevado al Instituto Federal de Acceso a la Información Pública (el IFAI), a trazar los límites del acceso a la información frente a otros derechos reconocidos en el orden jurídico nacional e internacional. Dicha labor ha sido desarrollada fundamentalmente desde dos frentes: el normativo y el resolutivo.

En el ámbito normativo se han expedido disposiciones de carácter administrativo como los Lineamientos en materia de clasificación, secretos y protección de datos personales, mientras que en ejercicio de las facultades cuasi-jurisdiccionales, concedidas al IFAI, se han venido delineando los criterios aplicables para aquellos casos que se encuentran en las zonas de penumbra, zonas grises de aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En el terreno de las resoluciones emitidas por el IFAI, la tarea ha sido particularmente compleja, dada la diversidad de situaciones a las que se enfrenta el Pleno del Instituto al momento de deliberar y resolver en torno a una controversia. Entre los asuntos relevantes y especialmente complejos que ha conocido el IFAI, se encuentran aquellos en los que se puede llegar a producir una colisión de derechos, en particular entre el derecho a la protección de datos personales y la transparencia gubernamental.

Es por ello que, a lo largo del presente estudio, nos enfocaremos a analizar la problemática descrita desde un nivel argumentativo distinto al hasta hoy planteado en esta materia, aportando una propuesta acorde con el diseño de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y armónica con los alcances del derecho a la protección de datos personales en el derecho comparado.

Como corolario de lo anterior, me permitiré explicar cómo el IFAI ha procurado la necesaria transparencia que ha de presidir la actuación pública, a través de la conciliación

en muchos casos del derecho a saber, con otros derechos fundamentales de las personas, como es el caso del derecho a protección de los datos personales y de la privacidad. Esta necesidad de conciliación, no siempre fácil de lograr, se hace aún más evidente si tenemos en cuenta la incidencia que, en la privacidad, pueden tener los vertiginosos avances de la tecnología.

Para lo anterior, nos serviremos de algunas resoluciones del IFAI, así como de votos particulares elaborados en procedimientos que han implicado una ponderación de valores en tensión.

2. El derecho a la protección de datos como instrumento para asegurar la información de las personas en posesión del gobierno.

En México, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental reconoce el derecho a la protección de datos personales y establece los derechos y principios de protección que deberán ser observados por todas las entes gubernamentales.

Derivado de las atribuciones del IFAI, se ha expedido regulación secundaria en la materia como lo son los Lineamientos de Protección de Datos Personales que tienen por objeto establecer las políticas generales y los procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para asegurar el adecuado tratamiento de los datos personales e impedir su transmisión ilícita y lesiva para la dignidad de las personas.

El Poder Ejecutivo Federal administra grandes bases de datos con información muy variada de las personas, ya que para el ejercicio de sus atribuciones y la correcta aplicación de las leyes, recaba cientos de datos personales. Es el caso por ejemplo de la Base Nacional de Datos de la Clave Única de Registro de Población del Registro Nacional de Población, la base de datos del Servicio de Administración Tributaria sobre contribuyentes, los sistemas de expedientes clínicos del sector salud como el Instituto Mexicano del Seguro Social o el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado en el que se alojan millones de expedientes de derechohabientes, o el padrón electoral del Instituto Federal Electoral. A julio de 2007 se habían registrado en el Sistema Persona, que es la herramienta informática para notificar al IFAI de la existencia de sistemas de datos personales, 2,200 sistemas de datos personales.

A efecto de lograr un adecuado tratamiento de datos personales, es un requisito sine qua non, la adopción de medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, con base en estándares de seguridad internacionales,

por lo que el IFAI en ejercicio de sus facultades, ha emitido las "Recomendaciones sobre las políticas generales para el manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las dependencias y entidades de la Administración Pública Federal".

Para lograr un efectivo entorno de seguridad, es necesario tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya sea que provengan de la acción humana o de las condiciones físicas y ambientales, por lo que las recomendaciones aludidas establecen distintos niveles de seguridad aplicables a cada categoría o tipo de datos alojados en los sistemas de datos personales.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales en razón de la criticidad de la información o la sensibilidad de los mismos. Así, las dependencias y entidades aplicarán el nivel básico a datos de identificación como nombre y domicilio por ejemplo, el nivel medio, a datos patrimoniales o migratorios, y nivel alto a datos ideológicos, de preferencia sexual o de salud.

Ahora bien, qué ha sucedido en México a partir de la entrada en vigor de la Ley en esta materia. Para responder esta pregunta vamos a relatarles algunos casos relevantes de colisión de derechos.

3. Transparencia gubernamental y Protección de datos personales

3.1 Actas de nacimiento y fuentes de acceso público

Con fecha 30 de noviembre de 2005, el Pleno del IFAI, a través de la resolución 1189/05, se determinó que si bien las actas de nacimiento, de matrimonio y de defunción, en su conjunto, que obran en los archivos de la Secretaría de Gobernación concretamente en el Registro Nacional de Población, no se consideran información confidencial por hallarse en registros públicos -en los registros civiles-, no por ello procede otorgar acceso, a cualquier persona que así lo requiera, al sistema de dichos datos personales, sino que se debe orientar al mismo para que acuda a los registros públicos, pues la finalidad para la cual se recabaron dichos datos en el Registro Nacional de Población, no fue la comunicación o cesión a terceros.

En ese orden de ideas, se consideró que el hecho de que un dato personal obre en una fuente de acceso público, no implica que las agencias gubernamentales puedan otorgar acceso al mismo, pues ésta no es la finalidad para la cual se obtuvo dicho dato; más aún, por mandato de Ley, dichas agencias se encuentran obligadas a proteger los datos personales que obren en sus archivos y en consecuencia a observar las distintas disposiciones

contenidas en la Ley y en los Lineamientos de Protección de Datos Personales que restringen el manejo de dichos datos, por lo que en casos como el que nos ocupa, bastaría con que se indique al solicitante por escrito, la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información en los archivos públicos existentes.

De esta suerte, fue necesario considerar que la solicitud que originó el recurso de revisión de referencia era una solicitud de acceso a una base de datos personales y no estaba referida a información gubernamental, situación que implicó analizar las disposiciones contenidas en la Ley y en los Lineamientos de Protección de Datos Personales, aplicables a las bases de datos personales que poseen las dependencias y entidades, en virtud de las atribuciones que tienen conferidas.

Aunado a lo ya expresado se argumentó conforme a lo establecido en el artículo 22 de la Ley de Transparencia, que aun cuando los datos personales en poder de los sujetos obligados también se encuentren en una fuente o registro público, será necesario requerir el consentimiento de los individuos para que éstos puedan ser proporcionados a terceros, al no encontrarse entre los supuestos legales en virtud de los cuales es posible transmitir datos personales sin el consentimiento de su titular.

3.2 Cartas en las que se otorga el consentimiento para participar en experimentos científicos.

Un caso particularmente interesante fue el recurso de revisión 1659/05 contra el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, en el que el Pleno del IFAI determinó procedente otorgar acceso a una versión pública de las cartas a través de las cuales cuarenta y cinco personas otorgaron su consentimiento para ser objeto de una investigación médica. Se trató de probar el efecto de un medicamento para evitar el embarazo entre mujeres que ya no podían, por diversas razones, quedar embarazadas.

Partiendo de la premisa de que se trataba de una solicitud de acceso a datos personales, toda vez que dar a conocer la decisión de participar en un proyecto de investigación científica de este tipo constituía información que afectaba la intimidad de las personas, se arribó a la conclusión de que la documentación solicitada también contenía información que permitía la rendición de cuentas a los ciudadanos por parte de funcionarios públicos puesto que, para participar en proyectos de investigación científica, es obligación legal contar con el consentimiento previo, voluntario e informado de las personas, en términos del artículo 100, fracción IV de la Ley General de Salud.

Es en este contexto que el IFAI consideró una versión pública de la documentación solicitada, en la que se omitieran todos aquellos datos que permitieran identificar bajo cualquier circunstancia a las participantes en el proyecto de investigación científica, en términos de lo dispuesto en el segundo párrafo del artículo 43 de la Ley Federal de

Transparencia y Acceso a la Información Pública Gubernamental, cumplía con la armonización de los dos objetivos: la rendición de cuentas y la protección de datos en posesión de los sujetos obligados. En términos de los razonamientos planteados se instruyó a la elaboración de una versión pública de cada una de las 45 cartas de consentimiento.

3.3 La localidad en la que reside una persona como un elemento que transparenta la debida gestión tratándose de programas sociales.

Otro de los casos a los que nos hemos tenido que se ha presentado es respecto de la localidad en la que residen algunos beneficiarios de programas de subsidios económicos por parte del Estado.

Ante estos supuestos, debemos pronunciarnos sobre qué derecho prevalece en el caso concreto, por un lado, la protección de ciertos datos personales, como lo es la localidad donde reside un individuo beneficiario de determinado programa –cuando dicha localidad permite conocer de manera casi exacta su domicilio conocido- y, por el otro, la publicidad de dicha información como instrumento de rendición de cuentas en la prestación de un beneficio económico a cuenta del erario público, puesto que en la mayoría de las ocasiones, el habitar en determinada localidad constituye uno de los requisitos para ser favorecido por el programa de que se trate.

Al respecto, cabe destacar que en diversas ocasiones –por ejemplo, a través de la resolución de los recursos de revisión con números de expediente 1401/06 y 2300/06, en las cuales el sujeto obligado era la Coordinación Nacional del Programa de Desarrollo Humano Oportunidades o la resolución al recurso de revisión 887/07 en la que la autoridad recurrida fue Caminos y Puentes Federales de Ingresos y Servicios Conexos- el IFAI se ha pronunciado a favor de la prevalencia de la publicidad de la localidad donde habitan los beneficiarios de algún programa de estímulos económicos, sobre la confidencialidad de revelar la localidad en la que residen dichos individuos. Este discernimiento ha sido sustentado en razón de que la publicidad de esta información permite que los ciudadanos puedan valorar el desempeño de los sujetos obligados en el ejercicio de los recursos públicos. Permite someter a escrutinio a programas sociales.

Lo anterior ciertamente no ha sido tarea fácil, sin embargo, hemos encontrado caminos que nos han permitido ser congruentes con el principio de máxima publicidad al que nos obliga el artículo 6 de la Ley y no violentar el derecho de los particulares a la protección de sus datos personales.

3.4 La fotografía de funcionarios públicos

Otro interesante debate en el IFAI fue el resuelto en los recursos de revisión 930/05, 931/05, 932/05, entre otros, motivados por diversas solicitudes de acceso en las que se

requirió obtener acceso a las fotografías de los servidores públicos adscritos a distintos entes públicos.

En respuesta a la solicitud los entes públicos a los que se requirió las fotos negaron el acceso a las mismas alegando que se trataba de información de carácter personal.

En aquella ocasión, la discusión se enfocaba en determinar si la fotografía de los funcionarios públicos debiera hacerse del conocimiento público como elemento que favorecedor de la transparencia gubernamental y rendición de cuentas ante los gobernados

Entre los argumentos vertidos se señaló que la fotografía de los servidores públicos no se encuentra dentro de la información que debe ser publicada por los entes públicos en cumplimiento de la Ley en cita. Asimismo se indicó que la fotografía de un servidor público no reflejaba su desempeño ni acreditaba su idoneidad en el cargo, por lo que no puede decirse que exista un interés público mayor, al derecho a la protección de datos, en conocer dicha información. Lo anterior con independencia de que para salvaguardar las garantías de legalidad y seguridad jurídica previstas en el artículo 16 de las Constitución Política de los Estados Unidos Mexicanos, los servidores públicos tengan que identificarse frente a los gobernados para efectuar cualquier acto de molestia. Al respecto, se citaron a manera de ejemplo diversos casos de procedimientos de los que derivan actos de molestia en los que el legislador expresamente previó los requisitos que deberá cumplir la autoridad competente para llevar a cabo el acto respectivo, entre los cuales se encuentra la identificación de los servidores públicos frente al gobernado.

En todos los casos señalados, se mostró que el legislador dispuso que los servidores públicos deben identificarse frente a los gobernados para no dejar duda alguna acerca de que quienes las practican son funcionarios que pertenecen a la entidad pública de que se ostentan, y que se encuentran facultados para ello precisamente para evitar abusos de autoridad. Lo anterior, según se expresó en la resolución respectiva, no implica que la fotografía del servidor público que efectúa un acto de molestia sea pública, puesto que su identificación frente a los gobernados se realiza con propósitos determinados inherentes a sus atribuciones.

En esa línea de argumentación también se señaló que pensar que mediante la difusión de la fotografía de los servidores públicos se fortalece la responsabilidad y la rendición de cuentas es un error, ya que las deficiencias en ciertos marcos institucionales no se subsanan con la publicidad de imágenes, por lo que dar la cara en términos "democrático-institucionales" no es dar la foto. Dado que el caso fue muy controvertido, se pidió adicionalmente la opinión de distintas autoridades en el ámbito internacional, tanto de acceso a la información, como de protección de datos personales, consulta de la que se obtuvo respuestas contundentes respecto de la confidencialidad de la fotografía de servidores públicos.4

3.5 Teléfonos de contacto

Se solicitó a la Secretaría de Medio Ambiente y Recursos Naturales conocer las unidades de manejo para la conservación de la vida silvestre (UMA) que fueran criaderos de aves de clima cálido (psitácidos), en específico se requirió: las especies que criaban, la ubicación de dichas unidades, responsable técnico y número telefónico para realizar el contacto.

La Secretaría de Medio Ambiente y Recursos Naturales, señaló que la información solicitada contenía información confidencial por tratarse de datos personales, en particular fueron omitidos los "números telefónicos de personas físicas".

A efecto de un mejor entendimiento del contexto en el que se desenvuelve la información requerida se hará una descripción normativa breve en torno a las UMA.

El artículo 3 fracción XLIV de la Ley General de Vida Silvestre establece que se entenderá por unidades de manejo para la conservación de vida silvestre (UMA): "los predios e instalaciones registrados que operan de conformidad con un plan de manejo aprobado y dentro de los cuales se da seguimiento permanente al estado del hábitat y de poblaciones o ejemplares que ahí se distribuyen".

Las UMA forman parte del Sistema de Unidades de Manejo para la Conservación de la Vida Silvestre al ser registradas ante la Secretaría de Medio Ambiente y Recursos Naturales de acuerdo con lo establecido en los artículos 39 y 40 de la Ley General de Vida Silvestre.

Por lo tanto, del análisis de la litis del presente recurso de revisión, se advirtió un enfrentamiento entre dos valores tutelados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por un lado, la confidencialidad de los datos personales de los titulares de las UMA y por el otro, el objetivo principal de dichas Unidades, que es la elaboración de los planes de manejo para la conservación de hábitat natural, poblaciones y ejemplares de especies silvestres, así como la difusión de dicha información ambiental.

En esa tesitura, se señaló si se optara por proteger el dato personal –número telefónico del titular de la UMA- se impediría identificar un medio de contacto con dicha Unidad. De esta manera, se puso de manifiesto que el número de teléfono resulta un elemento socialmente útil para identificar y contactar a una UMA, situación que resulta superior a la posible afectación –en algunos casos- a la confidencialidad del dato personal de ciertos titulares de las UMA.

En virtud de lo anterior, dado que los teléfonos requeridos se refieren a los que se encuentran registrados a nombre de la UMA correspondiente y que la finalidad última de las UMA es integrar el Sistema Nacional de Unidades de Manejo para la Conservación de la Vida Silvestre, cuyo objetivo principal es difundir la información ambiental nacio-

nal y el registro de dichas UMA es público –y está disponible para consulta- de conformidad con la Ley General de Vida Silvestre, se revocó la clasificación como confidencial de los números telefónicos de las UMA, aun cuando estos pudieran corresponder a particulares, puesto que dicho dato constituye información de utilidad social.

4. La Suprema Corte de Justicia de la Nación y el concepto de vida privada5.

La Primera Sala del Máximo Tribunal señaló lo que para efectos de la resolución al amparo directo en revisión número 402/2007 supone el derecho a la privacidad, argumentos que en su parte medular nos permitiremos citar a la letra:

> Por vida privada se entiende aquella parte de la vida humana que se desarrolla a la vista de pocos o que constituye la vida personal y particular....6
>
> El derecho a la vida privada es un derecho fundamental consistente en la facultad que tienen los individuos para no ser interferidos o molestados por persona o entidad alguna, en todo aquello que desean compartir únicamente con quienes ellos eligen; tal derecho, deriva de la dignidad de la persona e implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás.
>
> El derecho a la vida privada es muy amplio y se constituye con diversos derechos que tienen relación directa con la dignidad de la persona. En efecto, existe una serie de derechos destinados a la protección de la vida privada, los cuales están vinculados a la propia personalidad, derivados por ello, de la dignidad de la persona. Entre esos derechos se encuentran, entre otros, el del honor y el de la intimidad.
>
> El honor es el aprecio y estima que una persona recibe en la sociedad en que vive, el cual se vincula directamente con la dignidad de la persona y por tanto, con su vida privada, pues de llegarse a afectar ese aprecio o estima, tal afectación no sólo tendrá un impacto estrictamente social, pues también lo tendrá en la vida privada, en la parte de la vida que la persona desarrolla a la vista de pocos...
>
> El concepto de vida privada engloba todo aquello que no se quiere que sea de general conocimiento, dentro de ello, existe un núcleo que se protege con más celo, con mayor fuerza porque se entiende como esencial en la configuración de la persona y es a lo que se le denomina intimidad.
>
> Dentro de la vida privada se encuentra inserta la intimidad; la vida privada es lo genéricamente reservado y la intimidad lo radicalmente vedado, lo más personal.
>
> Así se tiene, que vida privada e intimidad son derechos distintos; la vida privada engloba a la intimidad y también al honor, por lo que la afectación ya sea de la intimidad o del honor, agravia a la vida privada...

5. Conclusiones

Se advierte que el IFAI ha tenido que actuar en una doble vertiente para asegurar la transparencia y rendición de cuentas, así como la protección de los datos personales en posesión de la Administración Pública Federal. Por un lado, se ha emitido la regulación necesaria para apuntalar el esquema normativo establecido en la Ley de Transparencia.

En ese orden de ideas, el IFAI en su carácter de autoridad protectora de datos, pondera la protección a la vida privada o intimidad de las personas frente a situaciones que involucren un interés público preponderante por dar a conocer cierta información personal, en ese sentido se llevan a cabo pruebas de equilibrio para que de manera excepcional y luego de un cuidadoso análisis, la sociedad pueda acceder a la misma.

Derivado de lo anterior podemos concluir que el derecho a la protección de datos está siendo sometido a diversos retos o tensiones que conviene tener muy en cuenta: protección de datos versus a) libertad de expresión; b) transparencia y acceso a la información; c) intereses y evolución del mercado; d) lucha contra el terrorismo y garantía de la seguridad pública.

En ese sentido, se estima que el IFAI debe mantener el delicado equilibrio entre transparentar la gestión pública y proteger a las personas en relación con la divulgación de la información de que son titulares y que el gobierno recabó y posee de manera originaria para otras finalidades.

La apuesta es por una política respetuosa de los derechos del gobernado en esta materia, apuntalando la estructura prevista en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por medio de lo que podría denominarse "jurisprudencia administrativa" formada a partir de las resoluciones emitidas, por lo que ahí donde exista la necesidad de conocer, habrá una resolución respetuosa de los derechos en juego, como debe ser en toda sociedad que se precie de ser democrática.

Notas

1 Lujambio Irazábal, Alonso y Lina Ornelas N., "Personal Data Protection by the Government: the action of the Instituto Federal de Transparencia y Acceso a la Información Pública", dataprotectionreview.eu, Madrid, España, octubre, 2007.

2 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.

3 Citado por BALLESTEROS MOFFA, Luis Ángel. La privacidad electrónica, Tirant lo Blanch, Valencia, 2005, pp. 30 y 31.

4 Tal fue el caso de Reino Unido, Canadá, Estados Unidos, España, Costa Rica y Australia.

5Amparo Directo en revisión número 402/2007.

6 NOVOA MONREAL, Eduardo. Derecho a la Vida Privada y Libertad de Información. Un conflicto de derechos. Ed. Siglo Veintiuno Editores. México, 1979, p. 31.

Bibliografía

BALLESTEROS MOFFA, Luis Ángel. La privacidad electrónica, Tirant lo Blanch, Valencia, 2005.

BARRERO ORTEGA, Abraham, Juicios paralelos y Constitución: su relación con el periodismo, en Revista andaluza de comunicación, 2001, primer semestre.

CASTILLO CÓRDOVA, Luis. Un caso de internacionalización y constitucionalización. Las Libertades de Expresión e Información en la Jurisprudencia, en: Boletín Mexicano de Derecho Comparado, nueva serie, año XL, número 119, mayo-agosto de 2007.

NOVOA MONREAL, Eduardo. Derecho a la Vida Privada y Libertad de Información. Un conflicto de derechos. Ed. Siglo Veintiuno Editores. México, 1979

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.

Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad nacional[1]

Lina Ornelas Núñez y*
Edgardo Martínez Rojas

I. Introducción

En las últimas décadas el desarrollo científico ha abierto una brecha tecnológica sin precedentes llevando al ser humano a explorar terrenos hasta ahora desconocidos.

Este desarrollo ha impactado significativamente y de diversas formas en el tejido social, provocando con ello la necesidad de conducir dentro de los causes del Derecho esta nueva realidad.

Dicho impacto se ha presentado como un fenómeno que trasciende fronteras y no sólo con un matiz doméstico, en el que es posible, gracias a los avances de la ciencia, intercambiar información a través de los medios telemáticos. Ello ha traído consigo grandes ventajas en materia de comunicaciones, como la transferencia de millones de datos a través de las herramientas que nos proporciona la nueva tecnología, el mejor ejemplo de ello es Internet.

La inmersión en este nuevo mundo, ha puesto delante del hombre nuevos retos, entre otros, de qué forma canalizar en el cauce de lo jurídico estos desarrollos, sin sobrepasar los límites de intervención del Estado en la actividad de los particulares, en donde aquel se constituya en el fiel de la balanza.

---

* Lina Ornelas Núñez es abogada egresada de la Facultad de Derecho de la Universidad de Guadalajara. Maestra en Cooperación Legal Internacional por la Universidad Libre de Bruselas (Vrije Universiteit Brussel). Coordinadora de subgrupos de trabajo de la Red Iberoamericana de Protección de Datos. Actualmente es Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública (IFAI). Edgardo Martínez Rojas es abogado egresado de la Escuela Libre de Derecho, ex becario de la Agencia Española de Protección de Datos y candidato a doctor por la Universidad San Pablo CEU, Madrid, España. Fungió como Subdirector de Protección de Datos y posteriormente como Director de Clasificación y Datos Personales del IFAI.

En el terreno de los derechos fundamentales, muchos han sido los efectos producidos por el avance tecnológico, entre otros en las esferas de la privacidad, la intimidad o más específicamente aún, en el terreno del derecho a la protección de los datos personales2.

Por lo anterior, desde hace décadas que se viene buscando la manera de dar una respuesta que satisfaga de la mejor forma posible al desafío que representa la evolución tecnológica en el terreno de la utilización y movilidad de la información de las personas.

Diversos modelos legislativos han sido aplicados, encontrando los primeros en Europa, en la que desde los años sesenta, del siglo pasado, se ha trabajado de manera sistemática e institucional al respecto. Algunos años más tarde aparecen los primeros modelos normativos en América, quizá con menos fuerza y uniformidad, hablando en términos continentales.

El derecho a la protección de datos personales como hoy se encuentra perfilado en la doctrina más calificada es de reciente acuñación, encontrando su germen en el derecho a la intimidad personal y familiar, reconocido en diversos textos de carácter internacional en la época de la posguerra. Bajo esta atmósfera, la realidad europeo-americana se desenvuelve, a nivel internacional, en relación con los derechos humanos en las primeras décadas de la segunda mitad del siglo XX.

Por lo tanto, es precisamente en el ámbito de los derechos humanos donde inicia la zaga del derecho a la protección de datos personales, encapsulado en otros derechos, el derecho a la privacidad o en el derecho a la intimidad, reconocidos expresamente en distintos instrumentos internacionales tanto del Sistema Universal como Interamericano de derechos humanos.3

Conviene aquí hacer una distinción entre el derecho a la intimidad y el derecho a la protección de datos personales, ya que en ocasiones son términos utilizados de manera indistinta en la doctrina. Según señala Piñar Mañas, el derecho a la protección de datos de carácter personal: …" presenta caracteres propios que le dotan de una naturaleza autónoma, de tal forma que su contenido esencial lo distingue de otros derechos fundamentales, específicamente, del derecho a la intimidad, en el que éste último, tiende a caracterizarse como el derecho a ser dejado solo y evitar injerencias en la vida privada mientras que el derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de tratamiento por responsables públicos y privados".4

El concepto de privacidad a nivel internacional ha buscado evolucionar a la par del desarrollo de las tecnologías de la información, debido a que a través de las mismas es posible tratar datos personales, es decir recabar, utilizar, almacenar y transmitir, tanto en el sector público como en el privado, con una facilidad, hasta hace algunas décadas, inimaginable, de manera tal que el tratamiento de datos personales sin una regulación adecuada puede llegar a constituir una seria amenaza a la privacidad.

Por lo anterior, la reacción en el terreno de los derechos humanos no se hizo esperar, y a partir de derechos preexistentes en el terreno de las libertades fundamentales, como el derecho a la intimidad, surge un nuevo derecho fundamental que posibilita la autodeterminación informativa de su titular.5

Resulta pertinente resaltar que el Tribunal Constitucional Español, en su sentencia 292/2000, del 30 de noviembre ha dado luz sobre los alcances del derecho fundamental a la protección de datos personales, estableciendo su carácter autónomo e independiente, cuyo contenido persigue garantizar un poder de control de los individuos respecto de sus datos personales, así como el uso y destino de los mismos, con el propósito de impedir su tráfico ilícito y lesivo.6

De la sentencia del Alto Tribunal se deduce que, a través de la regulación del artículo 18 numeral cuarto de la Constitución Española, el constituyente quiso garantizar un verdadero derecho fundamental a la protección de datos, cuya garantía deberá preservarse frente a cualquier invasión o intromisión ilegítima, merced a un sistema de protección específico e idóneo, marcando las diferencias existentes entre el "habeas data" y el derecho a la intimidad".

Como se puede ver, el impacto de la ciencia, ha sido global7, influyendo prácticamente en todos y cada uno de los ámbitos de la convivencia humana, sin que hasta el momento sea posible afirmar que la fuerza con la que se ha intentado hacer frente a la situación hasta ahora generada por el avance tecnológico haya sido proporcional a la magnitud con la que la misma se presenta, sin echar por tierra los loables esfuerzos hasta ahora llevados a cabo en la Unión Europea.

Considerando la importancia de los efectos producidos por el avance de la tecnología en relación con la privacidad de las personas, el presente artículo tiene como finalidad poner de manifiesto la importancia de conocer y contar con un derecho a la protección de datos personales y como se ha convertido en un asunto de interés internacional.

A efecto de lo anterior se describirán, en lo general, el concepto de derecho a la protección de datos y su recepción en México, para inmediatamente después enfocar el análisis en las transferencias internacionales de datos personales, abordando aspectos como definición y tipos de regímenes a que se sujetan las transferencias internacionales de datos, para de esta forma mostrar la importancia de contar con un instrumento que las regule, tanto en el terreno del comercio internacional, fundamentalmente dirigido al intercambio comercial desarrollado en el sector privado, como en el ámbito de la seguridad nacional, en cuanto a las transmisiones de datos que se producen entre Estados.

Conviene señalar que el estudio en relación con las transferencias internacionales de datos personales, dada la amplitud de la materia, se circunscribirá al comercio internacional en Internet, así como a la seguridad nacional.

II. Actualidad del derecho a la protección de datos en México

A manera de preámbulo, conviene apuntar que el primer instrumento legislativo, en el que se regula el derecho a la protección de datos de carácter personal es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental8, (LAI) misma que, paradójicamente, tiene por finalidad proveer lo necesario para garantizar el acceso de toda persona a los documentos en posesión de las entidades públicas-gubernamentales en el ámbito federal.9

Como consecuencia de lo anterior, por lo que hace al ámbito de aplicación, la regulación establecida en la LAI se limita a los sistemas de datos personales del sector público-gubernamental a nivel federal.

En cuanto a las disposiciones de carácter sustantivo como los principios, derechos y deberes en relación al derecho a la protección de los datos de carácter personal en el Capítulo IV, del Título Primero de la LAI se dispone lo siguiente:

Se establecen los principios de calidad, finalidad y consentimiento (con un listado de excepciones al principio del consentimiento);

Se reconocen los derechos de los interesados al acceso, rectificación e información respecto a sus datos;

Se señalan como deberes de los sujetos que traten datos personales el relativo a la adopción de las medidas necesarias que garanticen la seguridad de los datos personales, así como el de confidencialidad.

Se prevé la existencia de un registro ante el que se deben inscribir los "sistemas de datos personales"10

En relación con la autoridad la LAI prevé en su artículo 33 la existencia de una "autoridad independiente" denominada Instituto Federal de Acceso a la Información (IFAI)11 al cual se le encomienda la función de garantizar el derecho de acceso a la información pública gubernamental por una parte y por la otra el derecho a la protección de datos de carácter personal.

Dicho lo anterior conviene preguntarse qué elementos de aquellos que componen la columna vertebral del derecho a la protección de datos no se encuentran presentes en el ordenamiento mexicano. En tal sentido, considerando los alcances del presente documento se han elegido tres instrumentos internacionales como referente para responder al cuestionamiento formulado, a saber la Directiva 95/46/CE de 24 de octubre de 1995 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46), la recomendación de la Organización para la Cooperación y Desarrollo Económicos en la que se contienen las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos

personales, adoptada el 23 de septiembre de 1980 (Recomendaciones de la OCDE) y la Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas (Resolución 45/95 de la ONU), de 14 de diciembre de 1990.

Entre los elementos comunes12 en la Directiva 95/4613, en las Recomendaciones de la OCDE y la Resolución 45/95 de la ONU, en términos generales, se advierte la ausencia de los siguientes en la norma mexicana:

Aplicación de la norma en la materia a los sistemas de datos personales de carácter privado;

Existencia de un régimen aplicable a los flujos transfronterizos de datos;

Reconocimiento de categorías especiales de datos, y

Delimitación expresa en ley de los supuestos de excepción a los principios aplicables en la materia.

De modo que resulta evidente la necesidad de contar con una ley comprehensiva en materia de protección de datos personales que abarque tanto al sector público como al privado, que además de contener los principios de protección internacionalmente aceptados y tutele los derechos de sus titulares a través de la creación de una autoridad independiente, prevea un régimen aplicable a los flujos transfronterizos de datos personales.

Lo anterior, incrementa su importancia en el caso mexicano dado que a diferencia de muchos de los países de la región cuenta con condiciones geopolíticas únicas y que le son propias, debido fundamentalmente a dos factores, el primero, su posición geográfica colindante con los Estados Unidos de América, el segundo, los acuerdos comerciales en los que se ha integrado como el Tratado de Libre Comercio de América del Norte (TLCAN) y el Tratado de Libre Comercio con la Unión Europea (TLCUE), así como la pertenencia a la Organización para la Cooperación y Desarrollo Económicos (OCDE) y al Acuerdo de Cooperación Asia Pacífico (APEC), entre otros instrumentos internacionales.

III. Concepto y tipos de transferencias internacionales de datos personales

En términos del criterio hasta ahora utilizado, para efectos del concepto y tipos de transferencias en razón de los sujetos, se hará alusión a los instrumentos internacionales citados en el apartado anterior, así como a algunas disposiciones de carácter nacional que de los mismos han derivado.

Las Recomendaciones de la OCDE, establecen que por "circulación transfronteriza de datos personales" se entenderá los movimientos de datos personales a través de fronteras nacionales.14

Tanto en el caso de la Directiva 96/46, como en el de la Resolución 45/95 de la ONU, no se establece propiamente una definición de lo que para efectos de dichos instrumentos debe entenderse por transmisión internacional de datos personales.

No obstante lo anterior, y derivado de la transposición de la Directiva 95/46, en el Reino de España, fue expedida por la Agencia Española de Protección de Datos la Instrucción 1/200015, de 1 de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos, la cual define las transferencias internacionales de datos como toda transmisión de los mismos fuera del territorio español, en particular, las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero16.

Las implicaciones de la definición propuesta en la Instrucción 1/2000, antes citada, nos lleva a hacer referencia a los tipos de transferencia que existen en razón de la calificación de los sujetos involucrados en la misma.

De acuerdo con lo expuesto, en el ordenamiento español es posible distinguir dos modalidades de transferencias internacionales en función de la calificación del sujeto receptor de los datos.

La primera modalidad se encuentra recogida en el artículo 11 de la LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), según la cual el sujeto transmitente puede provocar una cesión o transmisión de datos a un tercero localizado en el extranjero, operación que supone que el tercero17 que actúa por cuenta propia decidiendo sobre la finalidad, uso y contenido del tratamiento.

La segunda modalidad está directamente relacionada con la hipótesis prevista en el artículo 12 de la LOPD, ya que en ésta el sujeto que comunica los datos, lleva a cabo la transmisión de los mismos, a otro sujeto ubicado en el extranjero, para que se realice un determinado tratamiento a su nombre y por su cuenta.

En ese orden de ideas, si bien es cierto las transferencias "relevantes" para efectos del ordenamiento español son aquellas que suponen una transmisión de un responsable a otro responsable, también califican como transferencias internacionales las que implican una transmisión de un responsable a un encargado.18

Aunado a lo anterior y debido a la gran relevancia que tienen en la actualidad las trasmisiones con fines comerciales, así como las gubernamentales por razones de seguridad nacional, se hará una mención especial a éstas en los apartados subsecuentes.

1. Transferencias internacionales de datos personales con fines comerciales

México tiene celebrados diversos acuerdos en materia de comercio internacional en diversos puntos del orbe, al amparo de los cuales el incremento de los flujos internacionales de datos promovidos en un contexto de internacionalización económica y de desarrollo tecnológico es cada día más grande.

Tal situación ha llevado en otras latitudes a la confrontación entre los intereses económicos de liberalización del tráfico de datos y la necesidad de proteger el derecho de las personas a disponer libremente de sus datos personales.

En el caso mexicano, derivado del intenso intercambio con sus socios comerciales (Estados Unidos de América y Canadá), se llevan a cabo constantes transferencias internacionales de datos personales, sin que hasta el momento exista una regulación mínima en la que se observen los principios internacionalmente reconocidos en la materia.

Lo anterior principalmente en la relación con los Estados Unidos de América, ya que el caso Canadiense es distinto, toda vez que dicho país cuenta con leyes tanto a nivel federal como provincial en materia de protección de datos, así como con el reconocimiento de la Unión Europea de país con nivel adecuado de protección19.

Por lo que hace al Acuerdo de asociación económica, concertación política y cooperación entre la Comunidad Europea y sus Estados miembros, por una parte, y los Estados Unidos Mexicanos, por la otra, también denominado Tratado de Libre Comercio con la Unión Europea (TLCUE), el artículo 41 contempla la cooperación en materia de protección de los datos de carácter personal con vistas a mejorar su nivel de protección y prevenir los obstáculos a los intercambios que requieran transferencia de datos de carácter personal, y en su artículo 51 se señala que las partes se obligan a garantizar un grado elevado de protección respecto al tratamiento de los mismos.

Las disposiciones de referencia implican para el Estado Mexicano un compromiso en dos vertientes, el primero implica el establecimiento de mecanismos que en este momento garanticen la protección de los datos personales provenientes de alguno de los países integrantes de la Unión Europea, y el segundo plantea la necesidad de resolver la cuestión mediante una solución de más largo alcance, en todos los sentidos, como lo sería el diseño de un marco normativo que sustente jurídicamente y con amplio espectro el actuar de los sujetos involucrados en el intercambio de datos desde y hacia nuestro país.

Frente a esta realidad, en una búsqueda de una solución inmediata debemos resaltar, en términos muy generales, la importancia de los mecanismos explorados en el seno del Asia Pacific Economic Cooperation (APEC)20, ante la carencia de marcos normativos nacionales, como lo es el "Marco de Privacidad de APEC" que fue desarrollado sobre la base de las Recomendaciones de la OCDE.

1.1 La autorregulación en las transferencias internacionales de datos en México

Es innegable que la autorregulación constituye una herramienta atractiva para los sectores comerciales o de servicios, entre otras cuestiones, porque se ajusta a sus necesidades siempre cambiantes, por tanto, hace flexible su modificación en caso necesario, sin tener que pasar por el complejo aparato legislativo.

La autorregulación ha surgido como la reglamentación derivada de la autonomía privada de los empresarios que tratan datos o de las organizaciones en que se agrupan para adoptar códigos de conducta o códigos tipo, ajustados a las peculiaridades del sector que representan.

La autorregulación es un mecanismo que ha sido fomentado desde la OCDE y también desde la normatividad de la Unión Europea a través de la Directiva 95/46, la Directiva 2002/58/CE sobre tratamiento de datos personales y protección de la intimidad en las comunicaciones electrónicas, así como la Directiva 2000/31/CE sobre el comercio electrónico.

Según quedó apuntado en el apartado anterior, México no cuenta actualmente con un marco normativo nacional en materia de flujos transfronterizos de datos de carácter personal, lo que no significa que la materia resulte del todo ajena en el país.

La Secretaría de Economía y la Procuraduría Federal del Consumidor, por una parte, y por la otra, la Asociación Mexicana de Internet, A.C. (AMIPCI) suscribieron, en noviembre de 2006, un convenio de colaboración con el objeto de establecer los mecanismos de cooperación para dotar a la industria de un medio que brinde elementos de confianza al consumidor respecto al cumplimiento de obligaciones contraídas por los proveedores de bienes y servicios a través de Internet, relativos entre otros, a la existencia física del proveedor y a la protección de los datos personales del consumidor mediante la implementación y uso de sellos de confianza.

En el mencionado Convenio se reflejan los principios de APEC21, y su suscripción derivará en convenios específicos entre la AMIPCI y empresas privadas, a efecto de que la primera revise la adecuada protección de datos personales y otorgue, en su caso, sellos de confianza a las mencionadas empresas. La figura de los sellos de confianza (trustmark) se ha establecido en otros países para diversos fines y con resultados exitosos.

En ese sentido, la existencia de los sellos de confianza y en general, el acreditar que se cumple con los estándares establecidos en un instrumento nacido en el terreno de la autorregulación, puede reportar grandes beneficios en el ámbito comercial, como lo es la obtención de una cartera de clientes fiel a la empresa, debido a la certidumbre generada por ésta, en relación al tratamiento de sus datos personales y su consecuente impacto económico, reflejado en las ganancias de la empresa.

En cuanto a las cuestiones que podrían mejorarse en el esquema de sellos de confianza está el que en su configuración e implementación se debería fomentar, entre otros elementos, la utilización de medios avanzados de cifrado para reforzar las garantías de confidencialidad de la información que circula por las redes abiertas de telecomunicaciones y en particular por Internet, y a través de la firma digital, la integridad de los mensajes y transacciones, sobre todo, porque no debemos olvidar que el acopio de datos permite obtener una evaluación de la personalidad de los individuos.

Es muy temprano todavía para determinar la eficacia de estos mecanismos en la efectiva protección de datos personales, ya que debemos reconocer que pueden tener deficiencias importantes como las señaladas anteriormente, a las que se puede agregar la carencia de verificación de la existencia de medidas de seguridad..

Sin embargo, y a pesar de lo anterior, deben alentarse modelos como el mexicano, que puede resultar ejemplar para el resto de los países de APEC, ya que la propia AMIPCI empieza a contar entre los poseedores de sellos de confianza con entidades gubernamentales, las cuales, voluntariamente aceptan que además de las reglas para llegar a ser miembros, se constriñan a la necesidad de cumplir con los Lineamientos de Protección de Datos Personales emitidos por el IFAI. Lo anterior con independencia de las facultades de dicha instancia como autoridad en materia de protección de datos dentro de la Administración Pública Federal.

De modo que la ausencia de un marco normativo no impide la combinación entre el sector privado y el público para lograr objetivos conjuntos. De hecho, el alentar este tipo de esfuerzos puede llevar a que se logren mejores prácticas y soluciones de impacto inmediato que a través de las leyes resulta difícil alcanzar.

2. Transferencias internacionales de datos personales entre gobiernos por motivos de seguridad nacional

Los gobiernos, en el ámbito de la cooperación internacional con otros países en materia de lucha contra el terrorismo y las formas graves de delincuencia organizada poseen sistemas de datos personales que permiten detectar a aquellos individuos que constituyen o pueden constituir un riesgo o amenaza potencial a la seguridad de uno o varios Estados.

Consecuencia de lo anterior, los gobiernos han venido intercambiando datos de las personas con los fines antes señalados, sin embargo, luego de los atentados terroristas del 11 de septiembre 2001 en los Estados Unidos de América, así como los subsecuentes de Madrid y Londres en 2004 y 2005, respectivamente, se ha acentuado el valor de estas bases de datos, en el sentido de mantenerlas actualizadas, de ampliar los tipos de datos recabados (que pueden incluir las intervenciones telefónicas por ejemplo), así como los perfiles que de las personas pueden obtenerse, y finalmente, se ha propiciado un intercambio más profuso e intenso de manera transnacional.

En materia de privacidad, la circulación transfronteriza de la información personal, plantea desafíos únicos relacionados con la protección de las personas en el ámbito de su información privada. Por lo anterior, las Autoridades de Protección de Datos Personales a nivel internacional, han llamado la atención en repetidas ocasiones a los Gobiernos, con el fin de encontrar un equilibrio entre la seguridad de los países y los límites en la

comunicación de la información privada de sus ciudadanos. Para lograr este objetivo, los Gobiernos, no pueden desconocer los alcances de los mandatos que tienen conferidos por ley. El reto en ese tenor, es lograr programas de información de inteligencia y análisis de riesgos que respeten en la mayor medida de lo posible las libertades y las garantías fundamentales de los gobernados.

Diversas son las medidas que los gobiernos han establecido para hacer frente al terrorismo en el plano doméstico como en el internacional, consecuencia de las cuales el Estado se ha visto en la necesidad de "irrumpir" en ámbitos de la esfera jurídica del ciudadano que pueden llegar a provocar una colisión de derechos.

Por una parte, se tiene la obligación del Estado de evitar la realización de actos lesivos de la seguridad nacional, y por la otra, el derecho de los ciudadanos a conservar un espacio propio dentro del cual desarrollarse libremente y sin injerencia alguna, incluido el propio Estado.

Los alcances de las disposiciones en materia de protección de datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental son limitados ya que el legislador en México, no estableció un régimen especial para regular sistemas de datos personales para la investigación del terrorismo y de formas graves de delincuencia organizada.

Con el fin de poner de relieve la importancia que en los últimos años ha cobrado el tema de la transferencia de datos personales entre gobiernos, con motivos de seguridad nacional, se expondrá de manera muy breve la problemática surgida a partir de los requerimientos efectuados por el Gobierno Norteamericano a las compañías aéreas o marítimas que operan en su territorio.

2.1 La transferencia de datos a raíz de la Patriot Act y la respuesta de la Unión Europea

Entre otras muchas cuestiones, los lamentables sucesos del 11 de septiembre vinieron a demostrar que el terrorismo es un problema no sólo internacional, sino mundial (cuestión que desafortunadamente se ha venido corroborando con posteriores ataques en ciudades europeas, así como en oriente medio y el sureste asiático).

Considerando los niveles que ha alcanzado el problema del terrorismo, no hay lugar a dudas de la necesidad que a nivel mundial existe de hacerle frente, la pregunta es ¿cómo hacerlo? Está claro que al interior cada país decidirá "soberanamente" cuál es la mejor estrategia para encararlo, dentro de los límites de su orden jurídico nacional. El problema se presenta respecto de las decisiones que se adopten con efectos que trasciendan al ámbito internacional.

Como es de conocimiento público, con motivo de los ataques terroristas del 11 de septiembre de 2001, los Estados Unidos de América adoptaron diversas medidas para hacerle frente a tal problema. Entre las mismas, el Gobierno Norteamericano expidió

la Patriot Act (Ley Patriota) en el mes de octubre de 2001, cuya finalidad, en términos generales, es salvaguardar la seguridad nacional en los Estados Unidos de América (en adelante EUA).

En este sentido y a raíz de la Patriot Act, EUA emitió disposiciones22 que establecen la obligación de que las compañías aéreas o marítimas que operen en su territorio le faciliten los datos relativos a los pasajeros y la tripulación. Estas transferencias se realizarán en un medio electrónico y deben ser completadas antes del despegue del avión.

Dicho medio electrónico es el Sistema de Información Avanzada sobre Pasajeros (APIS) y se compone de una lista de datos respecto de cada persona física que viaja de y a Estados Unidos. En un principio, los datos requeridos estaban intrínsecamente relacionados con el vuelo tomado, el visado o el permiso de residencia para los Estados Unidos, así como con información identificativa como la que figura en los pasaportes. Sin embargo, ahora no sólo se requieren esos datos sino otros más. En general, los datos que se transfieren son los siguientes: nombre, fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los EUA, lugar y fecha de expedición (si corresponde), número de registro extranjero (si corresponde), domicilio en los EUA durante la estancia, así como cualquier otro dato que se considere necesario para identificar a los viajeros, fecha de la reservación, la agencia de viajes cuando corresponda, la información que se muestra en el boleto, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de asiento y datos anteriores del PNR (Passenger Name Records). En estos últimos pueden constar no sólo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etc.), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (Frequent Fliers number).23

Asimismo, dichos datos pueden ser transmitidos a otras autoridades federales, estatales y locales, así como a agencias extranjeras encargadas de la investigación y persecución de actos violatorios de leyes civiles y penales, en caso de que se advierta la posibilidad de una potencial violación de dichas leyes.24

Teniendo en cuenta el impacto que la normatividad emitida por los EUA produciría en el ámbito comunitario, se dio inicio a una serie de negociaciones entre autoridades europeas y norteamericanas, adoptándose con fecha 14 de mayo de 2004, por parte de la

Comisión Europea, la Decisión sobre el carácter adecuado de la protección, en la que se determinó que la Oficina de Aduanas y Protección de Fronteras de los EUA garantizaba un nivel de protección adecuado de los datos transferidos desde la Comunidad. Por su parte, con fecha 17 de mayo de 2004, el Consejo adoptó la Decisión por la que aprobó la celebración de un Acuerdo entre la Comunidad Europea y los EUA sobre el tratamiento y la transferencia de los datos de los pasajeros y la tripulación por parte de las compañías aéreas establecidas en el territorio de los Estados miembros de la Comunidad a la Oficina de Aduanas y Protección de Fronteras de EUA.25

Derivado de lo anterior, el Parlamento Europeo requirió al Tribunal de Justicia de las Comunidades Europeas que anulase la Decisión del Consejo (asunto C-317/04) y la Decisión sobre el carácter adecuado de la protección (asunto C-318/04), alegando fundamentalmente que esta última Decisión se adoptó ultra vires, que el artículo 95 CE no constituye una base jurídica procedente para la Decisión por la que se aprueba la celebración del Acuerdo y que en ambos casos existe una violación de los derechos fundamentales26.

El Tribunal de Justicia resolvió anular las decisiones de referencia sobre la base de la Directiva 95/46/CE en el sentido de que el artículo 3, apartado 2 de la Directiva excluye de su ámbito de aplicación el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario y, en cualquier caso, el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

El Tribunal advirtió que, de la Decisión sobre el carácter adecuado de la protección, se desprende que la exigencia de que se transfieran los datos se basa en la normativa estadounidense relativa a la intensificación de la seguridad. En consecuencia, la transferencia de los datos de los pasajeros y tripulación a la Oficina de Aduanas y Protección de Fronteras de los EUA constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal.

En resumen, lo anterior significa que en virtud de la arquitectura competencial trazada en la Unión Europea (UE), los acuerdos celebrados entre ésta y los EUA son declarados nulos por haberse celebrado por autoridades incompetentes en la materia.

Más allá de la nulidad declarada por el Tribunal de Justicia de las Comunidades Europeas para este caso en particular, en razón de la competencia y atribuciones de las autoridades correspondientes, conviene analizar la razón por la cual se celebraron los acuerdos entre la UE y los EUA, que derivaron en las decisiones anuladas.

En el ámbito de la protección de datos personales, de competencia comunitaria, por lo que se refiere a transferencias internacionales de datos a países terceros, el principio que rige es que los Estados Miembros de la UE sólo pueden autorizar transferencias a aquéllos que aseguren un nivel de protección adecuado.

De acuerdo con el artículo 25 de la Directiva 95/46/CE, el carácter adecuado del nivel de protección que ofrece un país tercero se evalúa atendiendo a todas las circunstancias que concurran en una transferencia en particular, de conformidad con la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

En tal sentido, la Comisión Europea puede hacer constar que un país tercero garantiza un nivel de protección adecuado, a la vista de su legislación interna o de sus compromisos internacionales suscritos.27

El punto de partida para llevar a cabo transferencias internacionales de datos a países terceros es la observancia de los siguientes principios generales:28

Limitación de objetivos: los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.

Proporcionalidad y calidad de los datos: los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

Transparencia: debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.23 y 13 de la Directiva.

Seguridad: el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

Derechos de acceso, rectificación y oposición: el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

Restricciones respecto a transferencias sucesivas a otros terceros países: únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.

En términos de lo descrito, el hecho de que los EUA no se encontrara entre los países considerados por la UE, como uno de aquellos que cuenta con un nivel adecuado de protección de datos, según los elementos señalados, y ante la anulación de las decisiones anteriormente señaladas, se hizo necesaria la celebración de una serie de negociaciones tendentes a remediar tal situación entre ese país y la UE.

Finalmente, con fecha 6 de octubre de 2006, se adoptó un nuevo acuerdo de carácter provisional entre los EUA y la UE, con fundamento en el cual podría continuarse con la transmisión de los datos de referencia, entre los EUA y la UE, bajo ciertos parámetros, vigente hasta el 31 de julio de 2007, salvo que se acuerde una extensión del mismo.29

Con el caso expuesto, queda claro que para la UE el que las transferencias internacionales de datos personales, incluso para aquellos transmitidos para la investigación del terrorismo, se llevan a cabo bajo un control mínimo de la autoridad competente representa uno de los temas de mayor relevancia dentro de su agenda internacional.

3. México y las transferencias internacionales

De acuerdo con lo indicado en el apartado anterior, es posible afirmar, al menos hasta el día de hoy, que existe una duda fundada de que los EUA cuenten con un marco normativo respetuoso del derecho fundamental a la protección de datos, entendido éste como el poder de disposición y de control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, sea el Estado o un particular, y que también permite al individuo saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso30

En el caso mexicano, el asunto de la transmisión de datos de los mexicanos a un gobierno extranjero se presenta de manera diversa a la realidad europea, debido, por una parte, a la ausencia de una disposición de carácter constitucional que reconozca expresamente el derecho a la protección de datos personales. 31

Como se apuntó en apartados anteriores, únicamente se cuenta con una regulación básica a nivel federal en torno al derecho a la protección de datos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y desarrollos administrativos posteriores (Lineamientos de Protección de Datos Personales), que permiten proteger aquellos datos de carácter personal objeto de tratamiento por parte de los entes gubernamentales, así como las leyes estatales, tal como la de Colima, que cumplen con funciones similares dentro de su ámbito competencial.

Es evidente que no resulta suficiente el esquema regulatorio en materia de protección de datos personales con que se cuenta actualmente, por el simple hecho de que hay sectores que carecen de una normatividad mínima que reconozca dicho derecho, esto es, se ha avanzado por el camino correcto, al haberse expedido ya una normatividad "secto-

rial" a través de la cual los particulares pueden exigir la tutela de ciertas prerrogativas, es necesario irradiarlo a toda la sociedad mexicana, en la que con independencia de las particularidades que deba observar este derecho en sus distintos campos de aplicación (gubernamental, mercantil, en Internet) debe existir un umbral mínimo de principios aplicables a todos los gobernados.

Ahora bien, en relación con los datos de pasajeros y tripulación que se transfieren a los EUA mediante el APIS, es de señalar que, si bien las transmisiones que se han mencionado son hechas directamente por aerolíneas privadas, lo cierto es que el Gobierno Mexicano requiere verificar que dichas transmisiones sean acordes con una política respetuosa de los derechos fundamentales.

En específico, no se advierte que se esté cumpliendo con el principio de información ni con el principio de finalidad. Es decir, no se ha demostrado la necesidad de realizar dicha transferencia y no parece aceptable que una decisión unilateral, tomada por un tercer país por motivos que obedecen a sus propios intereses públicos, lleve a efectuar de manera periódica y sistemática las transferencias de datos antes señalados.

Cabe señalar, a manera de referencia, que en leyes como LOPD, si bien exceptúa de su ámbito de aplicación a los datos personales relacionados con los sistemas de datos personales establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, prevé para los responsables de este tipo de sistemas, la obligación de comunicar de manera previa a la Agencia Española de Protección de Datos lo siguiente:

1. La existencia del sistema;
2. Las características generales del sistema, y
3. La finalidad para la que será utilizado el sistema.

Se considera por tanto que, si bien como se ha dicho, las transmisiones son hechas por aerolíneas privadas, sean los gobiernos quienes determinen, a través de normatividad que emitan ambos, los datos que deben transmitirse y la protección adecuada a los mismos.

Ahora bien, cabe señalar que en el ámbito continental, existe la Alianza para la Seguridad y la Prosperidad de América del Norte, la cual es un proceso trilateral, permanente, para una mayor integración de América del Norte, a través de la cual México, Estados Unidos y Canadá comparten una agenda en materia de prosperidad y seguridad.

De los dos Informes que se han presentado a los Mandatarios, en junio de 2005 y agosto de 2006, se desprende claramente que se han iniciado acciones para el intercambio de información de diversa índole entre los tres países. Dentro de los puntos a destacar, contenidos en la Agenda de Seguridad cuyo desarrollo se encuentra ya en proceso se encuentran los siguientes:

> "Trabajaremos para desarrollar sistemas que impidan que los viajeros de alto riesgo ingresen a América del Norte, que a la vez faciliten el tránsito legal de personas hacia

> y dentro de la región, a través de mejoras a nuestra capacidad para verificar la identidad de los mismos…probaremos tecnología y realizaremos recomendaciones para mejorar el uso de la biométrica en la inspección de viajeros con destino a América del Norte, con miras a desarrollar sistemas biométricos fronterizos y de migración compatibles. Desarrollaremos estándares seguros para documentos de status migratorio y de nacionalidad con un menor costo, que faciliten el cruce transfronterizo, con el fin de obtener una producción óptima antes del 1 de enero de 2008. Dentro de los próximos 36 meses, diseñaremos un sistema de registro único e integral de los programas de viajeros confiables en América del Norte...
>
> Dentro de un período de 36 meses, diseñar un programa único e integrado de inscripción global para viajeros de confianza de América del Norte (p. Ej. NEXUS, FAST, SENTRI) para el viaje por aire, tierra y mar...
>
> Mejorar la cooperación de intercambio de información y aplicación de la ley entre investigadores y fiscales, para dirigirse a actividades ilegales entre puertos de entrada y crimen organizado transfronterizo, contrabando de bienes, crímenes económicos, y el trafico de alcohol, armas de fuego, drogas ilegales y explosivos...
>
> Mejorar nuestras capacidades para combatir el terrorismo a través del intercambio apropiado de listas de terroristas (terrorist wathclists) y el establecimiento de vínculos entre las autoridades de Canadá, Estados Unidos y México...
>
> A fin de fortalecer la integridad y seguridad de los sistemas de determinación de asilo y refugiados, Estados Unidos y Canadá lanzaron un proyecto piloto para compartir información de solicitantes de refugio y de asilo con base en la comparación de registros de huellas digitales."32

A partir de lo anterior, se advierte que México está coadyuvando en el ámbito de América del Norte de diversas formas en términos de lo antes apuntado, intercambiando, entre otros datos información relativa a la comisión de delitos.

Se considera que dicho intercambio es importante para lograr los diversos objetivos de seguridad y prosperidad de los Estados. No obstante, es de vital importancia que dicho intercambio cuente con la base jurídica adecuada, y que los datos que se transfieran cumplan de manera estricta con los principios de protección de datos personales internacionalmente reconocidos, incluyendo específicamente el principio de finalidad y las medidas de seguridad adecuadas en la transmisión33.

IV. Conclusiones

El derecho a la protección de datos puede definirse como el poder de disposición y de control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero,

así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.

En el actual contexto de internacionalización económica y desarrollo tecnológico, la existencia de un régimen que regule el flujo transfronterizo de datos constituye un elemento a través del cual es posible garantizar la libre circulación de datos personales, así como el respeto a derechos fundamentales.

En ese sentido, al establecerse un régimen que regule las transferencias internacionales de datos el legislador debe tener en todo momento en cuenta los intereses en presencia, de manera tal que, por una parte, los controles que el Estado establezca no se traduzcan en obstáculos o barreras que entorpezcan injustificadamente la actividad comercial, y por la otra, que la política a seguir al respecto, no resulte tan laxa que el derecho a la protección de datos quede vaciado de contenido, una vez que los datos hayan salido del territorio nacional.

De esta forma, el primer paso que el Gobierno Mexicano debe dar en aras de alcanzar la meta apuntada, es el promover una reforma constitucional que reconozca el derecho fundamental a la protección de datos personales, para que a partir de ella, en un esfuerzo conjunto entre gobierno y sociedad, se continúe con el proceso para la emisión de una ley de protección de datos personales, que permita el ejercicio efectivo de este derecho en todos los ámbitos en los que son recabados dichos datos.

Considerando que las reformas constitucional y legislativa constituyen objetivos que, en el mejor de los escenarios se alcanzarían en el mediano plazo, se hace necesario que el Gobierno Federal adopte medidas de manera inmediata tendentes a mejorar la situación que actualmente subsiste en ámbitos como el de la seguridad nacional. Dichas medidas se pueden traducir en la celebración de convenios internacionales, en los que el Estado Mexicano, empiece a preparar el camino sobre el que se transitará en los próximos años.

El contar con una regulación equilibrada en materia de protección de datos, y en consecuencia tratándose de transferencias internacionales, puede llegar a erigirse en un factor que fortalezca la integración económica en bloques comerciales de los que México ya es parte.

Es importante hacer notar que la existencia de una normatividad en materia de protección de datos, en la que se encuentren debidamente ponderados los intereses en presencia, no constituye un freno a la actividad económica sino más bien representa una herramienta eficaz para potenciar las transacciones económicas, así como para proteger los derechos de las personas vinculadas a dichas transacciones, por lo que a esta materia se refiere.

En cuanto al intercambio que entre Estados se llegue a generar en el ámbito de la seguridad nacional, la normativa relativa a la protección de datos tampoco representa

un límite para los gobiernos en el intercambio institucional que se deba llevar a cabo, ni para lograr acciones eficaces en contra de la delincuencia organizada, ya que sólo se observarán aquellos principios de protección esenciales para que el flujo que de los datos se produzca.

De modo que es imprescindible que los gobiernos adopten medidas eficaces en la lucha contra el terrorismo y que de igual forma, al aplicarlas se respeten los derechos fundamentales, ya que de lo contrario, como han afirmado las autoridades de protección de datos personales en el ámbito internacional, se estaría produciendo ya la primera y capital victoria de los terroristas: restringir el marco de las libertades y derechos que, afortunadamente caracterizan a las democracias en el mundo. Por lo anterior, es indispensable contar con la regulación adecuada que dote al gobernado de un blindaje especial, en el que a nivel gubernamental se garantice una protección a su información de carácter personal, con la que actualmente no se cuenta.

Notas

1 Ornelas Núñez, Lina y Edgardo Martínez R., "Transferencias internacionales de datos personales: su protección en el ámbito del comercio internacional y de seguridad nacional", Obra en homenaje al Dr. Héctor Fix Zamudio del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, Marcial Pons, España, 2007.

2 La expresión protección de datos hace alusión al amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte en su entorno personal, social o profesional. Vid. DAVARA RODRÍGUEZ, Miguel Ángel. Manual de protección de datos para abogados, Aranzadi, Navarra, 2006, p. 177.

3 El artículo 12 de la Declaración Universal de los Derechos del Hombre (10 de diciembre de 1948) 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. En el mismo sentido, el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales (14 de noviembre de 1950) reconoce el derecho de la persona al respeto de su vida privada y familiar, de su domicilio y correspondencia.Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966) 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. En el mismo tenor, la Convención Americana sobre derechos humanos (22 de noviembre de 1969) en su artículo 11, apartado 2 establece 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.

4 Vid. PIÑAR MAÑAS, José Luis. La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos), Tirant lo Blanch, Valencia, 2006, p 32.

5 El antecedente más importante de interpretación Constitucional se dio en Alemania con la sentencia del Tribunal Constitucional Federal Alemán sobre la Ley de Censos (1 BvR 209/83 ua), en el cual se reconoce la existencia de un nuevo derecho a la autodeterminación informativa, por el cual las personas pueden conocer quien, cuándo y cómo utiliza sus datos personales, además de reconocer que deben existir autoridades independientes que garanticen ese nuevo derecho.

6 GÓMEZ ROBLEDO Alonso y ORNELAS NÚÑEZ Lina, "La Protección de datos personales en México: El caso del Poder Ejecutivo Federal" UNAM, 2006, p. 15 y 16.

7 Ciertamente el desarrollo y creciente arraigo de las comunicaciones electrónicas en nuestra sociedad, en particular de Internet y su universo de servicios, ha supuesto un sinfín de nuevas necesidades o problemas en el contexto de la silenciosa revolución protagonizada por las nuevas tecnologías. Vid. BALLESTEROS MOFFA, Luis Ángel. La privacidad electrónica, Tirant lo Blanch, Valencia, 2005, p. 133.8Publicada en el Diario Oficial de la Federación el 11 de julio de 2002.

9Disponible en el vínculo: http://www.ifai.org.mx

10 "Conjunto ordenado de datos personales" de acuerdo con la definición aportada por la propia LAI (artículo 3 fracción XIII).

11 Es importante destacar que de acuerdo con la LAI, el IFAI es la autoridad competente a nivel administrativo para conocer de cuestiones relacionadas con acceso a la información y protección de datos, únicamente por lo que se refiere al Poder Ejecutivo Federal (artículo 33), ya que los Poderes Legislativo y Judicial, así como los órganos constitucionales autónomos cuentan con instancias espejo (artículo 61) al IFAI que llevan a cabo esta función de garante.

12 Comunes al menos en dos de los instrumentos jurídicos de referencia.

13 Se toma como referencia, al ser la norma jurídica conforme a la cual se encuentra regulado el derecho a la protección de datos en la Unión Europea.

14 Numeral 1, inciso a).

15 La LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, si bien, al igual que sucede en el caso de la Directiva 96/46, establece un articulado dedicado a los movimientos transfronterizos de datos personales, tampoco establece qué debe entenderse por los mismos.

16 Disponible en el vínculo: https://www.agpd.es/index.php?idSeccion=77.

17 Este tercero tiene la consideración de responsable del tratamiento.

18 Vid. SANCHO VILLA, Diana. Transferencia internacional de datos, Agencia Española de Protección de Datos, Madrid, 2003, p.25-27.

19 Para mayor referencia ver la Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act, consultable en https://www.agpd.es/index.php?idSeccion=256.

20 México tuvo un papel muy activo en el pasado foro denominado "APEC Australia 2007 meeting", en específico en el Seminario denominado "First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 2007: Creating Trust in developing Cross-Border Privacy Rules: Making Compliance Possible and Enforcement Credible when Personal Information Moves between Economies", cuyo centro de intercambio de experiencias y discusión fue el tema de la transferencia internacional de datos personales. También se participó en la Reunión del subgrupo de Privacidad de APEC (Asia-Pacific

Economic Cooperation).

21 México intervino en los Breakout Groups que se formaron a efecto de analizar las diversas alternativas que existen para establecer Cross Border Privacy Rules (CBPR) que permitan la implementación del APEC Privacy Framework de manera uniforme, a efecto de que la protección que otorga una empresa a los datos personales de sus clientes, sea reconocida en la transferencia internacional de dichos datos, por los demás países pertenecientes a APEC.

Asimismo, participó en el Subgrupo de Privacidad de APEC, el cual depende del Electronic Commerce Steering Group (ECSG), el cual presidió (a través de la Secretaría de Economía), abordándose diversas cuestiones relativas a proyectos existentes en materia de protección de datos personales dentro de las economías de APEC.

Dentro de las funciones específicas del ECSG (establecido en febrero de 1999) está el desarrollo de legislaciones y políticas compatibles entre las economías en el campo de la Privacidad, para lo cual ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguro y sin obstáculos. En este caso es importante resaltar, como se parte de un mecanismo de autorregulación destinado a provocar una respuesta legislativa contundente.

22 The Aviation and Transportation Security Act (noviembre de 2001) y The Enhanced Border Security and Visa Entry Reform Act (mayo 2002).

23 Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, aprobado el 24 de octubre de 2002 por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp66_es.pdf.

24 Privacy Impact Assessment, Advance Passenger Information System (APIS), Department of Homeland Security, 21 de marzo de 2005, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbpapis.pdf

25Boletín de prensa del Tribunal de Justicia de las Comunidades Europeas consultable en el sitio de Internet: http://curia.europa.eu/es/actu/communiques/cp06/aff/cp060046es.pdf

26 Idem.

27 Para mayor referencia ver artículo 25 de la Directiva 95/46.

28 Idem.

29 Documento consultable en el sitio de Internet http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/er/91183.pdf

30 Sentencia 292/2000 del Tribunal Constitucional de España, consultable en el sitio de Internet https://www.agpd.es/upload/Canal_Documentacion/Sentencias/Sentencia292.pdf

31 A pesar de que se han presentado diversas iniciativas de ley para regular la protección de los datos personales, es importante destacar que éstas no han sido aprobadas, entre otras razones de índole técnico-jurídico, porque no existe un fundamento expreso en la Constitución para que el Congreso legisle en la materia, de modo que será muy importante el impulso que se dé en lo particular, a dos iniciativas de Reforma Constitucional que podrán dar cauce al ejercicio de este derecho. La primera de las iniciativas de referencia fue presentada con fecha 5 de abril de 2006, por parte del senador Antonio García Torres del grupo parlamentario del Partido Revolucionario Institucional, ante la Cámara de Senadores. Dicha iniciativa fue formulada como una adición al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos -en adelante la Constitución Federal- para reconocer al derecho a la protección de datos personales, como

un derecho fundamental, en los siguientes términos:

"PROYECTO DE DECRETO POR EL CUAL SE ADICIONAN DOS PARRAFOS AL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

ARTÍCULO ÚNICO. Se adicionan tres párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que se insertan luego del primer párrafo y se recorren los subsecuentes, para quedar en los siguientes términos:

"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción 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 público, seguridad, salud o para proteger los derechos de tercero.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado."

Un aspecto de la mayor relevancia en cuanto a este proyecto es que el mismo fue aprobado en la anterior legislatura, con 77 votos a favor y 5 abstenciones, en la Cámara de Senadores y fue enviado a la Cámara de Diputados para los efectos constitucionales correspondientes, estando aún pendiente su discusión y aprobación en ésta última.

La segunda iniciativa de reforma constitucional se presentó el pasado 27 de marzo de 2007 de abril, por el Diputado Gustavo Parra del Partido Acción Nacional, que vendría a reforzar la señalada anteriormente, ya que dota al Congreso de facultades expresas para expedir la ley de la materia, esgrimiendo que es relevante no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino por los efectos esenciales que estos tienen sobre la economía nacional.

32Primer Reporte a Mandatarios,

http://web2.senasica.sagarpa.gob.mx/xportal/sen/qesen/Doc1914/SPP062705Report.pdf

[33] Cabe mencionar que con fecha 28 de mayo de 2007, se publicó el "Acuerdo del Consejo de Seguridad Nacional por el que se establece un Comité Especializado de Alto Nivel para coordinar las acciones del Poder Ejecutivo Federal" a efecto de dar cumplimiento a las obligaciones internacionales del Estado Mexicano en el ámbito nacional en materia de desarme, terrorismo y/o seguridad internacionales, por el cual se crea el Comité Especializado de Alto Nivel en materia de Desarme, Terrorismo y Seguridad Internacionales integrado por representantes de las secretarías de Relaciones Exteriores; Defensa Nacional; Marina; Seguridad Pública; Hacienda y Crédito Público; Comunicaciones y Transportes; de la Procuraduría General de la República; así como del Centro de Investigación y Seguridad Nacional, el cual ostentará la Secretaría General del Comité. Entre las facultades a destacar del citado Comité se encuentran las siguientes:

- Establecer las reglas para el intercambio de informes, datos o cooperación técnica entre las dependencias, relacionados con las obligaciones del Estado mexicano frente a la comunidad internacional en materia de desarme, terrorismo y/o seguridad internacionales;
- Solicitar, a través de su Secretaría General, la información exigida por los organismos y mecanismos establecidos por virtud de los tratados e instrumentos internacionales, a las personas físicas o jurídicas afectadas por los mismos.

Bibliografía

ARENAS RAMIRO, Mónica. El derecho fundamental a la protección de datos personales en Europa, Tirant lo Blanch, Valencia, 2005.

BALLESTEROS MOFFA, Luis Ángel. La privacidad electrónica, Tirant lo Blanch, Valencia, 2005.

CORROPIO GIL-DELGADO, María de los Reyes. Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet, Arellano, Madrid, 2000.

CORROPIO GIL-DELGADO, María de los Reyes. El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, De Arellano, Madrid, 2001.

CRAIG, Paul & BURGA, Gráinne De. EU Law text, cases and materials, Oxford, third edition, Oxford, 2003.

DAVARA RODRÍGUEZ, Miguel Ángel. Manual de protección de datos para abogados, Aranzadi, Navarra, 2006.

DAVARA RODRÍGUEZ, Miguel Ángel. La seguridad en las transacciones electrónicas, Universidad Pontificia Comillas, Madrid, 2005.

DAVARA RODRÍGUEZ, Miguel Ángel. La transposición de la Directiva sobre la privacidad y las comunicaciones electrónicas, Universidad Pontificia Comillas, Madrid, 2005.

FERNÁNDEZ SALMERÓN, Manuel. La protección de los datos personales en las Administraciones Públicas, Thomson-Civitas, Madrid, 2003.

GÓMEZ ROBLEDO Alonso y ORNELAS NÚÑEZ Lina, "La Protección de datos personales en México: El caso del Poder Ejecutivo Federal" UNAM, 2006.

MANGAS MARTÍN, Araceli y LIÑÁN NOGUERAS, Diego J. Instituciones y derecho de la Unión Europea, Tecnos, 5 edición, Madrid, 2005.

PIÑAR MAÑAS, José Luis. El derecho fundamental a la protección de datos personales, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Tirant lo Blanch, Valencia, 2005.

PIÑAR MAÑAS, José Luis. La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos), Tirant lo Blanch, Valencia, 2006.

SANCHO VILLA, Diana. Transferencia internacional de datos, De Arellano, Madrid, 2003.

UNIVERSIDAD DE NAVARRA Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Jornadas sobre la protección de la privacidad (Telecomunicaciones e Internet), Universidad de Navarra, Pamplona, 2000.

Direcciones electrónicas

http://www.un.org/spanish/aboutun/hrights.htm

http://www.derechos.org/nizkor/espana/doc/conveudh50.html.

http://www.derechos.org/nizkor/ley/pdcp.html

http://www.oas.org/juridico/spanish/Tratados/b-32.html
http://www.oas.org/juridico/spanish/Tratados/b-32.html
http://www.oecd.org/dataoecd/16/51/15590267.pdf
http://www.unhchr.ch/spanish/html/menu3/b/71_sp.htm
http://www.ifai.org.mx
https://www.agpd.es/upload/Canal_Documentacion/Sentencias/Sentencia292.pdf

El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a las redes sociales

Lina Ornelas

[…] la humanidad debe al niño
lo mejor que puede darle.1

Introducción

El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, a efecto de asegurar la autonomía de los individuos para decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias en dicha esfera personal. En particular, debe protegerse la información personal que niñas, niños y adolescentes proporcionan e intercambian en Internet a efecto de impedir su utilización inadecuada con fines distintos para los cuales ellos la proporcionaron.

Debe existir un balance entre asegurar la libertad de expresión en Internet de las niñas, niños y adolescentes sin que se afecte su dignidad como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un "espacio privado" sin tener consciencia plena de que son observados y monitoreados.

La evidencia muestra que en todos los países, se han verificado afectaciones al desarrollo de la personalidad de menores de edad, derivado de las invasiones a los espacios de intercambio de información e imágenes que ellos frecuentan.2 Los perfiles creados son almacenados, por lo que, aún borrada dicha información en Internet, ésta podrían ser utilizada en el futuro para conculcar otros derechos y libertades de los menores de edad ya en su vida adulta. Como afectación concreta podría ilustrarse a manera de ejemplo la no obtención de un determinado empleo por el hecho de que se conozcan cuáles eran sus gustos o preferencias durante la adolescencia.

Es innegable que hay un gran interés por conocer la información de los menores de edad. Internet ha facilitado dicha tarea. Distintos actores explotan la información de este

sector de la población, tales como la industria, a la cual le interesa por ejemplo, conocer hábitos de consumo, lugares visitados y su frecuencia, composición y situación de las familias, entre otros aspectos.

Por su parte, los trasgresores de la ley -ahora también virtuales- obtienen información de los propios menores de edad o bien, la extraen por otros medios, para la comisión de delitos como el secuestro, trata o explotación sexual.

Frente a la vulnerabilidad de los menores de edad y las nuevas formas de convivencia social a través de redes sociales digitales, el derecho no puede quedarse rezagado. Internet es un espacio lleno de oportunidades, es la puerta al mundo del conocimiento urbi et orbe, y uno de los nuevos roles del Estado consiste en el deber de esclarecer que no se trata de un espacio sin ley.

De tal forma que, el presente artículo se propone reflejar la evolución que han tenido los derechos humanos en general; el reconocimiento reciente de los derechos del niño y el nacimiento de un nuevo derecho fundamental a la protección de datos personales; las propuestas del Memorándum sobre la Protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes –Memorándum de Montevideo-, para concluir que los principios y derechos de protección de datos también resultan aplicables a este colectivo, y por tanto, el Estado debe actuar para garantizar su efectiva tutela.

Evolución de los derechos humanos

Los derechos humanos son normas que reconocen y protegen la dignidad de todos los seres humanos. Desde la perspectiva occidental de los derechos humanos, estos rigen la forma en que los individuos viven en sociedad, así como su relación con los gobiernos y las obligaciones que los gobiernos tienen para con ellos. De tal forma que, la ley de los derechos humanos obliga a los gobiernos a tomar una serie de medidas, y les impide tomar otras.

Los individuos, por su parte, también tiene responsabilidades: al hacer uso de sus derechos humanos, deben respetar los derechos de los demás. De esta forma, ningún gobierno, grupo o persona individual tiene derecho a llevar a cabo acto alguno que vulnere los derechos de los demás.

Los derechos humanos están basados en el respeto a la dignidad y el valor de cada persona como individuo y también como miembro de la sociedad. La responsabilidad para asegurar que los derechos sean respetados, protegidos y satisfechos reside finalmente en los gobiernos nacionales.

Esta responsabilidad también concierne a otros elementos de la sociedad a nivel de las instituciones internacionales, pasando por la comunidad y llegando hasta los individuos en sus familias.

Sin embargo, cabe recordar que lo que hoy se conoce como derechos humanos, es producto de la evolución histórica reflejada en generaciones de derechos. Esto es, los derechos humanos para su comprensión, han sido divididos en categorías históricas que encuentran sus orígenes en el seno de la modernidad.

Esta perspectiva evolutiva de los derechos humanos implica el reconocimiento de nuevos derechos que intentan dar respuesta, en su gran mayoría, a las nuevas necesidades históricas. Por otro lado, otros suponen la redimensión de viejos derechos.3 Tal como acontece en el fenómeno continuamente evolutivo de la sociedad tecnológica.

Derivado de lo anterior, ha prevalecido el reconocimiento de tres generaciones de derechos4 y se vislumbra una nueva oleada; aquella relativa a los derechos en el ciberespacio y la libertad informática.5 Así, cada etapa ha correspondido a un momento ideológico y social, con características particulares y rasgos diferenciadores, dependiendo de las necesidades de cada proceso evolutivo.

De tal forma que, la época burguesa del siglo XVIII marca el inicio de las etapas de los derechos humanos y, surgen de la Revolución Francesa como rebelión contra el Absolutismo. Las libertades individuales y la defensa de la persona se enmarcan como limitantes al poder público. Esta fase, se enfoca en la no injerencia con las libertades individuales y se configuran una serie de derechos relativos al aislamiento, tal como lo fue el derecho al honor, a la vida, a la integridad personal, así como el propio reconocimiento a la intimidad de la persona. Derecho que hoy, como consecuencia del desarrollo tecnológico y las nuevas formas de comunicación e información, ha sido necesario reformular en su alcance y contenido.

En consecuencia, una segunda generación de derechos humanos, encuentra sus orígenes en las luchas sociales del siglo XIX y abarca hasta ya entrado el siglo XX. Estos movimientos reivindicatorios pusieron en tela de juicio la necesidad de contemplar el catálogo de derechos y libertades de la primera generación, con una segunda oleada de derechos económicos, sociales y culturales, incorporados en la Declaración Universal de 1948, debido a los cuales, el Estado de Derecho pasa a una etapa superior, es decir, a un Estado Social de Derecho.

Dicha fase, se enfoca en garantizar los derechos de participación a través del involucramiento activo de los poderes públicos mediante prestaciones y servicios; más aun, se incorpora de una tradición del pensamiento humanista y socialista. Si bien, los derechos de primera generación defendían a los ciudadanos frente al poder estatal, en esta etapa se exige cierto grado de intervención del Estado para garantizar un acceso igualitario a los derechos de carácter económico y social, esto es, para compensar las desigualdades naturales e inherentes a todo entorno social.

Cabe destacar que, en los años transcurridos desde la Declaración Universal de Derechos Humanos de 1948, y con mayor urgencia desde el final de la Guerra Fría, un gran sistema internacional de lo que se llaman instrumentos jurídicos del activismo y la defensa se ha desarrollado para proteger los derechos humanos. En otras palabras, se han integrado en los sistemas jurídicos de la gran mayoría de los Estados.

En consecuencia al intervencionismo estatal para garantizar los derechos de segunda generación, subyace la tercera generación encaminada a salvaguardar los derechos de la solidaridad. Esta generación encuentra su auge a partir de la segunda mitad del siglo XX, donde se incentiva el progreso social y la calidad de vida de todos los pueblos.

Los derechos de tercera generación, son el resultado del reconocimiento de un nuevo contexto en el que surgen necesidades humanas particulares y donde las exigencias obligan a desarrollar nuevos derechos que garanticen el acceso universal a formas más avanzadas de ciudadanía y civilidad, de libertad y de calidad de vida.

Más aun, son indicios claros que el mundo cambió drásticamente en la última mitad del siglo XX. Transformación que es perceptible en nuestros días y que tiende a continuar. Está revolución se hace latente con mayor claridad en el uso de las nuevas tecnologías, vislumbrándose así el nacimiento de una cuarta generación de derechos humanos, en los que la universalización del acceso a la tecnología, la libertad de expresión en la web y la libre distribución de la información juegan un papel fundamental y son elementos esenciales para su definición.

Gracias al desarrollo generacional de los derechos y a su incorporación en el sistema jurídico internacional, hemos podido alcanzar la difusión global de los derechos humanos. Por lo tanto, hoy se da por sentado que corresponde al Estado y a la sociedad en su conjunto, el deber de proteger a cada individuo y garantizar el respeto irrestricto a los derechos humanos en su conjunto.

Evolución de los derechos del niño

En lo que respecta a la protección del niño en particular, esta idea no es añeja, en tanto que es a finales del siglo XX cuando se reconoce a éste como sujeto de derechos. Aunado al hecho que, es en tiempos relativamente recientes que evoluciona la sociedad de la información y se precisa la protección del niño en este ámbito.

En 1945, la Carta de las Naciones Unidas estableció las bases de la Convención sobre los Derechos de los Niños -en adelante, la Convención- al exhortar a todos los países a promover y alentar el respeto por los derechos humanos y las libertades fundamentales para todos. Posteriormente, con la aprobación de la Declaración Universal de Derechos Humanos se reforzó la idea del respeto a los derechos de la infancia.

La segunda Declaración de los Derechos del Niño, adoptada en 1959, consagra algunos principios de fundamental importancia en esta materia. En particular, el derecho del niño a una protección especial se vincula con el concepto del desarrollo integral del niño, de su libertad y de su dignidad (v. Principio 2).

Posteriormente, con la Declaración de los Derechos del Niño y la consiguiente Convención, se establecen los derechos y obligaciones para asegurar el respeto irrestricto de la infancia.6 Este último es reconocido como el instrumento internacional por excelencia para la protección de la infancia.

La Convención es el tratado internacional que ha sido más ampliamente ratificado en la historia de las Naciones Unidas. Ha sido ratificada por 192 países desde que la Asamblea General de las Naciones Unidas la aprobó de manera unánime en noviembre de 1989.7 Si bien, es una Convención articulada ad hoc para la protección de la niñez - pues se concluyó que los menores de 18 años precisan de cuidados y protección especiales-,8 también es cierto que, está fundamentada en otros instrumentos internacionales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales.9 De tal forma que la normatividad internacional sobre derechos humanos contempla dentro del término niño tanto a las niñas y niños como a los adolescentes.

Es de hacer notar que el Preámbulo de la Convención reitera una frase contenida en el Preámbulo de la Declaración de 1959, que reza a la letra: "el niño, por su falta de madurez física y mental, necesita protección y cuidado especiales, incluso la debida protección legal […]".10

La Convención además de estar fundamentada en la Declaración de 1959 y otros instrumentos internacionales ya mencionados, está basada en diversos sistemas jurídicos y tradiciones culturales, además se compone de normas y obligaciones. Estas normas básicas -denominadas también derechos humanos- establecen derechos y libertades mínimas que los gobiernos deben cumplir y, se basan en el respeto a la dignidad y el valor de cada individuo, independientemente de su raza, color, género, idioma, religión, opiniones, orígenes, riqueza, nacimiento o capacidad.11

Cabe mencionar que la Convención es el primer instrumento jurídicamente vinculante que incorpora toda la gama de derechos humanos: civiles, culturales, económicos, políticos y sociales. En 54 artículos y dos Protocolos Facultativos,12 se definen los derechos básicos que deberán disfrutar todos los niños y niñas inherentes a su dignidad humana y desarrollo armonioso. De tal forma que, la Convención es un documento moderno que refleja una nueva visión sobre la infancia, como seres humanos y titulares de sus propios derechos.13

Al ser un instrumento internacional ratificado por los Estados, éstos se comprometen a cumplir con un código de obligaciones vinculantes a favor de la infancia. Al aceptar

las obligaciones -mediante su ratificación o adhesión-, los gobiernos se comprometen a proteger y asegurar los derechos de la infancia y aceptan que se les considere responsables de este compromiso ante la comunidad internacional. En consecuencia, los Estados parte de la Convención están obligados a llevar a cabo todas las medidas y políticas necesarias para proteger el interés superior del niño y,14 son vigilados por el Comité de Derechos del Niño -órgano de expertos independientes que supervisa la aplicación de la Convención y los dos Protocolos, por sus Estados partes-.

En este tenor, es la sociedad en su conjunto quien debe asegurar su cumplimiento como una obligación jurídica, un imperativo moral y una prioridad en materia de desarrollo. Se entiende que es labor del Estado, la sociedad y la familia -cada uno en su ámbito de competencia- hacer cumplir las disposiciones estipuladas en la Convención. Las normas y los principios que se articulan en la Convención solamente pueden convertirse en realidad cuando sean respetados por todos, en la familia, en las escuelas y en otras instituciones que proporcionan servicios a la niñez, en las comunidades y en todos los niveles de la administración pública.

La Convención ofrece una visión del niño como individuo y como miembro de una familia y una comunidad, con derechos y responsabilidades apropiadas para su edad y etapa de desarrollo.

A este respecto, vale la pena mencionar que según la Convención, son los padres quienes tienen la responsabilidad primordial tanto de la crianza de sus hijos como de la satisfacción de las necesidades que permitan su sano desarrollo.15 En la medida en que los padres, no estén en condiciones de cumplir con estas responsabilidades por sus propios medios, el Estado tiene el deber de apoyarlos –v. arts. 18.2 y 27.3-. Esta relación de co-garantes es reafirmada por el artículo 3.2. que establece a la letra lo siguiente:

> "2. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con este fin, tomarán todas las medidas legislativas y administrativas adecuadas".

De tal forma que, en la medida que los padres no cumplan sus obligaciones a cabalidad, las autoridades tienen el derecho y el deber de intervenir para proteger los derechos del niño. En lo posible, la intervención consistirá en dar a los padres la orientación y el apoyo necesarios para superar los problemas que afectan la forma como cumplen estos deberes.

En este sentido, la Convención prevé disposiciones que abarcan derechos y libertades civiles, el entorno familiar, la salud básica y el bienestar, la educación, recreación, las actividades culturales y las medidas especiales necesarias para su protección.

En lo relativo a los derechos, la Convención establece principios fundamentales como

la no discriminación, el derecho a la supervivencia, al desarrollo y la opinión del niño. Asimismo, establece como principio básico contemplar en todo momento el interés superior del niño como consideración primordial en todas las medidas y decisiones que le atañen, y debe utilizarse para resolver cualquier confusión entre los diferentes derechos.

En particular, tomar en consideración los puntos de vista de los niños y las niñas se refiere a la importancia de escuchar y respetar su opinión en todas las cuestiones relacionadas con sus derechos. De ahí que la Convención ha exhortado a los países a promover una participación activa, libre y significativa de la infancia en las deliberaciones para tomar decisiones que les afecten.

Cabe destacar, para efectos del presente análisis, el artículo 16 de la Convención establece el derecho y obligación a la protección del niño, por ministerio de ley, y a letra dispone lo siguiente:

> "1. Ningún niño 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 a su reputación.
>
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".16

Por otra parte, la participación de la niñez constituye un aspecto con grandes potenciales en el vasto derecho de la infancia. También en esta área la Convención ha incorporado las bases para una profunda transformación cultural, introduciendo el principio de la autonomía progresiva de la infancia, tal como se consagra en el artículo 12.17

Asimismo, en el artículo 19 se establece la obligación del Estado a proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo custodia de los padres. A la letra señala lo siguiente:

> "1. Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo.
>
> 2. Esas medidas de protección deberían comprender, según corresponda, procedimientos eficaces para el establecimiento de programas sociales con objeto de proporcionar la asistencia necesaria al niño y a quienes cuidan de él, así como para otras formas de prevención y para la identificación, notificación, remisión a una institución, investigación, tratamiento y observación ulterior de los casos antes descritos de malos tratos al niño y, según corresponda, la intervención judicial".18

Por su parte, en el marco interamericano sobresalen el Pacto Interamericano de Derechos Civiles y Políticos y la Convención Americana, que reconocen el derecho del niño a "las medidas de protección que su condición de menor requiere". Si bien, la normativa interamericana no contempla una definición explícita del niño, el artículo 4.1. de la Convención Americana precisa que el derecho a la vida "estará protegido por la ley y, en general, a partir del momento de la concepción".19 Asimismo, en el artículo 19 relativo a los derechos del niño, se lee:

> "Todo niño tiene derecho a las medidas de protección que su condición de menor requieren por parte de su familia, de la sociedad y del Estado".20

Esto es, la Convención Americana sigue lo establecido en la Convención al establecer que los niños y niñas necesitan protección especial precisamente por ser niños, y por lo tanto dependientes y potencialmente vulnerables.

Ahora bien, resulta pertinente señalar que pese a ser un tratado vinculante para los países que lo han ratificado, la Convención es un instrumento legal relativamente joven y en proceso de implementación en todos los Estados miembros.

De tal forma que, veinte años después de la aprobación de la Convención puede afirmarse que su implementación en América Latina continúa siendo un proceso dinámico y continúo no solo en su relación con las reformas legales y modelos institucionales, sino también respecto a cualquier situación nueva que pueda afectar directa o indirectamente la vida o libre desarrollo de los niños, niñas y adolescentes –tal es el caso de las tecnologías del conocimiento y la información-.

Un nuevo derecho fundamental: la protección de datos personales

Una vez que se ha abordado la evolución de los derechos humanos, conviene puntualizar que el derecho a la protección de datos personales como se concibe en la actualidad, también deviene de una transformación, desde la concepción del derecho a la vida privada y la intimidad, hasta la conformación de un nuevo derecho fundamental dotado de caracteres propios, que otorgan a la persona un haz de facultades concretas. Por tanto, se trata en sí mismo de un derecho activo.21

Diversos instrumentos internacionales reconocieron el derecho de toda persona a no ser objeto de injerencias en su vida privada o familiar.22 Aunado al desarrollo normativo y los avances científicos y tecnológicos, surge en Europa el germen y acuñación del derecho a la protección de datos como se desarrolla en líneas subsiguientes.

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos

de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los "derechos humanos y nuevos logros científicos y técnicos".23

En un momento posterior, surgen diversas leyes nacionales alrededor de Europa. De tal forma que en 1977 era aprobada la Ley de Protección de Datos de la República Federal Alemana, mucho más ambiciosa que su predecesora del Land de Hesse. En 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979).24

Hacia la década de los años ochenta -cuando comienzan a utilizarse las primeras computadoras personales o PC´s surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal -en adelante, el Convenio 108-.25

De modo que, existen diversos instrumentos internacionales que dan fundamento al derecho a la protección de datos personales entre los que destacan los que se desarrollan brevemente a continuación.

Directrices de la Organización para la Cooperación y el Desarrollo Económico

La recomendación de la Organización para la Cooperación y el Desarrollo Económico -OCDE- en la que se contienen las "Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales" -en adelante, directrices de la OCDE-,26 fue adoptada el 23 de septiembre de 1980, y constituye el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.27

Estas Directrices se emiten partiendo de una realidad innegable que la OCDE vislumbró y que se traduce en tres problemáticas centrales, a saber:

El uso de la tecnología para el tratamiento de datos personales, las posibilidades bastantemente extendidas de almacenamiento, contrastación, vinculación, selección y acceso a los mismo que en combinación con la informática y la tecnología de telecomunicaciones, pueden poner los datos personales simultáneamente a disposición de miles

de usuarios en lugares geográficamente dispersos y la creación de redes complejas de datos nacionales e internacionales.

El peligro que representa las disparidades en las legislaciones nacionales tendentes a conciliar la protección de la información de carácter personal con la transmisión de enormes cantidades de datos a través de las fronteras nacionales, a fin de impedir vulneraciones a los derechos fundamentales de los titulares de esa información como el almacenamiento ilícito de datos personales o el abuso o la revelación no autorizada de los mismos.

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

Su adopción se fundamenta en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos.28

Las directrices de la OCDE se componen de 5 secciones fundamentales. En la primera parte, se establecen las definiciones aplicables, la parte segunda señala los principios básicos relativos al tratamiento de los datos personales. Por su parte, la tercera sección está dedicada a las transferencias internacionales de datos y la cuarta trata, en términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores. Finalmente, la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembros.

De manera específica, el Capítulo II de dichas directrices señala los siguientes principios básicos en materia de protección de datos personales:

"Principio de limitación de la recogida

7. Debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

Principio de calidad de los datos

8. Los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.

Principio de especificación de la finalidad

9. Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.

Principio de limitación de uso

10. Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de

otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo:
a) con el consentimiento del sujeto de los datos, o
b) por imperativo legal.
Principio de salvaguardas de seguridad
11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.
Principio de apertura
12. Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.
Principio de participación individual
13. La persona debería tener derecho a:
a) recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma;
b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;
c) que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, y
d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.
Principio de responsabilidad
14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba".

En resumen, la OCDE con la emisión de estas Directrices intenta equilibrar dos valores básicos fundamentales, a saber: la protección de los datos personales y la libre circulación de estos mismos a nivel internacional.

Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal

El Convenio 108 es creado con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades.29 Entró en vigor el 1 de octubre de 1985, en particular para proteger el derecho a la vida privada frente a los tratamientos

de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los Estados.

De esta forma el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

En términos del artículo 1, el objeto y fin del Convenio 108 es garantizar, en el territorio de cada Estado Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

En cuanto a su ámbito de aplicación, el Convenio 108 se aplica, en general a los tratamientos automatizados de datos de personas físicas, sin perjuicio de lo cual los Estados miembros podrán aplicar el Convenio a los datos de personas jurídicas y a los tratamientos manuales de datos, aunque tal circunstancia no se imponga obligatoriamente en el Convenio.

El artículo 5 establece los principios rectores que trazan el tratamiento automatizado de los datos de carácter personal:

Tratamiento leal y legítimo.

Principio de finalidad: los datos personales deben ser tratados únicamente para finalidades determinadas y legítimas y no utilizados de una forma incompatible con dichas finalidades.

Principio de proporcionalidad: los datos deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

Principio de calidad: los datos personales deben ser exactos (puestos al día).

Conservación de datos: la información de carácter personal debe ser conservada de tal forma que permita la identificación de los titulares durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Es importante mencionar que la firma del Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto se debió esencialmente a la naturaleza del Convenio, en virtud de que el mismo, a pesar de tener una naturaleza vinculante, establecía únicamente unos principios mínimos, permitiendo que, posteriormente, fueran los Estados firmantes los que los desarrollaran. Por este motivo se ha mantenido de forma unánime que el punto más débil del Convenio 108 fue, y sigue siendo, su aplicación. Es decir, se deja que sean los Estados miembros los que apliquen y desarrollen los principios contenidos en el Convenio y, de la misma forma, se les da libertad para aplicar las excepciones a los mismos.30

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

La Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas del 14 de diciembre de 1990,31 contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial. Se mencionan, entre otros, los principios de licitud, exactitud, finalidad, acceso y no discriminación.

Los principios consignados en la Resolución 45/95 deben ser aplicables a todos los archivos informatizados públicos y privados, pudiendo extenderse dicha aplicación a los archivos manuales y a las personas jurídicas que contengan alguna información relativa a personas físicas, mediante la expedición de disposiciones especiales.32

Ahora bien, la lista básica de principios reconocidos por esta Resolución son:

Principio de legalidad y lealtad: la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales.

Principio de exactitud: las personas responsables de la compilación de archivos o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible.

Principio de especificación de la finalidad: la finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada.

Principio de acceso de la persona interesada: cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.

Principio de no discriminación: sin perjuicio de los casos susceptibles de excepción, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

Principio de seguridad: deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, pérdida o destrucción accidental, como peligros humanos que se traducen en acceso no autorizado, uso fraudulento de los datos o la contaminación mediante virus informáticos.

Autoridad garante: el derecho de cada país debe designar a una autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la ob-

servancia de los principios establecidos. Esta autoridad deber ser imparcial, independiente frente a las personas o agencias responsables de procesar y establecer los datos y con competencia técnica.

Transferencias internacionales: debe existir un flujo libre de datos personales entre los Estados en el cual se establezcan garantías suficientes de protección a la vida privada.

Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

La Directiva 95/46, fue aprobada con un doble objetivo: por un lado garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado, impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.33

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizaron, dado que diversos estados consideraron que no era posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.34

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido a la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.35 En ese sentido, la directiva resultaba indispensable para la consecución de mercado único.

Finalmente, la Directiva 95/46 fue aprobada el 24 de octubre de 1995. Con base en esta directiva, los Estados miembros de la Unión Europea han transpuesto en sus normas nacionales los principios que regulan un derecho fundamental sin entorpecer el flujo de información.

Citando a Puente Escobar,36 las innovaciones introducidas por la Directiva 95/46/CE pueden esquematizarse de la siguiente manera:

La ampliación del ámbito de aplicación.

La regulación del encargado del tratamiento

El desarrollo de los principios de calidad.

El "interés legítimo" como legitimador del tratamiento.
La cláusula sobre la libertad de expresión.
El reconocimiento del derecho de oposición.
El reconocimiento de los derechos relacionados con las decisiones individuales automatizadas.
El desarrollo de sistemas de autorregulación sectorial.
El régimen sistemático de las transferencias internacionales de datos.
El reforzamiento de las funciones de las autoridades de protección de datos.
La creación del Grupo del Artículo 29.

En materia de principios, la Directiva 95/46/CE dispone en el artículo 6 lo que a continuación se indica:

"Artículo 6.-

1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos....

Carta de Derechos Fundamentales de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea,37 fue aprobada el 7 de diciembre de 2000 por la Cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza, Francia. Reconoce entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8 al establecer que toda persona tiene

derecho a la protección de los datos de carácter personal que le conciernan, sin hacer mención a la intimidad o a la vida privada. También el artículo 8 señala que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

De esta forma, a partir de la aprobación de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y autónomo del derecho a la intimidad y a la privacidad de las personas. Cabe precisar a este respecto, que en su artículo 7 aborda los derechos de manera separada, recoge el derecho a la vida privada y familiar.38

Ahora bien, cabe mencionar que paralelamente ha habido un rico desarrollo jurisprudencial que por razones de espacio no se desarrollará exhaustivamente, sin embargo, es importante señalar en concreto el caso particular del Tribunal Constitucional Español, el cual arrojó luz sobre el contenido y alcances del derecho a la protección de datos personales en su sentencia 292 del 30 de noviembre de 2000,39 por la cual definió los contornos de este nuevo derecho al establecer a la letra lo siguiente:

> "7… [E]l contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular".

Sin afán de exhaustividad, los instrumentos internacionales aquí referidos dan forma y contenido al derecho de la protección de datos, al tiempo de sentar las bases para su reconocimiento y difusión en otras regiones del mundo.

La Carta de Derechos Fundamentales de la Unión Europea fue aprobada el 7 de diciembre de 2000 por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza, Francia. Reconoce entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8 al establecer que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, sin hacer mención a la intimidad o a la vida privada. También el artículo 8 señala que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

De esta forma, a partir de la aprobación de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y autónomo del derecho a la intimidad y a la privacidad de las per-

sonas. Cabe precisar a este respecto, que en su artículo 7 aborda los derechos de manera separada, recoge el derecho a la vida privada y familiar.

La protección de datos personales de niñas, niños y adolescentes

Como se ha venido desarrollando, a nivel internacional se han realizado valiosos esfuerzos por establecer reglas para el tratamiento e intercambio de información de las personas al tiempo que se respeta su privacidad. Ese equilibrio se ha podido plasmar en leyes que prevén los principios y derechos de los titulares de los datos, así como el diseño de instituciones que podrían denominarse como "órganos garantes" de la adecuada protección de datos, con independencia y facultades de sanción.

Empero, no existe un modelo único de regulación a este respecto. Por un lado, contamos con el modelo europeo, que podría denominarse como universal al ser comprehensivo para la protección de los datos personales (ya que prevé los principios, derechos, procedimientos y autoridad independiente) el cual ha sido adoptado con matices e innovaciones importantes por países como Canadá. Por otra parte, existen modelos sectoriales en los que conviven algunas regulaciones específicas y mecanismos de autorregulación. En este último grupo podríamos ubicar a los Estados Unidos de América y al propio México.40

Es importante mencionar que en el ámbito europeo, así como en Canadá, las autoridades en materia de protección de datos han promovido intensamente el derecho a la protección de datos de menores a través de campañas de sensibilización dirigidas a padres y educadores, folletos informativos, creación de sitios en Internet de autoayuda, concursos, entre otros mecanismos para fomentar el conocimiento y alcances de este derecho fundamental.

Hay que recordar que la definición de dato personal adoptada de manera quasi generalizada en el ámbito internacional, señala que se trata de información relativa o concerniente a una persona física, identificada o identificable. En ese sentido, el ámbito de protección es hacia la persona en relación con el tratamiento que se dé a su información, la cual se puede encontrar en posesión de los gobiernos o de los particulares.

Por lo anterior, puede decirse válidamente que las niñas, niños y adolescentes gozan, en tanto que son personas, del derecho a la protección de sus datos personales, el cual se traduce en la debida observancia de una serie de principios y derechos, tutelados a través de un procedimiento, ante una autoridad independiente como se verá en el siguiente apartado.

La falta de dicha observancia ha traído consigo no solo la violación del derecho de protección de datos personales, sino implicaciones en el desarrollo social, psicológico y emocional de muchos de los menores. Existen innumerables casos ilustrativos de las consecuencias de dicha carencia, que por razones de espacio no podemos exponer, sin embargo, se describen cuatro casos ilustrativos y recientes al final del documento para

mayor referencia.

La propuesta del Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes

Ahora toca el turno de explicar las distintas propuestas del Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, mejor conocido como Memorándum de Montevideo –en adelante, el Memorándum -, para lograr la efectiva protección de los datos personales de las niñas, niños y adolescentes, en éste ámbito.

Hasta este punto, cabe destacar que el servicio de redes sociales ha sido definido por el Grupo de Trabajo de Protección de Datos (Artículo 29), como las "plataformas de comunicación en línea que facilitan a los individuos a crear o unirse a una red con usuarios de ideología afín. En el sentido legal, las redes sociales son servicios sociales de información, como se definen en el artículo 1, párrafo 2 de la Directiva 98/34/EC y reformada por la Directiva 98/48/EC".41

Ahora bien, el objeto de la elaboración del Memorándum nace del reconocimiento de los riesgos a los que están sujetos los menores al momento de navegar en Internet. Los niños, niñas y adolescentes conciben el espacio virtual como un espacio privado, con la posibilidad de actuar y expresarse libremente sin estar plenamente conscientes sobre el control de su información y las implicaciones existentes. Esto genera "bienestar físico y psicológico, así como espiritual" como se ha demostrado desde la psicología".42

Más claro, el derecho a la protección de datos personales y la privacidad de los menores se traduce en la no injerencia, el respeto a su dignidad e identidad como personas. Si bien es cierto, el avance tecnológico y la vinculación de los menores con las nuevas tecnologías representa un elemento del proceso evolutivo de la sociedad, también es cierto que este nuevo espacio debe ser regulado para proteger los derechos de la niñez en todos sus ámbitos. Mismos, que al no ser garantizados tendrían implicaciones en su desarrollo y en la estigmatización social consiguiente.43

Por lo que hace a las redes sociales, el uso que de ellas hacen los niños, niñas y adolescentes y los abusos a los que podrían ser sujetos, a continuación se abordan las secciones medulares en referencia a la protección de datos y la responsabilidad del Estado y de la Industria. Si bien, el Memorándum aborda diferentes aristas de la problemática, en las secciones sucesivas se analizan respecto de la aplicación al derecho fundamental de la protección de datos personales y las implicaciones en la vida presente y futuro de los menores.44

Recomendaciones para los Estados sobre el marco legal

A este respecto, cabe destacar el numeral 6 denominado "Recomendaciones para los Estados sobre el marco legal" que a la letra establece lo siguiente:

"6. La protección de los datos personales requiere del desarrollo de una normativa nacional, aplicable al sector público y privado, que contenga los derechos y principios básicos, reconocidos internacionalmente, y los mecanismos para la aplicación efectiva de la misma. Los Estados deberán tomar en especial consideración, en la creación y en el desarrollo de dichas normativas, a las niñas, niños y adolescentes".

La mención anterior tiene varias implicaciones relativas a la protección de los datos personales de los menores. La primera es que los Estados que utilicen como principios orientadores el Memorándum de Montevideo a la hora de legislar en materia de protección de datos personales deberán contemplar, entre otros los aspectos que se señalan a continuación.

En principio, el ámbito de aplicación de la norma debiera ser para entes públicos -el Estado en todos sus niveles de gobierno- así como para entes privados. La emisión de una ley de protección de datos brindaría la garantía a toda persona -incluidos los menores de edad- de que su información será manejada conforme a lo que establezca esta ley, por lo que si bien, el Memorándum se enfoca a la protección de menores de edad, se recomienda la expedición de una norma de aplicación general, dado que los principios y derechos que se desarrollan en los siguientes párrafos, también son transversalmente aplicables sin distingo de edad, aunque explicaremos las variaciones en su ejercicio al caso concreto.

Una novedad del Memorándum es la recomendación al legislador de tomar en cuenta en el proceso legislativo y de diseño de la norma, la opinión de las niñas, niños y adolescentes, sobre todo, en aquellas disposiciones particulares que se refieran a la forma en que debe llevarse a cabo el tratamiento de su información en Internet, de modo que ellos puedan aportar su opinión.

Los principios de protección de datos

En cuanto a los principios de protección de datos, existe un consenso más o menos generalizado a nivel internacional en reconocer los siguientes:

Consentimiento;
Información;
Finalidad;
Proporcionalidad;
Calidad y
Seguridad

Es importante mencionar que como premisa principal el proveedor de toda red social

digital debiera comprometerse al tratamiento leal de los datos que no se traduce en otra cosa sino en el hecho de efectuarlo con estricto apego y respeto a los derechos del titular de la información.

Por ello, el consentimiento es el principio rector del derecho a la protección de datos personales dado que se trata del poder de disposición del titular de la información para decidir quién, cómo, cuándo y para qué utiliza sus datos, pudiendo oponerse a dicha utilización.

Aquí hay un punto importante a dilucidar y es el tema de la edad ya que no existe consenso acerca de a partir de qué edad se considera que un niño es maduro para poder ejercer su consentimiento y por tanto, manifestar su voluntad para otorgar su información personal. Dicha cuestión dependerá de la legislación que adopte cada país y de conformidad a ello, se establecerían las modalidades para expresar el consentimiento.

Ahora bien, otra complejidad se presenta a la hora de comprobar por parte de la industria, que realmente se obtuvo el consentimiento de un menor con la edad establecida por ley. Ello implica el desarrollo de mecanismos para conocer de manera fehaciente, la madurez del titular del dato.

En cuanto al principio de información, este se traduce en la obligación del proveedor de una red social digital de dar a conocer las reglas de privacidad con que cuentan, los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, así como el nombre del responsable de su tratamiento. También se conoce como el principio de la transparencia en el tratamiento de la información ya que se está utilizando información ajena y por tanto, debe ventilarse de qué manera se hará uso de la misma y bajo qué condiciones podrá el titular de los datos, ejercer los derechos a que se refiere el próximo apartado.

Veamos ahora el principio de finalidad que consiste en que los datos se recaban para cierto objeto concreto y conocido de antemano. Si la finalidad cambia, es necesario obtener el consentimiento del titular para poder utilizar los datos para nuevos objetivos.

Por su parte, el principio de proporcionalidad se traduce en que al tener el tratamiento una finalidad concreta, los datos que se recaben deberán ser directamente proporcionales a dicho fin, por lo que este principio indica que debe darse un tratamiento mínimo a la información, ya que en la medida que se obtenga más, podría rebasarse el fin primario. A este principio también se le conoce como principio de minimización del tratamiento de datos.

En lo que respecta al principio de calidad de los datos, éste consiste en mantenerlos actualizados y puestos al día de modo que reflejen verazmente la información acerca de una persona. Un dato inexacto es un dato falso y no rectificarlo podría acarrear consecuencias nefastas.

Finalmente, los datos deben estar seguros, es decir, íntegros y accesibles sólo para aquellos que estén autorizados para ello, como se verá más adelante.

Los derechos de las niñas, niños y adolescentes en materia de protección de datos

Por lo que ve a los derechos del titular de los datos, también hay coincidencia internacional en reconocer los siguientes:

Acceso;
Rectificación;
Cancelación, y
Oposición.

Para saber cómo se despliegan los derechos de las niñas, niños y adolescentes a la protección de sus datos personales, el Memorándum en el apartado denominado "Recomendaciones para los Estados sobre el marco legal" en su numeral 8 establece lo siguiente:

> "8. Los Estados deben legislar el derecho que tienen las niñas, niños y adolescentes directamente o por medio de sus representantes legales, a solicitar el acceso a la información que sobre sí mismos se encuentra en bases de datos tanto públicas como privadas, a la rectificación o cancelación de dicha información cuando resulte procedente, así como a la oposición a su uso para cualquier fin".

De acuerdo con dicho numeral, queda claro que los menores de edad podrían solicitar acceso a la información personal que de ellos se conserve, manipule y transmita en las redes sociales. Este derecho se relaciona directamente con el principio de información, ya que solo mediante un aviso de privacidad en el que se establezca la persona responsable del tratamiento de los datos, así como los derechos que tiene el titular de la información, los menores de edad podrán conocer qué información se detenta de ellos.

También deben poder solicitar la rectificación de datos erróneos o desactualizados para su puesta al día. Este derecho se relaciona directamente con el principio de calidad a que se hizo referencia en el apartado anterior. Finalmente, podría pedirse la cancelación del dato que trae como consecuencia la supresión o eliminación de dicha información. Cabe mencionar que en este punto es importante establecer mecanismos efectivos de supresión total de la información, porque en ocasiones se solicita eliminar una invitación a formar parte de una red social y esta sigue apareciendo ad infinitum, sin que sea respetada la voluntad del interesado o titular del dato.

El derecho de oposición también debe poder ejercitarse cuando los datos se hayan obtenido sin el consentimiento de los menores de edad (por encontrarse en fuentes de acceso público por ejemplo) y en este caso, la consecuencia sería la cancelación del dato.

El procedimiento de tutela y autoridad independiente

Pasando a otro tema nodal del Memorándum, vale la pena resaltar la mención especial que hace a los "mecanismos para la aplicación efectiva de la norma". Esta cuestión se refiere a la necesidad de que en los marcos normativos correspondientes se prevea un procedimiento de tutela de derechos de protección de datos; dicho procedimiento debiera ser efectivo, expedito y gratuito, además de poder desahogarse ante una autoridad independiente.

La autoridad no necesariamente tendría que ser –aunque idealmente sí- una autoridad especializada en protección de datos personales. Dicha tarea bien podrían llevarse a cabo por las defensorías del pueblo o comisiones de derechos humanos, las procuradurías o los jueces. Por ello, resulta relevante que el procedimiento sea expedito y claro para no hacer nugatorio el derecho.

Recomendaciones para la Industria en materia de protección de datos

Las recomendaciones concretas del Memorándum a la industria establece que las empresas que proveen los servicios de acceso a Internet, aquellas que desarrollan las redes sociales digitales, o bien, las aplicaciones que éstas contienen, deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada —en particular de niñas, niños y adolescentes—, a cooperar con los sistemas de justicia nacionales, desarrollar campañas de prevención y desarrollo de capacidades, entre otros instrumentos mediante compromisos o códigos de conducta, que deben incluir:

> " 19. No permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento.

También se señala que en el caso de niñas y niños se deberá considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara".

Dado que en varios países ya existe la obligación para la industria de establecer controles para limitar la información que las niñas y niños proporcionan en Internet, de igual forma, el Memorándum señala de manera contundente que la industria deberá considerar la prohibición de llevar a cabo el tratamiento de datos de niñas y niños, con lo cual se busca limitar la recolección y almacenamiento de información solo al caso de los adolescentes.45

Lo anterior tiene una lógica subyacente y es el hecho de que a partir de cierta edad, el ser humano comienza a ser consciente de su voluntad y de los efectos de sus actos u

omisiones. En la infancia, la inocencia e inmadurez de las niñas y niños los lleva a intercambiar toda la información que les sea solicitada acerca de sí mismos, así como de sus padres, hermanos y amigos, a cambio de conseguir puntos para ver a sus mascotas favoritas. Aquí tenemos una clara tensión entre el modelo de negocio de juegos para niños en redes sociales y los derechos de la niñez.

Conviene entonces recordar que el artículo 16 de la Convención sobre los derechos de los niños establece que no serán objeto de injerencias en su vida privada, por lo que la prohibición al tratamiento de sus datos no surge en el Memorándum, sino que más bien se retoma de los derechos del niño reconocidos en los instrumentos internacionales. En otras palabras, la actividad que actualmente lleva a cabo la industria al recabar información que los propios niños proporcionan en redes sociales, tiene claros vicios del consentimiento, por lo que podría ponerse en tela de juicio la licitud de dicha actividad.

Ahora bien, en el caso de los adolescentes, de acuerdo con las edades que cada país determine, éstos podrían proporcionar algunos de sus datos, siempre y cuando puedan conocer de manera clara las reglas del juego, el cual podría denominarse "intercambio de privacidad a cambio de diversión" como veremos más adelante.

Otras recomendaciones a la industria en materia de protección de datos, establecen lo siguiente:

> 20. Proteger la vida privada debería ser la característica general y por defecto en todas las redes sociales digitales, bases de datos y sistemas de comunicación, entre otros. Los cambios en el grado de privacidad de su perfil de usuario que se quieran realizar deben ser sencillos y sin costo alguno.
>
> 21. Las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes.
>
> Se deberá proveer información sobre los propósitos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a terceros. De igual modo se deberá indicar la persona o personas responsables del tratamiento de la información.…

Esta mención es importante, ya que dicha recomendación se traduce en la obligación de la industria de proveer los llamados avisos de privacidad para dar cumplimiento al principio de información antes abordado. En ese sentido, el aviso deberá transmitir de forma clara y sencilla las reglas sobre privacidad, los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, así como el nombre del responsable de su tratamiento, dado que si no se le puede identificar claramente, tampoco podrían ejercitarse los derechos de acceso, rectificación, cancelación u oposición. A mayor abundamiento, el Memorándum establece lo siguiente:

Se debe igualmente ofrecer un enlace hacia los "parámetros de privacidad" en el momento de la inscripción, conteniendo una explicación clara sobre el objeto de dichos parámetros.

Debe hacerse accesible igualmente un aviso sobre el hecho de que la red social ha preseleccionado los parámetros, si éste es el caso, y que pueden ser cambiados en todo momento, según las preferencias de las niñas, niños y adolescentes.

Sería deseable igualmente que se cambien los "parámetros por defecto" de los contenidos personales, para que puedan ser únicamente accesibles por los amigos y las redes que el usuario determine.

22. Toda red social digital debe indicar explícitamente en la parte relativa a la "publicidad" contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.

23. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital.

Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria.

La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.

24. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley.

Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable. Asimismo se deberá eliminar la información de no usuarios, considerando un límite razonable de conservación cuando han sido invitados a ser parte de las redes. Las redes sociales digitales no deben utilizar la información de no usuarios.

Las dos opciones que permitan desactivar y suprimir las cuentas deben ser totalmente visibles para los usuarios, que deben poder comprender qué supone cada opción en cuanto a la gestión por parte del servicio de los datos contenidos en dichas cuentas.

Se tiene que informar a los usuarios de las obligaciones de privacidad frente a terceros, dicha política debe ser explícita, clara y visible.

25. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos".

Uno de los aspectos que más han preocupado a las autoridades de protección de datos en el mundo, así como a otros actores importantes, es el hecho de que la información que se "sube" a las redes sociales se indexa a buscadores en Internet. Lo anterior significa que si la gente no está consciente de ello y no cuenta con la información necesaria ni los mecanismos para oponerse a esa acción, toda la información que considera que comparte únicamente con sus "amigos" en la red, también puede ser conocida y copiada por el resto de la gente que pueda tener acceso a buscadores comunes de información. Bastaría entonces con buscar el nombre de una niña, niño o adolescente, para que cualquier persona sin ser su "amigo" pueda saber todo lo que hace y quienes forman parte de su círculo social, además de otra información derivada.

Por ello, en el caso particular de las redes sociales digitales, se ha solicitado por autoridades como la Comisaria Europea para la Sociedad de la Información, que dichas redes garanticen que "al menos" las cuentas de los menores de edad sean "privadas por defecto e inaccesibles" a través de los buscadores de la red. Lo anterior busca la mayor protección de los menores al asegurar que no sean indexados sus datos en las herramientas para la búsqueda de información en Internet, impidiendo con ello seguir su rastro.46

En lo que respecta al acceso por parte de terceros, el Memorándum en cuestión dispone lo siguiente:

"26. Toda red social digital debe establecer las medidas necesarias para limitar el acceso por parte de los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros), a los datos personales de los usuarios cuando éstos no sean necesarios ni pertinentes para el funcionamiento de dichas aplicaciones.

La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas únicamente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación.

Es igualmente importante que se tomen las medidas necesarias para evitar toda comunicación de datos personales de aquellos usuarios que no han decidido expresamente por ellos mismos el instalar alguna aplicación".

De nuevo, el hilo se rompe por lo más delgado. De entrada, hay que reconocer que existe un interés claro de la industria en identificar a las personas con sus gustos, necesidades y hábitos de consumo, para que a partir de ello, puedan ofrecerles bienes o servicios ad-hoc. A esta actividad se le denomina behavioral targeting.

Sabido lo anterior, es necesario que el proveedor del la red social digital establezca medidas para que terceros desarrolladores de las aplicaciones que se ofrecen (como los juegos), estén limitados en cuanto al acceso a los datos personales de los usuarios, de lo contrario se tiene entonces a un sinnúmero de polizontes que aprovechan estos esquemas abiertos.

Por ello, se recomienda la programación de filtros especiales para que dichos terceros sólo puedan obtener aquella información que el titular ha consentido expresamente "compartir" y no toda aquella que se encuentra en su cuenta.

Finalmente, el Memorándum hace una mención relevante a la seguridad de la información que se vierte en las redes sociales, al señalar lo siguiente:

> 29. La industria debe establecer medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la integridad, disponibilidad y confidencialidad.

Queda claro con lo anterior que la observancia de los principios y derechos en materia de protección de datos personales no serviría de mucho, si no se prevén las medidas necesarias para impedir la pérdida, destrucción o acceso no autorizado de la información contenida en redes sociales, las cuales pueden llegar a conformar archivos inmensos con datos de millones de personas, que permiten la creación de perfiles detallados y complejos que mal utilizados, pueden provocar violaciones a otros derechos y libertades como ya se ha dicho. 47

Conclusiones

Como se desprende de la larga marcha que han emprendido los derechos humanos, al tiempo que evolucionó la ciencia y la tecnología surgió un nuevo derecho fundamental a la protección de datos personales y la necesidad de desplegar sus mecanismos de tutela, para la efectiva protección de las niñas, niños y adolescentes.

Es claro que la protección de los datos personales como un derecho fundamental y autónomo, contempla en su amplio espectro la salvaguarda de los menores, por el simple hecho de ser. Sin embargo, la realidad nos demuestra la urgente necesidad de comprometernos en todos los niveles para que no se irrumpa en ese ámbito, por demás delicado. La afectación en la vida presente y adulta de los niños, niñas y adolescentes no

solo pone en riesgo su integridad personal sino además su desarrollo en todas las esferas de su crecimiento. De ahí, la urgente necesidad de regular las nuevas tecnologías, que si bien nos acercan cada día más, no vienen exentas de peligros.

Si bien los Estados no han adoptado un modelo único para la tutela del derecho a la protección de datos, cuando se trata de proteger a la infancia, las cosas cambian. El ejemplo quizá más palpable sea el hecho de que en los Estados Unidos de América existe una ley para proteger la privacidad de los niños cuando navegan en Internet, sin que exista una ley marco en materia de protección de los datos personales de otros sectores de la población.48 Es por ello que dado que existe consenso en cuanto a la necesidad de proteger a los menores de edad en general en Internet y más recientemente en redes sociales, es necesario actuar para garantizar una tutela efectiva.

Existe la urgente necesidad de que los Estados comiencen a establecer mecanismos integrales de protección que arranquen con la expedición de normatividad en materia de protección de datos, pero que además de manera sistémica, se contemple la prevención a través del fomento educativo sobre los riesgos que enfrentan y las alternativas con que cuentan las niñas, niños y adolescentes al utilizar redes sociales digitales. Lo anterior también implicará necesariamente el involucramiento de los poderes judiciales, para que una vez que se han conculcado los derechos de los menores de edad, estos puedan ser resarcidos. Es un deber del Estado y una obligación democrática.

La confianza y la seguridad en la utilización del Internet y, en particular de las redes sociales, son aspectos fundamentales en la construcción de una sociedad mundial de información segura y abierta a todos. Ello urge la inmediata cooperación internacional y de abordar la ciber-seguridad de forma holística, resolviendo cuestiones jurídicas, técnicas, orgánicas y procedimentales.

De igual forma, la protección de la infancia en el ámbito tecnológico necesita de los padres. Las barreras tecnológicas instaladas en algunas páginas de Internet, como filtros o mecanismos de verificación de edad e identidad, no han sido suficientes para garantizar un uso seguro de la red a niños y adolescentes. Es necesaria la combinación de estas medidas técnicas con otros elementos, como la supervisión de los padres, la educación, el refuerzo de la ley y la puesta en marcha de políticas de seguridad entre los proveedores y las páginas que alojan redes sociales. La protección de los datos personales y de la integridad del niño demandan un esfuerzo conjunto.

Así como se establece en la Convención sobre los Derechos del Niño, los Estados deben tomar las medidas apropiadas para garantizar su protección y bienestar. La experiencia demuestra que el nivel de responsabilidad de un gobierno para implementar acciones concretas en este rubro, determina la importancia que se otorga a la conformación de sociedades futuras.

De ahí que la socialización del Memorándum de Montevideo, contribuye a los esfuerzos de la región encaminados a salvaguardar y proteger a las niñas, niños y adoles-

centes ante los cambios tecnológicos y las nuevas formas de vida. Más aun, coadyuva a la transformación cultural que comprende la construcción de la ciudadanía desde el mismo momento en que empieza la vida, y en la fase más importante de formación del ser humano: la infancia.

La protección de sus datos y vida privada en las redes sociales digitales es un paso más a favor de su desarrollo integral, y una obligación de cada Estado miembro. Imprescindible, por tanto, incluir en la agenda nacional el desarrollo de las políticas públicas en esta materia.

Referencias bibliográficas

Anaya Muñoz, Alejandro et.al. (2005) Glosario de términos básicos sobre derechos humanos, Comisión de Derechos Humanos del Distrito Federal, Universidad Iberoamericana Ciudad de México, México.

Arenas Ramiro, Mónica (2006). El derecho fundamental a la protección de datos personales en Europa, Tirant lo Blanch, Valencia, España.

Derecho Internacional de los Derechos Humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano (2004). Oficina de Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Bogotá, Colombia.

Caney, Simon y Peter Jones (eds.) (2001), Human Rights and Global Diversity, Frank Cass Publishers, London.

Friedman, Milton (1990), The Republic of choice. Law, Authority and Culture, Harvard University Press, Cambridge.

Jourard, S.M. (1966), "Some Psychological aspects of Privacy", Law and Contemporary Problems, Duke University School of Law, no. 31., Durham, NC.

Murillo de la Cueva, Pablo y José Luis Piñar Mañas (2009). El derecho a la autodeterminación informativa, Fundación Coloquio Jurídico Europeo, Madrid.

Newell, P.B. (1994), "A System of Model Privacy", Journal of environmental Psychology, Publisher Academic Press, no. 14., U.K.

Piñar Mañas, José Luis (2005), "El derecho fundamental a la protección de datos personales", Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.

----- (2008), ¿Existe la Privacidad?, CEU Ediciones, Madrid.

Oñate, Araceli e Iñaki Piñuel (2007), Mobbing Escolar, Ediciones CEAC, Madrid.

Puente Escobar, Agustín (2005), "Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal", Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.

Pupavac, Vannesa (1998), "The Infantilization of the South and the UN Convention on the Rights of the

Child", Human Rights Law Review, University of Nottingham, Centre for Human Rights, March, U.K.

Rodríguez Palop, María Eugenia (2002), La nueva generación de derechos humanos. Origen y justificación, Dykinson-Universidad Carlos III de Madrid, Madrid, España.

Vasak, Karel (1982), International Human Rights Vol. 1., Greenwood Press, San Francisco, EUA.

Vincent, R.J. (1999), Human Rights and International Relations, Cambridge University Press, Cambridge.

Sitios consultados en Internet

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. http://www2.ohchr.org/spanish/law/crc.htm

Carta de Derechos Fundamentales de la Unión Europea.
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/union_europea/common/pdfs/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf
Convención Americana sobre Derechos Humanos.
http://www.oas.org/Juridico/spanish/tratados/b-32.html

Convenio para la Protección de los Derechos y las Libertades Fundamentales.
http://www.acnur.org/biblioteca/pdf/1249.pdf

Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf
Children´s Online Privacy Protection Act, 1998.

http://www.ftc.gov/ogc/coppa1.htm

Preámbulo de la Declaración de los Derechos del Niño de 1959. Documento de Naciones Unidas A.G. res. 1386 (XIV), 14 U.N. GAOR Supp. (No. 16), p. 19, ONU Doc. A/4354 (1959). http://www.iin.oea.org/BADAJ2/pdf/Normativa%20ONU/Declaraci%C3%B3n%20de%20los%20Derechos%20del%20Ni%C3%B1o%201959.pdf

Declaración Universal de los Derechos del Hombre.
http://www.un.org/es/documents/udhr/

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos.
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

Documento de trabajo 1/08 sobre la protección de datos personales de los niños. Unión Europea.
https://212.170.242.196/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2008/common/menores_es.pdf

El Universal. Lunes 28 de septiembre de 2009. "Reclutadores de empleo buscan información en redes sociales".

http://www.eluniversal.com.mx/articulos/55885.html

Guidelines on Child Online Protection. Presentado en Unión Internacional de Telecomunicaciones el 5 de Octubre de 2009.
http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

Ley Federal de Transparencia y Acceso a la Información Pública (México).
http://www.ifai.org.mx/

Nota informativa publicada por la Agencia Española de Protección de Datos del 15 de octubre de 2009. Barómetro de septiembre de 2009 del CIS. "La AEPD destaca la alta desconfianza de los ciudadanos españoles en la seguridad de sus datos en Internet".
http://www.alfa-redi.org/noticias.shtml?x=11602

Opinión 5/2009 sobre redes sociales en línea del grupo de Trabajo de Protección de Datos de la Comisión Europea. http://ec.europea.eu/justice_home/fsj/privacy/index_en.htm

Página oficial de Internet de la Organización de Estados Americanos. http://www.oas.org/Juridico/spanish/tratados/b-32.html

Pacto Internacional de Derechos Civiles y Políticos.
http://www.cinu.org.mx/onu/documentos/pidcp.htm

Recomendaciones Derechos de niños y niñas deberes de los padres y madres 2008. España.
http://www.ftc.gov/ogc/coppa1.htm

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas.
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

Revista de derecho informático Alfa-Redi.
http://www.alfa-redi.org/rdi.shtml
http://www.alfa-redi.org/noticias.shtml?x=11602

Revista Informador.
http://www.informador.com.mx/tecnologia/2009/144861/6/filial-de-deutsche-telekom-pierde-datos-personales-de-clientes-estadounidenses.htm

Texto constitucional mexicano reformado en su artículo 16. http://www.diputados.gob.mx/LeyesBiblio/

Tribunal Constitucional de España. Sentencia 292 del 30 de noviembre de 2000. http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467

Casos ilusrativos

Algunos casos prácticos sobre el uso y abuso de las redes sociales para el acoso y explotación de menores, se exponen a continuación:

Caso 1: Una adolescente británica a la cárcel por bullying49 en Facebook.
País: Reino Unido de la Gran Bretaña (Worcester, Inglaterra).
Fecha: 24 de agosto de 2009.
Disponible en el vínculo: http://www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/

DG_070501
Exposición de caso.
Una adolescente de 18 años se ha convertido en la primera persona encarcelada en Gran Bretaña por hacer 'bullying' e intimidar a una compañera de instituto a través de una la red social.

Keeley Houghton había acosado a Emily Moore durante la etapa en la que acudieron juntas al colegio. Houghton se jactaba en su página de Facebook de que iba a matar a su compañera.

La joven inglesa fue condenada a tres meses de encierro en una institución para delincuentes juveniles, tras declararse culpable de acoso. Houghton también recibió una orden de restricción que impide acercarse a Emily Moore, ya sea por internet o por cualquier otro medio.
Observaciones
A este respecto, cabe destacar que el gobierno británico ha implementado la campaña "Laugh at it and you are part of it",50 que pretende generar consciencia sobre el ciberbullying y sus consecuencias sociales.

Caso 2: Viví un infierno, todo por ser buen estudiante
País: Colombia.
Fecha: 6 de septiembre de 2009.
Disponible en: http://www.eltiempo.com/archivo/documento/MAM-3606418
Exposición de caso.
El adolescente, que hoy tiene 13 años, estudiaba en un prestigioso colegio de Bogotá. Ingresó en cuarto de primaria. Sus padres lo matricularon allí porque el plantel donde estudiaba no era bilingüe.

"Venía de un colegio muy estricto -cuenta él-. Estaba acostumbrado a la disciplina, y muchas cosas que enseñaban, ya las sabía. Me la empezaron a montar de nerdo".

Y por eso, por ser estudioso y respetuoso, un par de compañeros empezaron a hacerle la vida imposible. Además de golpearlo e insultarlo a diario, lo excluían todo el tiempo. Lo dejaban solo a la hora del descanso, no le permitían jugar con ellos.

Todo se complicó cuando las agresiones trascendieron al escenario virtual. En el Messenger era costumbre que cada uno de los compañeros de curso pusiera, en su estado, un mensaje insultante hacia él. Hacían concursos de la mejor frase, y él las veía cuando se conectaba.

Todo el tiempo recibía mensajes en su correo electrónico y en su celular. El adolescente, narró: "Empecé a tener pensamientos malos, a perder las ganas de vivir. Quise morirme, no quería ser el rechazado del curso".
Tal fue la presión que, según su médico de cabecera, sufrió un bloqueo de la hormona del crecimiento

Caso 3: Ciberbullying: Cuatro adolescentes demandados por crear un perfil falso en Facebook.
País: Estados Unidos de América
Fecha: 29 de septiembre de 2009.
Liga disponible: http://cyberbullying.us/blog/lori-drew-officially-acquitted.html
http://arstechnica.com/tech-policy/news/2009/09/that-obscene-racist-may-be-fake-4-sued-for-profile-prank.ars
Exposición de caso.
Cuatro adolescentes han sido acusados por crear un perfil falso de un compañero en Facebook, presentándolo como racista y sexualmente obsceno, y en continua búsqueda de nuevos amigos para expandir su red social. El perfil fue suficientemente creíble para hacerse de 580 amigos. Al respecto, la madre del adolescente

ha puesto una demanda en contra de los cuatro adolescentes, acusándolos de difamación y por causar stress emocional severo a su hijo.

Aparentemente, los cuatro estudiantes difamaron el nombre de un compañero, usando fotografías y registrando información real en sus datos de contacto, como su número celular. Asimismo, el grupo también expuso numerosas frases obscenas, racistas y sexuales.

El grupo, en nombre del adolescente, efectuaba comentarios denigrantes en contra de los demás miembros asociados en su página. Lo que resultó en un severo desgaste emocional, implicaciones para sus familiares –al tener que cambiar de club social, transporte escolar, etc.-, gastos económicos, entre otros.
La demanda fue hecha ante la Corte de Illinois y busca además del castigo, compensar los daños.

Caso 4.
País: España (Cádiz).
Fecha: 15 de junio de 2009.
Disponible en: http://www.elpais.com/articulo/sociedad/ciberamigo/chantajea/elpepisoc/20090615elpepisoc_5/Tes
Mi ¨ciberamigo¨ me chantajeaba. Ingresa en prisión un joven que acosó desde Cádiz a más de 250 mujeres, muchas de ellas menos, a través de la red.
Exposición de caso.
El detenido en Chipiona (Cádiz) era, en realidad, varón y tenía 24 años pero se había inventado hasta 12 personalidades distintas para ganarse la confianza de sus víctimas de diferentes maneras. Durante semanas habló con ellas a través de Internet. Se intercambiaron palabras en el chat, mensajes por correo y fotografías en algunas redes sociales como Facebook.

Cuando la amistad se consolidaba y reunía material suficiente, él desvelaba su verdadero rostro. El que amenazaba y chantajeaba a las que supuestamente eran sus amigas. Así engañó a 250 personas, la mayoría mujeres y menores. La Policía le detuvo una vez en octubre del año pasado. Pero siguió actuando. A la segunda le han llevado a prisión.

El método usado por este delincuente cibernético se conoce como grooming, nacido de la revolución que ha supuesto el auge de programas de mensajería instantánea, chats, redes sociales donde es fácil encontrar amigos pero no siempre con buenas intenciones. La operación policial que ha acabado con el arresto y encarcelamiento de este joven se ha hecho pública justo cuando el Ministerio del Interior ha emprendido una campaña para advertir de los riesgos de poner en Internet datos e imágenes privados, sobre todos, de menores. El detenido conocía estas facilidades y dominaba la técnica informática y las fórmulas para obtener de sus víctimas lo que buscaba.

La policía conoció los hechos a través de una denuncia registrada en Madrid. Una joven reveló que alguien al que había conocido en Internet la estaba chantajeando. Ella misma le había entregado, en virtud de la confianza ganada, una foto con una imagen suya desnuda. Ahora su supuesto amigo cibernético le amenazaba con difundirla y humillarla públicamente si no le entregaba semanalmente un vídeo de contenido sexual en el que ella apareciera. Esa denuncia permitió seguir la pista al acosador. La Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía le localizó en octubre de 2008 en Chipiona y se le intervinieron dos ordenadores portátiles y dos discos duros. Fue detenido pero quedó en libertad.

El material intervenido fue analizado y se constató la existencia de más víctimas. Este descubrimiento abrió una nueva investigación que se ha prolongado todos estos meses y que ha permitido cifrar en 250 las víctimas, la mayoría de ellas mujeres y menores de todo el territorio español, aunque también había extranjeras. El acosador no se limitó a utilizar la información personal que sus víctimas le habían cedido voluntariamente, sino también usó programas de control remoto para acceder al contenido de cuentas de correo electrónico y los archivos personales de sus ordenadores.

Protección de datos clínicos*

*Jesús Rubí Navarrete***

Quiero en primer lugar felicitar a la CONAMED, y sumarme a la celebración de su Décimo Aniversario, agradecer la invitación que me han cursado y abordar con todos ustedes un aspecto tan importante como es el tratamiento de los datos relacionados con la información clínica.

La estructura del presente trabajo contiene, primeramente, una referencia a la perspectiva española en relación con esta materia que incluye dos aspectos. Por una parte, la regulación de la materia, que es compleja porque se interrelacionan dos normativas distintas. De un lado, la normativa de protección de datos personales que es una exigencia necesaria en cualquier Estado miembro de la Unión Europea y, por otra parte, la normativa sectorial sanitaria que se refiere específicamente a la historia clínica. Además, comentaré al hilo de la exposición algunos casos concretos que se han suscitado sobre esta materia en la experiencia práctica de la Agencia Española de Protección de Datos que es el órgano administrativo independiente que tiene la obligación y la facultad de aplicar estas normas.

También haré una breve referencia a un documento de trabajo provisional, que está pendiente de aprobación, elaborado en el marco de la Red Iberoamericana de Protección de

Datos y que se refiere específicamente a esta materia. Y, finalmente, plantearé una reflexión sobre los puntos de conexión normativa en relación con la regulación del tratamiento de datos de la historia clínica que pueden existir entre la normativa europea y la de los Estados Unidos de México.

Por lo que se refiere al régimen jurídico del tratamiento de datos de la historia clínica, haré referencia a las normas más importantes. La primera es un convenio internacional,

---

* Con ocasión de la celebración del Día Internacional de protección de datos y de la celebración de un acto del máximo nivel institucional en la Honorable Cámara de Diputados, promovido por el Instituto Federal de Acceso a la Información Pública Gubernamental, y atendida la sensibilidad con que en México está abordado la protección de datos personales y especialmente la relacionada con la historia clínica, agradezco la oportunidad que se me rinda para reproducir la Conferencia Magistral que dicté con ocasión del Décimo Aniversario de CONAMED. Rubí Navarrete, Jesús, "Protección de Datos Clínicos", *Revista CONAMED,* Vol. 11, No. 8, octubre-diciembre, México, 2006.

** Adjunto al Director de la Agencia Española de Protección de Datos, Madrid, España.

el Convenio 108 del Consejo de Europa relativo al tratamiento de datos personales con previsiones específicas respecto del tratamiento de datos de salud. La segunda norma es una Directiva Comunitaria; la 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 que ha exigido que en todos los países de la Unión Europea exista un sistema armonizado en materia de protección de datos personales de manera que sean posibles los flujos transfronterizos de datos entre todos los estados miembros con un régimen de garantías homogéneos y, de este modo, no haya obstáculos al desarrollo del mercado interior. Son dos normas que quiero destacar específicamente porque posteriormente, en el último punto de mi intervención, volveré a hacer referencia a ellas. La tercera norma es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (LOPD) donde se establece el sistema de garantías y de derechos en materia de protección de datos con un tratamiento específico respecto de los datos de salud. Dentro de esos derechos se reconoce el derecho al acceso y también los de rectificación y cancelación, que han planteado dudas y situaciones conflictivas en el ámbito de la historia clínica. La última norma es una regulación sectorial; es la Ley 41/2002, de 14 de noviembre, que regula los derechos de autonomía del paciente y contiene , también, una regulación detallada sobre el tratamiento de la información clínica y su protección.

Los datos de la historia clínica son una modalidad, quizás la más importante, de los datos de salud. Los datos de salud, en la normativa a la que he hecho referencia se consideran datos sensibles o datos especialmente protegidos y como tales tienen un régimen de garantías más reforzado que el que tiene el tratamiento de cualquier otra información personal. Existen otros datos especialmente protegidos como son las creencias religiosas, el origen racial, la ideología, o la afiliación sindical. Pero entre los datos especialmente protegidos el que quizá, en la práctica, ha planteado más conflictos es el tratamiento de los datos de salud.

En relación con el tratamiento de los datos de salud, la primera cuestión que se ha planteado es la de qué debemos entender por datos de salud. De los datos de salud se trata constantemente: hay referencias al derecho a la salud en las constituciones, en las regulaciones sanitarias y en los convenios internacionales pero no se define qué es un dato de salud o hasta dónde llega el concepto de datos de salud. Esta es una cuestión extraordinariamente relevante porque según se tenga una interpretación expansiva o restrictiva de lo que son datos de salud, todo el sistema de garantías que acompaña al tratamiento de esos datos será, a su vez, más amplio o más reducido. Por otra parte, la cuestión tiene también importancia porque que exista un criterio expansivo o restrictivo en la consideración de los datos de salud afecta a las limitaciones que se establezcan a ese régimen de garantías. Si se adopta una postura expansiva resultará que las limitaciones

deberán interpretarse restrictivamente y si se adopta una postura restrictiva resultará que esas limitaciones al régimen de garantías se podrán interpretar extensivamente.

En nuestra experiencia hemos tenido un problema concreto en un procedimiento por infracción de la ley en el cual se planteaba si la referencia a datos de discapacidad o a grados de minusvalía debía o no considerarse como un dato de salud a efectos de la adopción de medidas específicas de seguridad de nivel alto. Ello dió lugar a que la Agencia Española de Protección de Datos adoptara una resolución que abordaba esta materia. En ella se toma como referencia la Carta de la Organización Mundial de la Salud en la que se considera que la salud es el estado completo de bienestar físico y mental de la persona y no sólo la ausencia de enfermedades; es decir, es un concepto expansivo. En el mismo sentido, La Memoria explicativa del Convenio 108 al que antes he hecho referencia considera datos de salud todas las informaciones pertenecientes a la salud pasada, presente y futura, física o mental de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido y también comprende informaciones relativas al abuso de alcohol y al consumo de drogas.

A su vez, uno de los órganos de este Convenio como es el Comité de Ministros, en el año 1997 hizo una recomendación específica sobre datos médicos en la cual se pone de manifiesto un criterio expansivo respecto del concepto de datos de salud. En ella, con una perspectiva de anticipación muy importante, se afirma rotundamente algo que en ocasiones ahora se discute, cómo que las informaciones genéticas son datos de salud. Asimismo, en la jurisprudencia europea se ha planteado esta cuestión. Citaré una sentencia muy significativa del Tribunal de Justicia de las Comunidades Europeas del año 2003, el asunto Lindqvist, en la cual se le plantea al Tribunal si una información incorporada en una página web sobre una lesión en un pie y una situación de baja laboral asociada a esa lesión, es o no un dato de salud. El Tribunal opta por un criterio expansivo en el sentido de que esa mera referencia constituye un dato personal relativo a la salud en el sentido del artículo 8 de la Directiva 95/46/CE. Por tanto, en el ámbito europeo y, en particular, en España, se puede concluir que el concepto de dato de salud es un concepto amplio y expansivo; que la interpretación en caso de duda tiene que seguir esa orientación amplia y que cualquier limitación que se establezca respecto al tratamiento de los datos de salud, al acceso a los datos de salud o cualquier limitación a los derechos de las personas en esa materia, puede ser legítima pero deberá interpretarse restrictivamente.

Los datos de salud son datos especialmente protegidos lo que determina que tengan unas garantías específicas. La primera de ellas es la que afecta a la legitimización para poder tratar o acceder al uso de la información relacionada con la salud. En el ámbito de la normativa comunitaria, las dos causas principales que habilitan el tratamiento de los datos de salud son el consentimiento explícito del afectado y el hecho de que, por motivos de interés general, una norma con rango suficiente establezca la posibilidad de poder acceder, tratar o utilizar aquellos datos.

En lo que se refiere a los datos de salud que constan en la historia clínica, la Ley 41/2002, de Autonomía del Paciente contiene una definición de la información clínica y de la historia clínica. Se define la información clínica como todo dato, cualquiera que sea su forma, clase o tipo que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona o sobre la forma de preservarla, cuidarla, mejorarla o recuperarla. Por tanto, en esta definición se mantiene un criterio expansivo, que trata de comprender un abanico muy amplio de informaciones relacionadas con la atención al paciente. La misma Ley define la historia clínica como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole -de nuevo este concepto abierto y expansivo, -sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial. En la Ley de Autonomía del Paciente esta definición se complementa a lo largo del articulado con elementos adicionales porque en otros artículos se aclara que en la historia deberá constar la identificación de los médicos y de los profesionales que intervienen en la asistencia del paciente, que la documentación clínica debe estar ordenada y seguir un criterio secuencial y que debe responder a un principio de máxima integración, por lo menos a nivel de centro. A esta última cuestión se hará referencia en un momento posterior puesto que vivimos en estos momentos una polémica muy intensa sobre la posibilidad de digitalizar y centralizar las historias clínicas o de permitir accesos remotos a las informaciones clínicas que constan en otras administraciones sanitarias.

La Ley contempla, además, un contenido mínimo de las historias clínicas. Esta regulación del contenido mínimo de las historias clínicas me parece particularmente relevante y creo que es una manifestación de la asunción de responsabilidades por parte de los poderes públicos. Los poderes públicos al delimitar este contenido mínimo de la historia clínica han permitido resolver, al menos parcialmente, un aspecto: todo aquello que sea el contenido mínimo de la historia clínica no se podrá considerar que forma parte de anotaciones o referencias subjetivas de los profesionales sanitarios; es un contenido mínimo de naturaleza objetiva sobre la información que la integra, a la que siempre se tendrá que permitir el acceso a los interesados.

La Ley también regula la finalidad de la historia clínica. La finalidad y el principio de finalidad en la normativa de protección de datos son claves porque delimitan el ámbito en el cual está legitimado el acceso y el tratamiento de la información; sólo se podrán tratar los datos para aquellas finalidades determinadas para las que la norma o el consentimiento informado de los pacientes permitan esa utilización. Por tanto, es un eje conductor muy relevante a la hora de analizar cualquier problema relacionado con el tratamiento de datos en general y, en particular, con el tratamiento de los datos de la información clínica. La ley delimita o señala un fin principal de la historia clínica que es facilitar la asistencia sanitaria al considerar la historia clínica como un instrumento des-

tinado a garantizar esa adecuada asistencia. De ello se derivan una serie de obligaciones para el paciente y para los profesionales sanitarios. Para el paciente porque la Ley le impone la obligación de facilitar información y de contribuir a su obtención, en particular, cuando puedan estar afectados intereses públicos relevantes. Y, para los profesionales sanitarios porque reitera lo que es y debe ser la buena práctica como es el incorporar a la historia clínica toda aquella información veraz y actualizada sobre el estado de salud del paciente.

Junto a esta finalidad principal, la ley reconoce otras posibilidades de uso y acceso de la historia clínica por razones de interés general, como son los fines epidemiológicos, de salud pública, de docencia e investigación, de inspección, evaluación, acreditación y planificación de la calidad de la asistencia sanitaria y de administración y gestión sanitaria -aunque aquí quiero hacer una referencia particular porque la Ley tiene la prevención de que, en lo que se refiere al acceso por parte de las propias unidades de administración y gestión sanitaria, ese acceso será un acceso limitado a aquello que esté vinculado a sus funciones-. También está habilitado el tratamiento y el acceso a los datos para investigaciones judiciales.

En lo que se refiere al acceso a la historia clínica hay que mantener un criterio prudente y realizar un análisis sistemático de dos normas complementarias: la Ley Orgánica de Protección de Datos, que recoge una serie de principios generales sobre el derecho de acceso y sobre otros derechos como los de rectificación y cancelación y la Ley de Autonomía del Paciente que, en ocasiones, supone una modulación o una adaptación a peculiaridades específicas relacionadas con el ámbito sanitario.

La LOPD recoge la estructura básica de estos derechos en general y, en particular, del derecho de acceso. Se reconoce el derecho y se establece que son derechos personalísimos; es decir que sólo podrían en principio, ser ejercidos por su titular. (Una de las modulaciones de la Ley de Autonomía del Paciente es que se reconoce, en el caso de la información clínica, derecho de acceso a terceros que son distintos del paciente).

La LOPD establece también una prioridad en el ejercicio del derecho por parte del paciente y en la selección de las modalidades de acceso; es el paciente el que ejercita su derecho y el que decide cómo lo va a ejercitar. Existen casos en la experiencia práctica de ejercicio del derecho de acceso a la información clínica en la cual se ha contestado adecuadamente, en principio, a la persona que ejerce su derecho, manifestándole que debe acudir al centro sanitario para obtener información. En nuestro sistema legal, ésta es sólo una posibilidad pues la regla general es que el paciente es quien tiene derecho a elegir cuál es la opción que selecciona para el acceso a la información clínica, aunque a veces el tomar esta decisión puede suponer para él, algunas consecuencias.

La normativa de protección de datos prevé que pueda elegir la visualización en pantalla, escrito, copia o fotocopia remitida por correo, telecopia o cualquier otro proced-

imiento adecuado a la configuración o implantación del fichero que le ofrezca el responsable de este fichero.

En algunos casos en que se ha planteado la situación citada, el centro sanitario ofrece la posibilidad de acudir al mismo porque estima más adecuado que se persone en el centro sanitario y acceda a la información, pero el paciente quiere que se le remita una copia por correo. En la resolución de este tipo de casos, el criterio que se ha sostenido es que la Ley reconoce ese derecho preferente al paciente pero, en la medida en que se le ha ofrecido una opción alternativa que también garantiza su derecho y que es más segura, los riesgos sobre la seguridad en el envío de la documentación correrán por cuenta del paciente que ha optado por esa modalidad en el ejercicio de su derecho y no de parte del centro sanitario. La LOPD también establece los plazos para atender el ejercicio del derecho de acceso, que es de un mes para analizar la petición y resolver y 10 días adicionales para hacer efectivo el ejercicio del derecho.

Por su parte la Ley de Autonomía del Paciente completa la regulación del derecho de acceso. La Ley considera que forma parte del contenido propio del derecho constitucional a la salud el acceso a la información clínica; es decir, desde el punto de vista jurídico, aunque no existiera el derecho de acceso en la normativa de protección de datos, en la medida en que la Ley de Autonomía del Paciente resalta que ese derecho de acceso forma parte integrante de un derecho constitucionalmente reconocido como es el derecho a la salud, deberían existir modalidades de acceso a la información clínica. La Ley permite el acceso de forma directa o por representación, reconoce expresamente que se tiene derecho a obtener copia de los datos; es decir, que no basta con la mera exhibición de la información salvo que el paciente admita dicha solución. El paciente tiene derecho de acceso al contenido mínimo de la historia clínica y también a los datos adicionales. No tiene derecho a disponer de la documentación original y sí a obtener copias de las pruebas y de los informes.

Este derecho de acceso del paciente tiene, no obstante, algunas limitaciones que están reconocidas en la misma norma. En primer lugar, el derecho de acceso está limitado respecto de aquellas informaciones que puedan suponer perjuicio para terceros, cuyos datos constan en la propia historia clínica en interés del propio paciente. En segundo lugar, la Ley reconoce la posibilidad de ejercer un derecho de reserva de los profesionales a sus anotaciones subjetivas, derecho que precisa algunas aclaraciones. Es un derecho reconocido normativamente; es decir, si la norma no lo reconociera, el derecho de acceso del paciente tendría efectividad de una manera absoluta y no habría posibilidad de oponer el derecho de reserva a las anotaciones subjetivas. Esto es así porque el dato de salud es un dato especialmente protegido, de forma que cualquier limitación al régimen de garantías de estos datos debe interpretarse restrictivamente.

Por otra parte, el derecho de reserva es un derecho de los profesionales que intervi-

enen en la elaboración y en la integración de la información clínica, no de los centros sanitarios. Se han planteado en la práctica de la Agencia Española de Protección de Datos casos en los cuales el paciente ejerce el derecho de acceso y el centro sanitario contesta dentro de plazo motivando que la ley reconoce el derecho a la reserva de las anotaciones subjetivas, y no facilita la información. En esos casos se ha solicitado la tutela de la Agencia Española de Protección de Datos cuyas resoluciones reconocen el derecho a la reserva, a las anotaciones subjetivas pero como derecho del profesional sanitario y no del centro o de la entidad, por lo que se acuerda que, o bien, se facilite la información, o bien se acredite que es el profesional el que ha ejercido el derecho de reserva a sus+ anotaciones subjetivas. En este ámbito se está extendiendo en la práctica el que haya formatos protocolarizados o estándares dentro de los centros sanitarios en los cuales se distinguen diversos apartados de forma que haya una mayor claridad para poder distinguir qué tipo de información tiene que ser considerada como información objetiva y dónde tienen que recogerse, en su caso, las anotaciones subjetivas, en la medida en que se generalicen esos protocolos, para lo cual pueden ser muy útiles instrumentos de auto-regulación, probablemente se conseguirán soluciones más equilibradas. Quizá en esa auto-regulación puedan tener un papel importante Instituciones como la CONAMED, también, el IFAI.

Otra modalidad de acceso a la historia clínica que, lógicamente, se reconoce es la de los profesionales que realicen el diagnóstico y el tratamiento del paciente; acceso que se legitima por una finalidad específica: garantizar la adecuada asistencia sanitaria. Sin embargo, basta con ser un profesional sanitario para acceder a la historia clínica. Se han producido casos en la experiencia de la Agencia Española de Protección de Datos en el que un profesional sanitario de un complejo materno-infantil solicita un acceso a información clínica de un paciente que resulta ser su cuñado y utiliza esa información para facilitarla a su hermana con el fin de que la aporte a un proceso de divorcio. Esta situación dio lugar a una declaración de infracción de esta normativa y a la exigencia de responsabilidades al profesional. Sin llegar a esos extremos es preciso tener en cuenta, conforme a una regla de proporcionalidad, que el acceso de los profesionales tiene que responder a la finalidad de garantizar la adecuada asistencia o a otras finalidades previstas por razones de interés público como las anteriormente citadas.

En cuanto a las modalidades de acceso, la Ley de Autonomía del Paciente establece que el acceso debe realizarse garantizando, como regla general, el anonimato, es decir, disociando la información personal de la información clínica que consta en la historia clínica. En la experiencia práctica los principales problemas que se nos ha suscitado ha sido el de analizar hasta qué punto el anonimato o la disociación de datos es reversible o irreversible. No basta en muchas ocasiones, con limitarse a omitir el nombre de una persona o a sustituir el nombre de una persona con unas iniciales o, en su caso, utilizar

un código alfanumérico si después existe la posibilidad dentro del sistema de documentación sanitaria de ese centro, de que cualquiera pueda volver a asociarla a la persona sin dificultad.

Esta regla general tiene una excepción específicamente prevista: la investigación judicial. Pero podría haber otras derivadas de otras legitimaciones, como el acceso a la historia clínica, por ejemplo, en el ámbito de la epidemiología, pues evidentemente si es necesario detectar qué persona o qué grupo de personas concretas han podido ser el origen de un fenómeno epidemiológico, habrá que permitir que se rompa la regla general de garantizar el anonimato.

En relación a los fallecidos, la Ley de Autonomía del Paciente reconoce el derecho de acceso a las personas vinculadas por razones familiares o de hecho con respeto al principio de finalidad y al de proporcionalidad. Al principio de finalidad porque podrán acceder siempre que esa información pueda ser relevante para prevenir un riesgo para la propia salud del que accede. Con arreglo al principio de proporcionalidad porque sólo se accederá a los datos que sean pertinentes para ese riesgo a la salud que habilita y legitima el acceso. En todo caso, es un acceso sujeto a limitaciones porque no podrá realizarse cuando el paciente lo haya prohibido expresamente, se generen perjuicios a terceros o se ejerza el derecho de reserva a las anotaciones subjetivas.

Hasta este momento se ha expuesto la doctrina y los precedentes de la Agencia española de protección de datos y de la legislación europea y española. Sin embargo, en este punto formularé una reflexión adicional de carácter estrictamente personal. La Ley de Autonomía del Paciente regula el derecho a la información en distintos lugares. A mi juicio, en esta norma hay dos bloques de derechos; unos que se refieren estrictamente a la autonomía del paciente y otros que tienen una relación más directa con la protección de datos personales. El derecho a la información asistencial creo que es un derecho que forma parte de esos derechos de la autonomía del paciente ¿Por qué? Porque es el derecho a obtener información para que el paciente pueda tomar decisiones sobre su proceso asistencial; para que pueda tomar la decisión de no querer recibir información o la de si se somete o no a una determinada prueba para que conozca los riesgos que asume, etc.; pero no es, en mi opinión, un aspecto directamente relacionado con la protección de datos, como sí sucede con el derecho de acceso a la información clínica. Aquel conjunto de derechos complementan las normas de protección de datos pero no son estrictamente derechos propios de esta regulación, salvo quizás en algunos aspectos puntuales, por ejemplo, en el hecho de que cuando se facilita información, se haga constar en la historia clínica. A través de la constancia en la historia clínica sí podría haber una conexión con la normativa de protección de datos personales. Pero la tutela de los derechos de información asistencial o de otros derechos propios de autonomía del paciente, como son todo el sistema de decisiones que articulan esa autonomía, creo que no son tanto

temas de protección de datos sino que más bien deben ser tutelados por las propias administraciones sanitarias.

Junto al derecho de acceso, la normativa de protección de datos reconoce otros derechos, como son los de rectificación y cancelación respecto de los cuales se han planteado conflictos en relación con la información clínica.

Sobre el derecho de rectificación reseñaré dos supuestos concretos. Una persona que plantea, a través de un procedimiento de tutela de derechos tramitado en la Agencia Española de Protección de Datos, que una información que consta en su historia clínica tiene que rectificarse porque dispone de un segundo diagnóstico y debe prevalecer el diagnóstico que ha emitido el segundo profesional sanitario. En esos casos, como regla general, la Agencia ha desestimado la tutela del derecho porque creo que no corresponde a nuestra función hacer esas valoraciones que son propias de profesionales sanitarios, por lo que habrá que acudir, en su caso, a un contraste realizado por esos profesionales.

También se han planteado supuestos relacionados normalmente con la obtención o el reconocimiento de prestaciones de la seguridad social. Se pretende que se rectifique la información clínica para solicitar una invalidez u otra prestación para cuya obtención la información que figura supone un obstáculo, por lo que se exige su rectificación adjuntando una segunda opinión.

Estas tutelas de derechos también se han desestimado en la medida en que hay procedimientos específicos a través de tribunales médicos especializados que son los que tienen que evaluar en qué medida se deben reconocer unas u otras prestaciones del sistema de la seguridad social.

Por lo que se refiere al derecho de cancelación se han suscitado casos en los cuales se ha solicitado la cancelación de datos que figuran en la historia clínica. Se pretende que no conste una información porque puede ser perjudicial en el ámbito laboral, el ámbito profesional, en el ámbito de la imagen, etc. En estos casos las resoluciones de la Agencia Española de Protección de Datos siempre han confirmado la denegación del derecho y la cancelación porque en la propia Ley de Autonomía del Paciente hay obligaciones específicas de conservación de la información clínica. La conservación y custodia de la información clínica está reglada por razones de interés público puesto que no sólo responde a intereses particulares sino a otros intereses generales. Por ello la Ley establece que deberá conservarse la información durante el tiempo necesario para realizar la asistencia sanitaria o para otras necesidades como las epidemiológicas, de investigación u organización y funcionamiento del sistema nacional de salud. Si bien existen normas autonómicas en algunas regiones españolas que han ampliado este plazo mínimo a periodos mucho más extensos, como puede ser el de treinta años, la Ley establece un periodo mínimo de conservación de cinco años.

El sistema de protección de datos de la historia clínica se completa con dos principios de protección de datos muy importantes, como son los de seguridad y de secreto. El

principio de seguridad responde a dos objetivos. El primero es el de mantener la integridad de la información para que ésta pueda ser recuperada. Hemos tenido casos en los cuales un incendio en centros de documentación clínica, ante la ausencia de medidas de seguridad como son las copias de respaldo, ha destruido información clínica que no puede recuperarse porque a las personas no se les puede volver a poner en las mismas situaciones o en los mismos estados de salud que han tenido a lo largo del tiempo.

El principio de seguridad pretende, en primer lugar, conseguir la integridad y la posibilidad de recuperar la información clínica y en segundo lugar, evitar accesos no autorizados a la información. Para ello se exigen medidas de seguridad que impidan tales accesos o permitan auditar si se han producido. Todas estas medidas de seguridad están reguladas en un Real Decreto que aprueba el Reglamento de Medidas de Seguridad con varios niveles que, en el caso de que afecten a los datos de salud y, por Medidas de Seguridad es accesible a través la página web de la Agencia Española de Protección de Datos (www.agpd.es).

La última garantía complementaria de protección de la información clínica es el deber de secreto que ha existido históricamente en el ámbito de las profesiones sanitarias.

Una cuestión adicional que se plantea cada vez con más intensidad en relación con el sistema de protección de la historia clínica es el de la centralización y el acceso remoto a la misma.

En efecto, se está produciendo una importantísima polémica sobre en qué medida las administraciones sanitarias tienen legitimación para realizar procesos de digitalización y de centralización de la información clínica sin el consentimiento de pacientes, ni de los profesionales sanitarios. Esta cuestión ha dado lugar a múltiples reclamaciones por parte de profesionales de la salud y también por parte de los propios pacientes. Desde el punto de vista de las administraciones sanitarias, se señala que la digitalización de la historia clínica tiene ventajas: es más segura, permite un acceso centralizado y completo a la información, evita la reiteración de pruebas, puede reducir costos en la medida en que se evita esa reiteración de pruebas, etc. Son razones de interés desde el punto de vista de la administración sanitaria, aunque exceden de la competencia específica de la Agencia; pero lo que sí es competencia de la Agencia es analizar si es necesario o no el consentimiento del profesional o el del propio paciente para realizar estos procesos de integración.

La conclusión ha sido que en la normativa española no es necesario. Es una decisión de auto-organización que pueden llevar a cabo las propias administraciones sanitarias, siempre y cuando se respeten las restantes garantías de protección de datos y, muy particularmente, un régimen muy riguroso de medidas de seguridad.

En nuestro sistema legal existe una habilitación específica en la Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud que regula el sistema de información

sanitaria del sistema nacional de salud y también el intercambio de información y las exigencias de seguridad en las redes de comunicación de dicho sistema (deben realizarse con procedimientos de firma electrónica y firma electrónica avanzada).

En otros casos se ha optado, no tanto por crear una base nacional de datos de salud sino, por permitir accesos remotos a las distintas bases de datos de las distintas administraciones sanitarias. Esto puede ser frecuente en estados federales como es el caso de México o en estados con un régimen autonómico muy desarrollado, como es el caso de España en el cual la prestación del servicio público de salud corresponde a las Comunidades Autónomas.

A este respecto, debe considerarse que el acceso a la información clínica, es una manifestación del derecho a la asistencia sanitaria en régimen de movilidad. Si no se permitiera ese acceso remoto a la información clínica cuando una persona se desplaza a otro Estado, o a otra Comunidad Autónoma, no se estaría garantizando el derecho a la salud que está reconocido constitucionalmente. Por eso la Ley de Calidad y Cohesión permite que pueda haber accesos remotos siempre que responda a las finalidades de permitir al interesado y a los profesionales que participen en la asistencia el acceso a la historia clínica, con limitación a los datos estrictamente necesarios para garantizar la calidad de la misma manteniendo la confidencialidad e integridad de la información.

En este ámbito está promoviéndose como herramienta apropiada para los procesos de acceso remoto y de reconocimiento del derecho a las prestaciones sanitarias la denominada tarjeta sanitaria individual (TSI).

La TSI, habilitada en la Ley de Cohesión y Calidad del Sistema Nacional de Salud, es un documento que emiten las administraciones sanitarias con tres finalidades. La primera, es el reconocimiento a su titular del derecho a la asistencia sanitaria en distintas modalidades de prestaciones -no sólo asistencia sanitaria sino, por ejemplo, la prestación farmacéutica u otras-. En segundo lugar, el conseguir una identificación unívoca e inequívoca del paciente que tiene derecho a esas prestaciones y, en tercer lugar y como consecuencia de esta identificación unívoca, el tener garantías de que cuando hay accesos remotos a la historia clínica la persona está siendo objeto de atención por parte de profesionales sanitarios.

Junto a estas finalidades se ha suscitado la posibilidad de incorporar a la TSI un chip en el que conste información clínica. El criterio que ha mantenido la Agencia Española de Protección de Datos es que en tal caso sería necesaria una habilitación legal específica que regulara qué información se recoge, para qué finalidad y quién podría tener acceso a ella.

Como se señaló anteriormente, a continuación se hará muy brevemente referencia a dos aspectos complementarios. El primero de ellos se refiere al documento de la Red Iberoamericana de Protección de Datos que ha estado elaborando un grupo de trabajo específico en Santa Cruz de la Sierra (Bolivia), en mayo de este año.

La Red Iberoamericana de Protección de Datos se crea en la Declaración de La Antigua, en el año 2003, como un foro abierto para potenciar experiencias y colaborar en materia de protección de datos personales. Recibió en noviembre de 2003, el respaldo de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno en cuya Declaración de Santa Cruz de la Sierra se reconoce expresamente el derecho fundamental a la protección de datos y se reconoce la labor de la Red Iberoamericana de Protección de Datos. Este reconocimiento se ha reiterado en la última Conferencia Mundial de protección de datos celebrada en Suiza en 2005. En ella están representados en este momento instituciones de 17 países iberoamericanos.

En el IV Encuentro Iberoamericano de Protección de Datos que se celebró en la Ciudad de México y se clausuró en Huixquilucan en noviembre del año pasado, uno de los paneles estuvo relacionado con el tratamiento de datos de la salud y su régimen de garantías y, particularmente, la cuestión del acceso a los datos de la información clínica.

Las conclusiones se recogieron en la Declaración de México mandándose a un grupo de trabajo para que elaborara un documento específico más desarrollado sobre el tratamiento de datos de la historia clínica. Este documento es el que, aún en borrador, es el que se ha elaborado en Santa Cruz de la Sierra y está pendiente de aprobación para el V Encuentro que se celebrará en Brasil en el año 2006.

En el documento, que aún no está disponible, todos los principios que se han tratado, se generalizan y se adaptan a un entorno más amplio como es el iberoamericano. En lo que se refiere al concepto de datos de salud, se ratifica un criterio amplio y expansivo basado en una referencia específica al acuerdo de integración de la Organización Panamericana de la Salud a la Organización Mundial de la Salud. El documento reitera la vinculación expresa entre el derecho a la salud y el derecho de acceso a la historia clínica cuya significación, desde el punto de vista jurídico, es la de que aún no existiendo una normativa específica de protección de datos personales se podría apoyar el derecho de acceso a la información clínica como parte del derecho a la salud reconocido constitucionalmente o en convenios internacionales. Contiene una referencia específica respecto a la posibilidad de que el profesional sanitario, si entiende objetivamente que por razones de necesidad terapéutica es mejor no informar a un paciente, no lo haga, dejando constancia en la historia clínica e informando a las personas vinculadas a él por razones familiares o de hecho. Pero señala que cuando no se informa al paciente, éste tendría derecho a acceder a esa constancia en la historia clínica de que no se le informó y a la información omitida. El documento aclara que debe reconocerse ese derecho a posteriori al paciente.

La última cuestión que se tratará, es una reflexión sobre los puntos de conexión entre la normativa europea y la normativa mexicana de protección de datos. En esta conferencia se ha expuesto el sistema de garantías del tratamiento de los datos de salud y, en

particular, de la historia clínica en el ámbito de la normativa europea y española. Como antes se señaló dos de los grandes puntos de referencia básicos son el Convenio 108 del Consejo de Europa y la Directiva 95/46/CE de protección de datos personales.

En relación a ellos creo que hay un elemento de debate basado en el Acuerdo de Asociación Económica, concertación política y cooperación entre la Comunidad Europea y sus Estados miembros y los Estados Unidos Mexicanos. Éste es un convenio internacional; es decir, forma parte del derecho interno de este país y también forma parte del derecho europeo y debe ser respetado por todos los Estados miembros de la Unión Europea que recoge algunas referencias específicas a la protección de datos personales.

La primera de ellas se refiere al reconocimiento de que debe garantizarse un grado elevado de protección conforme a las normas adoptadas por los organismos internacionales competentes y por la Comunidad Europea. Esta declaración podría considerarse una pura declaración formal, una declaración de intenciones. Pero dicha declaración, en este Convenio Internacional, remite expresamente a las normas del Anexo que forman parte integrante del mismo.

En el Anexo se recogen como normas específicas, las Directrices para la reglamentación de los archivos de datos personales de la Organización de las Naciones Unidas, las Recomendaciones de la OCDE, el Convenio del Consejo de Europa sobre Protección de Datos Personales, (Convenio 108) que tiene garantías específicas respecto del tratamiento de datos de salud y la Directiva 95/46/CE de Protección de Datos Personales que tiene previsiones normativas más detalladas en materia de protección de datos personales y, muy especialmente, en lo que se refiere a la legitimación y acceso a la información.

Sobre la base de este reconocimiento del derecho a la protección de datos y a las normas en las cuales debe ampararse el derecho a la protección de datos, el Acuerdo prevé que haya una cooperación en materia de protección de datos para mejorar el nivel de protección, contempla la posibilidad de asistencia técnica y recoge una última previsión que puede tener interés conexo o colateral en la medida en que se reconoce la importancia de la sociedad de la información y de las tecnologías de la sociedad de la información, las cuales, en el ámbito del tratamiento de datos de la historia clínica, van teniendo de una forma creciente un desarrollo importante.

Acceso al expediente médico*

*José Roldán Xopa***

Introducción

El acceso del paciente a su expediente es una condición para el ejercicio del derecho a estar informado y tomar decisiones acerca de su salud. No obstante, de acuerdo a una disposición administrativa de carácter técnico: la Norma Oficial Mexicana (NOM) 168-SSA1-1998, solamente obliga al médico o a la institución a otorgar "la información verbal y el resumen clínico" previa petición por escrito "especificándose con claridad el motivo de la solicitud". Lo anterior, crea una limitación general para que el paciente acceda directamente a la información del expediente. El impedimento, además de limitar la posibilidad de un paciente informado, tiende a reforzar una cultura paternalista del médico sobre el paciente, incrementa los costos de decidir cambio de médico o pedir segundas opiniones, y refuerza la protección gremial en casos de mala práctica, entre otros efectos.

El derecho de acceder a la información del expediente. Avances

La emisión de Ley de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) y la actuación del Instituto Federal de Acceso a la Información (IFAI) vino establecer un medio por el cual, los pacientes podían intentar acceder a su expediente cuando los mismos estuviesen a cargo de entidades públicas de salud. La presentación de dichas peticiones llevó a plantear el enfrentamiento de la regulación que obstaculiza el acceso.

La justificación de las instituciones de salud fue que la NOM establecía el "quantum" de la información a que estaban obligadas a proporcionar, así como un derecho de propiedad del expediente en favor del médico y de la institución de salud. La negativa

---

* Roldán Xopa, José, "Acceso al expediente médico", *Derecho a saber. Balance y perspectivas cívicas, Jonathan Fox*, Fundar, México, 2007.

** Jefe del Departamento Académico de Derecho. Profesor de Derecho Administrativo.

a dar la información motivó que diversos peticionarios acudieran ante el IFAI promoviendo el recurso de revisión (Art. 39 de la LFTAIPG). La apertura de esta instancia de control llevó a enfrentar una diversidad de problemas, siendo los principales: cómo abordar la limitación regulatoria (NOM) y cuál es la extensión de la información accesible al paciente.

La NOM 168-SSA1-1998 como barrera de acceso a la información

La NOM es una norma administrativa general de carácter obligatorio para sus destinatarios incluyendo, por supuesto, a los médicos e instituciones públicas de salud. Por tanto, sus objeciones para no aplicarla no son triviales: la inobservancia podría ser causa de responsabilidad administrativa. El IFAI resolvió la oposición, señalando que la NOM 168 es de inferior jerarquía a la LFTAIPG. En la resolución de los recursos de revisión 314/03 y 315/03, se revocaron las respuestas iniciales que negaban el acceso a los expedientes, argumentando que:

> [...] una ley federal tiene supremacía sobre una Norma Oficial Mexicana. Desde el 12 de junio de 2003, la Ley Federal de Transparencia y Acceso a la Información es la ley específica que protege los datos personales en posesión de los sujetos obligados en el ámbito federal y regula el acceso a los mismos, por parte de sus titulares o representantes.3

El conflicto es resuelto por el IFAI acudiendo a un criterio de jerarquía (la norma superior prevalece). La situación de los sujetos obligados cambia: una obligación proveniente de la norma es suplida por una orden de la autoridad reguladora del acceso a la información. Esto permite a los sujetos colocarse en situación de ser ejecutoras de una obligación y no de ordenadoras. El cambio de posición es relevante, ya que la existencia de una regulación contradictoria coloca al servidor público en un dilema que le crea inseguridad personal y afecta el desempeño de su función.

La extensión de la información disponible

¿Debe permitirse al paciente el acceso a toda la información?, ¿debe limitarse?, ¿por qué razones? En este terreno la intervención del IFAI ha ido cambiando y se aprecia una ruta de aprendizaje. En sus primeras resoluciones se instruye a las instituciones de salud a que entreguen copia del expediente completo4.

El argumento que funda las decisiones del IFAI se basa en el derecho de la persona a sus datos personales. Bajo la LTAIPG, la información concerniente a los datos de salud física o mental son datos personales (art. 4, fracción II), y por tanto confidenciales ante terceros, pero sobre los que la persona tiene derecho (arts. 20 a 25).

Si bien la consideración de que son datos personales, desde la perspectiva de acceso a la información, es el núcleo de la cuestión, desde la perspectiva de "salud", se introducen matices mucho más finos no siempre presentes en las decisiones. Este es sin duda uno de los mayores problemas que enfrenta el IFAI en el ejercicio de una función cuya característica es la "horizontalidad". Expliquemos lo anterior, la regulación de acceso a la información cruza una diversidad de materias sectoriales, entre ellas las de salud. El encuentro no es solamente una cuestión de cruce normativo sino cruce de "ratio", si la regulación de salud supone sus propios valores, propósitos de política pública, fines de interés público o de salubridad general, la sola perspectiva de datos personales resultaría parcial e inclusive contraproducente.

El expediente médico puede contener información que involucre datos personales de un tercero, información que pudiera dañar la estima del paciente respecto de otra persona (p. ej. Datos de un familiar que revele información acerca del paciente), información sobre un tratamiento que clínicamente resulte admisible pero que su conocimiento por el paciente ponga en riesgo su eficacia (placebos, información que de ser conocida pueda poner en peligro al paciente, etc.), información que involucre alguna investigación científica, las notas subjetivas de los médicos, etc. Los anteriores temas son motivo de debate tanto en el foro de la discusión jurídica como de la lex artis. Involucran determinados modelos de relación médico-paciente (los extremos entre el paternalismo del médico y el paciente informado que toma sus decisiones). El gran reto del órgano de transparencia y acceso a la información va siendo la reconstrucción de la "horizontalidad" de su materia y la "verticalidad" de las regulaciones sectoriales. El dilema es si la regulación de transparencia sirve a la racionalidad sectorial o si la regulación sectorial sirve a la transparencia.

En este terreno, las resoluciones del IFAI escasamente han dado luz a los problemas

Limitaciones

Creación de asimetrías regulatorias

La limitación de jurisdicción del IFAI a la información pública gubernamental origina una segmentación en los sujetos a los que se dirige la NOM: público y privado. Solamente los médicos e instituciones del sector público estarían obligados por sus decisiones. En cambio, para servicios médicos privados la NOM es plenamente aplicable: el expediente es propiedad de ellos y solamente están obligados a dar un resumen. Por supuesto, no se puede pedir que el IFAI no cree tales consecuencias, ni está en su competencia resolverlo.

Entendimiento de la racionalidad sectorial

La horizontalidad de la transparencia y acceso a la información tiene el mérito de cruzar las distintas materias sectoriales que atiende la administración pública, pero a la vez le plantea el reto de la falta de especialización y por tanto de limitaciones en el conocimiento de la racionalidad que anima a la regulación sectorial. El IFAI supone conocimiento y expertisse en su competencia, más no en medio ambiente, inversión extranjera, energía, telecomunicaciones, salubridad, etc. Puede darse el caso de que el acceso a cierta información plantee un conflicto entre interés público vs interés privado, o entre el fin sectorial y el interés de acceder a la información. El anterior conflicto como se ha visto en el caso del expediente clínico puede ser muy complejo y no siempre tocado con fortuna en las resoluciones del IFAI. El criterio de prevalencia de uno u otro es difícil de decidir. El IFAI tendrá siempre un incentivo para hacer prevalecer el criterio de acceder a la información lo que puede llegar a transtornar políticas públicas sectoriales. Si bien podría invocarse el buen juicio del IFAI, no deja de presentarse el riesgo.

Las zonas grises: los servicios médicos subrogados

En el material analizado no se encontró algún caso en el que se solicitara información a un médico privado que atendiera a un paciente que fuese derechohabiente de un servicio público (p. ej,. Seguro Social). Lo anterior plantearía el problema acerca de la jurisdicción del IFAI sobre médicos particulares que por un contrato de servicios profesionales con alguna entidad del sector público prestan el servicio que originalmente corresponde a éstos.

Perspectivas

El IFAI ha sentado ya un criterio positivo: los pacientes tienen derecho a la información de su expediente. Sin embargo, en perspectiva se encuentra la necesidad de que el IFAI afine sus criterios matizando aquellos casos que por necesidades sectoriales debe mantenerse confidencialidad de ciertas datos que por buenas razones no debe conocer el paciente. Por supuesto, hay cuestiones debatibles, pero deben ser abordadas.

Conclusiones y recomendaciones

El balance es positivo, los ciudadanos, al menos quienes tienen acceso a servicios públi-

cos, cuentan con una poderosa herramienta para mejorar la protección de sus derechos. El papel del IFAI ha ayudado a configurar un paciente más informado y con mayores instrumentos para activar la rendición de cuentas a los servidores públicos y a incentivar un mejor desempeño. No obstante, se requiere afinar la herramienta para paliar sus efectos secundarios.

Notas

[3]Recurso de revisión 315/03 y 314/03, disponibles en: http://www.ifai.org.mx/resoluciones/anual.php, fecha de consulta: 25 de junio de 2006.

[4] Esto se aprecia en los expedientes 314/03, 315/03, 476/03, 338/03, 285/05, entre otros.

Algunos aspectos sobre protección de datos: análisis comparativo internacional*

Análisis comparativo sobre principios, derechos y procedimientos

	PRINCIPIOS					DERECHOS					PROCEDIMIENTOS	
Instrumento jurídico	Consentimiento	Finalidad	Calidad	Información	Seguridad	Acceso	Rectificación	Cancelación	Oposición	Impugnación de valores	Sancionador	De recurso (judicial o administrativo)
APEC	sí	sí	sí	sí	sí	sí	sí	sí	sí	no	sí	sí
Directiva 95/46/CE	sí	sí	sí	sí	sí	sí	sí	sí	sí	sí	no	sí
OCDE	sí	sí	sí	sí	sí	sí	sí	sí	no	no	no	no
Puerto Seguro	no	sí	sí	sí	sí	sí	sí	sí	no	no	no	sí
FIPP	sí	no	no	sí	sí	sí	no	no	no	no	no	sí
Convenio 108 CE	no	sí	sí	sí	sí	sí	sí	sí	no	no	no	sí

*Davara Abogados, S.C., 2010

Análisis comparativo sobre principios, derechos y procedimientos

	TRUSTe	EuroPriSe
Objeto	Privacidad online	Privacidad online/ Derecho fundamental a la protección de datos de carácter personal
Criterios para la concesión del sello	Sí	Sí
Fecha de inicio del sello	1997	2007
Destinatarios del sello	Entidades privadas y ámbito educativo (padres y profesores	Entidades públicas y privadas. Productos de tecnologías de la información
Ámbito normativo	Puerto Seguro y COPPA	Puerto Seguro y COPPA
Directorio de entidades que cuentan con sello	Sí	Sí
Dirección de Internet	www.truste.com	www.european-privacy-seal.eu

Principales normas estadunidenses en privacidad

TÍTULO	OBJETO DE LA NORMA
Title V of the Gramm-Leach-Bliley Act (GLBA)	Establece condiciones para la cesión por entidades financieras de información financiera de consumidores a terceras entidades no filiadas. A tal fin tienen que informar a los consumidores sobre sus prácticas de recogida y cesión de datos. También están obligadas a proporcionar a los consumidores la posibilidad de oponerse (opt-out) a la cesión de sus datos.
The Children's Online Privacy Protection Act (COPPA)	Protege la recogida de datos personales de menores de 13 años por medios electrónicos. Se aplica a los operadores de sitios web comerciales que estén dirigidos a menores de 13 años o si el operador conoce que está obteniendo información de menores de 13 años. El tratamiento de datos de menores de 13 años requiere informar a los padres y obtener su consentimiento.
Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act)	Tipifica como crimen federal la transmisión o uso intencionado, "sin autoridad legal, de los datos de identificación de otra persona con la finalidad de cometer, ayudar o auxiliar en, una actividad ilícita que constituya la violación de una ley federal o que constituya delito conforme a cualquier ley estatal o local aplicable".
The Health Insurance Portability and Accountability Act of 1996	Establece estándares para proteger la privacidad de los datos de salud. Se aplica a planes y centros de salud, y proveedores de servicios médicos que transmitan información por medios electrónicos. Las entidades sujetas tienen que informar a los interesados sobre los usos y cesiones de sus datos, obtener el consentimiento para poderlos tratar y ceder, y proporcionar acceso a los datos que son objeto de tratamiento.
The Cable Communications Policy Act of 1984	Impone a los operadores de cable la obligación de informar y obtener el consentimiento de los consumidores para poder tratar sus datos. El consentimiento es exigible para comunicar datos a terceros, salvo orden judicial o el cumplimiento de los servicios contratados. Los abonados tienen el derecho de acceso y rectificación de sus datos.
The Fair Credit Reporting Act (FCRA)	Aplica a los burós de créditos y permite la cesión de información crediticia únicamente a entidades que tengan finalidades adecuadas. Establece el derecho de los consumidores a acceder y rectificar la información en los informes de crédito.
The Federal Videotape Privacy Protection Act	Obliga a las entidades que se dedican a la venta o alquiler de vídeos a obtener el consentimiento de los clientes para poder ceder sus datos personales. Sólo podrán facilitar listas de consumidores que incluyan nombres y direcciones si se les ha ofrecido previamente la opción de ser excluidos (opt-out) de dicho listado.

Principales normas estadunidenses en privacidad (cont.)

REFERENCIA LEGAL	AUTORIDAD	SANCIONES
15 U.S.C. § 6801, et seq.	FTC	Dependerá de cada caso atendiendo a quién sea la autoridad competente.
15 U.S.C. § 6501, et seq.	FTC	15 U.S.C. 41 et seq.
18 U.S.C. § 1028, 1028(a)(7)	Autoridad competente en cada caso.	1 año de cárcel cuando lo obtenido tenga un valor acumulado igual o superior a 1000 dólares
42 U.S.C. § 1320d, et seq.	Oficina de Derechos Civiles del Ministerio de Salud y Servicios Humanos (Office of Civil Rights, U.S. Department of Health & Human Services)	Sanciones civiles y penales que pueden llegar hasta 1 500 000 dólares
47 U.S.C. § 551	Acción civil ante los Tribunales de Distrito de los Estados Unidos.	1. Daño emergente que no sea inferior al daño asegurado a razón de 100 dólares por cada día de infracción o 1000 dólares, cualquiera que sea la cantidad superior. 2. Lucro cesante. 3. Costas de abogado y otras costes de litigio razonables.
15 U.S.C. § 1681, et seq.	FTC, limitada a algunas entidades financieras.	—
18 U.S.C. § 2710	Acción civil ante los Tribunales de Distrito de los Estados Unidos.	1. Daño emergente que no sea inferior al daño asegurado a razón de 2500 dólares. 2. Lucro cesante. 3. Costas de abogado y otras costes de litigio razonables. 4. Otra compensación que el tribunal estime adecuado para reparar el daño

Segunda Parte
NORMATIVIDAD INTERNACIONAL Y NACIONAL

Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid

Presentación

Es para mí un placer presentar la Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid.

La labor conjunta de los garantes de la privacidad de casi cincuenta países, bajo coordinación de la Agencia Española de Protección de Datos, ha desembocado en un texto que trata de plasmar los múltiples enfoques que admite la protección de este derecho, integrando legislaciones de los cinco continentes. Su carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado, enfatiza la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información.

Desde este momento, las autoridades de supervisión y control de la privacidad asumimos la exigente tarea de difusión y promoción desde nuestro firme compromiso de garantizar a nuestros ciudadanos una mejor protección de la privacidad y de los datos de carácter personal.

Artemi Rallo Lombarte
Director de la Agencia Española de Protección de Datos

Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal.[1]

Parte I: disposiciones generales

1.Objeto

El objeto del presente Documento es:

a. Definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal; y

b. Facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado.

2. Definiciones

En el contexto del presente Documento, se entenderá por:

a. "Dato de carácter personal": cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados.

b. "Tratamiento": cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.

c. "Interesado": persona física cuyos datos de carácter personal sean objeto de tratamiento.

d. "Persona responsable": persona física o jurídica, de naturaleza pública o privada que, sola o en compañía de otros, decida sobre el tratamiento.

e. "Prestador de servicios de tratamiento": persona física o jurídica, distinta de la persona responsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable.de carácter personal.

3. Ámbito de aplicación

1. El presente Documento está dirigido a su aplicación a todo tratamiento de datos de carácter personal, total o parcialmente automatizado, o realizado de forma estructurada en caso contrario, llevado a cabo tanto por el sector público como por el privado.

2. La legislación nacional aplicable podrá establecer que las disposiciones del presente Documento no sean de aplicación al tratamiento de datos de carácter personal realizado por una persona física en el ejercicio de actividades relacionadas exclusivamente con su vida privada y familiar.

4. Medidas adicionales

1. Los Estados podrán completar el nivel de protección definido en el presente Documento con otras medidas adicionales que garanticen una mejor protección de la privacidad en relación con el tratamiento de datos de carácter personal.

2. Las disposiciones del presente Documento constituirán base apropiada para permitir las transferencias internacionales de datos de carácter personal, cuando éstas se realicen según lo indicado en el apartado 15 del presente Documento.

5. Excepciones

Los Estados podrán limitar el alcance de las disposiciones recogidas en los apartados 7 a 10 y 16 a 18 del presente Documento cuando sea necesario, en una sociedad democrática, para preservar la seguridad nacional, la seguridad pública, la protección de la salud pública, o la protección de los derechos y las libertades de los demás. Tales limitaciones deberán estar expresamente previstas por el derecho interno, de tal modo que se establezcan sus límites y se prevean las garantías adecuadas para preservar los derechos de los interesados.

Parte II: principios básicos

6. Principio de Lealtad y Legalidad

1. Los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el presente Documento y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

2. En particular, se considerarán desleales aquellos tratamientos de datos de carácter personal que den lugar a una discriminación injusta o arbitraria contra los interesados.

7. Principio de Lealtad y legalidad

1. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable.

2. La persona responsable se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

8. Principio de proporcionalidad

1. El tratamiento de datos de carácter personal deberá circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior.

2. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario.

9. Principio de calidad

1. La persona responsable deberá asegurar en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados.

2. La persona responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.

10. Principio de Transparencia

1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.

2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.cionado [sic] a la persona responsable.

4. Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

11. Principio de Responsabilidad.
La persona responsable deberá:

a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y

b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.

Parte III. Legitimación para el tratamiento

12. Principio general de legitimación.
Como regla general, los datos de carácter personal sólo podrán ser tratados cuando concurra alguno de los siguientes supuestos:

a. Previa obtención del consentimiento libre, inequívoco e informado del interesado.

b. Cuando un interés legítimo de la persona responsable justifique el tratamiento, siempre y cuando no prevalezcan los intereses legítimos, derechos o libertades de los interesados;

c. Cuando el tratamiento sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el interesado;

d. Cuando el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable, o sea llevado a cabo por una Administración Pública que así lo precise para el legítimo ejercicio de sus competencias;

e. Cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona.

2. La persona responsable deberá habilitar procedimientos sencillos, ágiles y eficaces que permitan a los interesados revocar su consentimiento en cualquier momento, y que no impliquen demoras o costes indebidos, ni ingreso alguno para la persona responsable.

13. Datos sensibles
1. Serán considerados sensibles aquellos datos de carácter personal:
   a. Que afecten a la esfera más íntima del interesado; o
   b. Cuya utilización indebida pueda:
      i.Dar origen a una discriminación ilegal o arbitraria, o
      ii Conllevar un riesgo grave para el interesado.

2. En particular, serán considerados sensibles aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a la sexualidad. La legislación nacional aplicable podrá establecer otras categorías de datos sensibles en caso de que concurran las circunstancias a las que se refiere el párrafo anterior.
3. La legislación nacional aplicable deberá establecer las garantías necesarias para preservar los derechos de los interesados, que deberán fijar condiciones adicionales para el tratamiento de datos de carácter personal considerados sensibles.

14. Prestación de servicios de tratamiento
La persona responsable podrá realizar tratamientos de datos de carácter personal a través de uno o varios prestadores de servicios de tratamiento, debiendo para ello:
   a. Velar por que cada prestador de servicios de tratamiento garantice, al menos, el nivel de protección previsto en el presente Documento y en la legislación nacional aplicable; y
   b. Articular la relación jurídica a través de un contrato u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido, y que establezca el compromiso del prestador de servicios de tratamiento de cumplir con estas garantías y de asegurar que los datos de carácter personal sean tratados siguiendo las instrucciones de la persona responsable.

15. Transferencias Internacionales
1. Como regla general, podrán realizarse transferencias internacionales de datos de carácter personal cuando el Estado al que se transfieran dichos datos ofrezca, cuando menos, el nivel de protección previsto en el presente Documento.
2. Será posible realizar transferencias internacionales de datos de carácter personal a Estados que no ofrezcan el nivel de protección previsto en el presente Documento, cuando quien pretenda transferir dichos datos garantice que el destinatario ofrecerá dicho nivel de protección; dicha garantía podrá derivarse, por ejemplo, de cláusulas contractuales apropiadas. En particular, cuando la transferencia se lleve a cabo en el seno de organiza-

ciones o de grupos multinacionales, dicha garantía podrán consistir en la existencia de normas internas de privacidad cuya observancia resulte vinculante.
3. Asimismo, cuando sea necesario en el marco de una relación contractual en beneficio del interesado, o para proteger un interés vital del interesado o de otra persona, o para el cumplimiento de una obligación legal para la salvaguarda de un importante interés público, la legislación nacional aplicable a quien pretenda transferir datos de carácter personal podrá permitir la transferencia internacional de datos de carácter personal a Estados que no ofrezcan el nivel de protección previsto en el presente Documento.
4. La legislación nacional aplicable podrá atribuir a las autoridades de supervisión previstas en el apartado 23 la facultad de autorizar, con carácter previo a su realización, todas o algunas de las transferencias internacionales de datos de carácter personal originadas en su jurisdicción. En todo caso, quien pretenda realizar una transferencia internacional de datos de carácter personal deberá poder acreditar que la transferencia cumple las garantías establecidas en el presente Documento, y en particular cuando así le fuera requerido por las autoridades de supervisión en cumplimiento de las facultades previstas en el apartado 23.2.

Parte IV: Derechos del interesado

16. Derecho de acceso
1. El interesado tendrá derecho a recabar de la persona responsable, cuando así lo solicite, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quienes se comuniquen o pretendan comunicar dichos datos.
2. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo.
3. La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo.

17. Derecho de rectificación y cancelación
1. El interesado tendrá derecho a solicitar a la persona responsable la rectificación o cancelación de los datos de carácter personal que pudieran resultar incompletos, inexactos, innecesarios o excesivos.
2. Cuando proceda, la persona responsable rectificará o cancelará los datos de carácter personal conforme a lo solicitado. Deberá, además, notificar este extremo a los terceros

a quienes se hayan comunicado los datos de carácter personal, siempre que los mismos fueran conocidos.
3. La cancelación no procederá cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable o, en su caso, por las relaciones contractuales entre la persona responsable y el interesado.

18. Derecho de oposición
1. El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.
2. No procederá el ejercicio de este derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.
3. Cualquier interesado podrá oponerse, igualmente, a aquellas decisiones que conlleven efectos jurídicos basadas únicamente en un tratamiento automatizado de datos de carácter personal, excepto cuando la decisión hubiese sido expresamente solicitada por el interesado o sea precisa para el establecimiento, mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el propio interesado. En este último caso, el interesado debe tener la posibilidad de hacer valer su punto de vista, a fin de defender su derecho o interés.

19. Ejercicio de estos derechos
1. Los derechos previstos en los apartados 16 a 18 del presente Documento podrán ser ejercidos:
   a. Directamente por el interesado, que deberá acreditar adecuadamente su identidad ante la persona responsable.
   b. Por medio de representante, que deberá acreditar adecuadamente tal condición ante la persona responsable.

2. La persona responsable deberá implementar procedimientos que permitan a los interesados ejercer los derechos previstos en los apartados 16 a 18 del presente documento de forma sencilla, ágil y eficaz, y que no conlleven demoras o costes indebidos, ni ingreso alguno para la persona responsable.
3. Cuando la persona responsable aprecie que, de acuerdo con la legislación nacional aplicable, no procede el ejercicio de los derechos previstos en la presente Parte, informará cumplidamente al interesado de los motivos que concurran en su apreciación.

Parte V: Seguridad

20. Derecho de oposición

1. Tanto la persona responsable como los prestadores de servicios de tratamiento deberán proteger los datos de carácter personal que sometan a tratamiento mediante aquellas medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad. Tales medidas dependerán del riesgo existente, de sus posibles consecuencias para los interesados, del carácter especialmente sensible de los datos de carácter personal, del estado de la técnica y del contexto en el que se efectúe el tratamiento, así como de las obligaciones establecidas en la legislación nacional aplicable.

2. Los interesados deberán ser informados por parte de quienes intervengan en cualquier fase del tratamiento de cualquier infracción de seguridad que pudiese afectar de forma significativa a sus derechos patrimoniales o extrapatrimoniales, así como de las medidas adoptadas para su resolución. Esta información deberá ser facilitada con antelación suficiente, para permitir la reacción de los interesados en defensa de sus derechos.

21. Deber de confidencialidad.

La persona responsable y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado o, en su caso, con la persona responsable.

Parte VI: Cumplimiento y supervisión

22. Medidas proactivas

Los Estados incentivarán, a través de su derecho interno, el establecimiento por quienes intervengan en cualquier fase del tratamiento de medidas que promuevan el mejor cumplimiento de la legislación que resulte aplicable en materia de protección de datos. Entre dichas medidas podrán encontrarse, entre otras:

a. El establecimiento de procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información.

b. La designación, de uno o varios oficiales de privacidad o de protección de datos, con cualificación, recursos y competencias suficientes para ejercer adecuadamente sus funciones de supervisión.

c. La realización periódica de programas de concienciación, educación y formación entre los miembros de la organización destinados al mejor conocimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto.
d. La realización periódica de auditorías transparentes por parte de sujetos cualificados y preferentemente independientes, que verifiquen el cumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, así como de los procedimientos establecidos por la organización a tal efecto.
e. La adaptación de aquellos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal a la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, en particular al decidir acerca de sus especificaciones técnicas y en su desarrollo e implementación.
f. La puesta en práctica de estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal, así como a la puesta en práctica de nuevas modalidades de tratamiento de datos de carácter personal o a la realización de modificaciones sustanciales en tratamientos ya existentes.
g. La adhesión a acuerdos de autorregulación cuya observancia resulte vinculante, que contengan elementos que permitan medir sus niveles de eficacia en cuanto al cumplimiento y grado de protección de los datos de carácter personal, y establezcan medidas efectivas en caso de incumplimiento.
h. La implementación de planes de contingencias que establezca unas pautas de actuación en caso de que se verifique un incumplimiento de la legislación que resulte aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal, y que incluya al menos la obligación de determinar la causa y alcance de la vulneración que se haya producido, de describir sus efectos negativos y de adoptar las medidas necesarias para evitar que se reproduzca en el futuro.

23. Supervisión
1. En cada Estado existirán una o más o autoridades de supervisión que, de acuerdo con su derecho interno, serán responsables de supervisar la observancia de los principios establecidos en el presente Documento.
2. Dichas autoridades de supervisión deberán ser imparciales e independientes, y contarán con la cualificación técnica, las competencias suficientes y los recursos adecua-

dos para conocer de las reclamaciones que le sean dirigidas por los interesados, y para realizar las investigaciones e intervenciones que resulten necesarias para garantizar el cumplimiento de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.
3. En todo caso, y sin perjuicio de los recursos administrativos ante las citadas autoridades de supervisión, incluyendo el control jurisdiccional de sus decisiones, el interesado podrá acudir directamente a la vía jurisdiccional para hacer valer sus derechos conforme a las previsiones establecidas en la legislación nacional aplicable.

24. Cooperación y coordinación
1. Las autoridades de supervisión previstas en el apartado anterior procurarán cooperar entre sí en aras a una más uniforme protección de la privacidad en relación con el tratamiento de datos de carácter personal, tanto a nivel nacional como internacional. A los efectos de facilitar esta cooperación, los Estados deberán estar en disposición en todo momento de identificar las autoridades de supervisión competentes en su territorio.
2. Dichas autoridades realizarán, particularmente, los mayores esfuerzos para:

a. Compartir estudios, técnicas de investigación, estrategias comunicativas y de regulación y demás información que resulte de utilidad para el más eficaz ejercicio de sus funciones, en especial tras recibir una petición de apoyo por parte de otra autoridad de supervisión en el marco de una investigación o intervención;

b. Realizar investigaciones o intervenciones coordinadas, tanto a nivel nacional como internacional, en asuntos en los que concurra el interés de dos o más autoridades de supervisión;

c. Participar en asociaciones, grupos de trabajo y foros conjuntos, así como en seminarios, talleres o cursos que contribuyan a adoptar posturas comunes o a mejorar la cualificación técnica del personal que preste sus servicios a dichas autoridades de supervisión;

d. Mantener los niveles apropiados de confidencialidad con respecto a la información intercambiada en el curso de esta cooperación.

3. Los Estados impulsarán la creación de convenios de colaboración entre autoridades de supervisión, tanto regionales como nacionales o internacionales, que contribuyan a una más eficaz observancia del presente apartado.

25. Responsabilidad
1. La persona responsable será responsable de aquellos daños y/o perjuicios, tanto morales como materiales, que hubiesen causado a los interesados como consecuencia de un tratamiento de datos de carácter personal que hubiese vulnerado la legislación aplicable en materia protección de datos, a menos que pueda demostrar que el daño no le puede

ser atribuido. Ello sin perjuicio de cualquier acción que la persona responsable pueda ejercer contra los prestadores de servicios de tratamiento que intervengan en cualquier fase del tratamiento.
2. Los Estados promoverán las medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos, judiciales o administrativos, que les permitan obtener la reparación de los daños y/o perjuicios anteriormente mencionados.
3. La responsabilidad prevista en los párrafos anteriores existirá sin perjuicio de las sanciones penales, civiles o administrativas previstas, en su caso, por violación de la legislación nacional aplicable en materia de protección de la privacidad en relación con el tratamiento de datos de carácter personal.
4. La adopción de medidas proactivas como las previstas en el apartado 22 del presente Documento será tenida en cuenta al fijar la responsabilidad y las sanciones previstas en el presente apartado.

Resolución sobre Estándares Internacionales de Privacidad

Proponentes:

Agencia Española de Protección de Datos
Comisario Federal de Protección de Datos y la transparencia (Suiza)
Supervisor Europeo de Protección de Datos
Comisión Nacional de la Informática y de las Libertades (Francia)
Comisario de Protección de Datos de Irlanda
Oficina del Comisario de Privacidad de Canadá
Oficina para la Protección de los Datos Personales (República Checa)
Comisario Federal para la Protección de Datos (Alemania)
Garante para la Protección de Datos Personales (Italia)
Autoridad Holandesa de Protección de Datos
Comisario de Privacidad de Nueva Zelanda
Oficina del Comisario de Información (Reino Unido)

Coproponentes:

Agencia de Protección de Datos de Andorra
Agencia Catalana de Protección de Datos
Agencia de Protección de Datos de la Comunidad de Madrid

Agencia Vasca de Protección de Datos
Oficina del Supervisor de Protección de Datos la Isla de Man
Inspección de Protección de Datos de Estonia
Inspección Estatal de Protección de Datos (Lituania)
Comisario para la Protección de Datos de Berlín (Alemania)
Comisario de Protección de Datos de Schleswig-Holstein (Alemania)
Director Nacional de Protección de Datos Personales (Argentina)
Comisario de Protección de Datos (Malta)
Comisión de la Informática y las Libertades (Burkina-Faso)
Comisario de Protección de Datos Personales (Chipre)
Defensor de la Protección de Datos (Finlandia)
Comisario de Información (Eslovenia
Autoridad Griega de Protección de Datos

Teniendo en cuenta que:

La 30ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad adoptó en Estrasburgo unánimemente la Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales.

La resolución estableció el mandato de crear un Grupo de Trabajo, bajo coordinación de la Agencia Española de Protección de Datos, como Autoridad organizadora de la 31ª Conferencia Internacional y con la participación de las Autoridades de protección de datos interesadas en ello, con el objetivo de elaborar una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal.

En consonancia con este mandato, la Agencia Española de Protección de Datos estableció un Grupo de Trabajo, promoviendo y coordinando los trabajos para la elaboración de una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal.

El Grupo de Trabajo redactó la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal, partiendo de los principios que resultan comunes a los diferentes textos legales, directrices o recomendaciones de alcance internacional, que han recibido un amplio consenso en sus respectos ámbitos geográficos, económicos o legales de aplicación. La Propuesta Conjunta se ha elaborado asumiendo que todos estos principios y enfoques comunes aportan elementos valiosos en la defensa y promoción de la privacidad y la información

personal, con el objetivo de expandir ese conjunto de principios y criterios comunes incorporando soluciones y previsiones específicas que resulten aplicables con independencia de las diferencias que pueden subsistir entre los diferentes modelos de protección de datos y privacidad existentes.

De acuerdo a esto, la Conferencia resuelve:

1. Acoge con satisfacción la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal que acompaña como Anexo 1 a esta Resolución. La Propuesta Conjunta demuestra la viabilidad de tales estándares, como un nuevo paso hacia la elaboración, en el momento oportuno, de un instrumento internacional vinculante.
2. Afirma que la Propuesta Conjunta ofrece un conjunto de principios, derechos, obligaciones y procedimientos que cualquier sistema jurídico de protección de datos y privacidad debe esforzarse por alcanzar. De este modo, el tratamiento de datos personales en el sector público y privado se llevaría a cabo, a través de un enfoque más uniforme a nivel internacional:
   a. de manera leal, lícita, y proporcionada en relación con finalidades determinadas, explícitas y legítimas.
   b. sobre la base de políticas transparentes, informando adecuadamente a los interesados y sin ninguna discriminación arbitraria en su contra.
   c. garantizando la exactitud, la confidencialidad y la seguridad de los datos, así como la legitimidad del tratamiento, y los derechos de los afectados a acceder, rectificar y cancelar los datos, así como a oponerse a un determinado tratamiento.
   d. aplicando el principio de responsabilidad, incluyendo la responsabilidad por daños, incluso si las operaciones de tratamiento se llevan a cabo por prestadores de servicios que actúen por cuenta del responsable.
   e. ofreciendo garantías más adecuadas cuando los datos son sensibles.
   f. garantizando que los datos personales transferidos internacionalmente se benefician del nivel de protección previsto en el mencionado conjunto de estándares.
   g. sometiendo el tratamiento a la vigilancia de autoridades de supervisión, independientes e imparciales, con poderes y recursos adecuados, y sometidas a un deber de cooperación entre sí.
   h. en un marco nuevo y moderno de medidas proactivas, orientadas en particular a prevenir y detectar infracciones y basadas en la designación de oficiales de privacidad, así como en auditorias eficaces y en evaluaciones de impacto de privacidad.

3. Instar a las Autoridades de Protección de Datos y Privacidad acreditadas ante la Con-

ferencia Internacional a dar la máxima difusión a la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal.

4. Encomendar a las Autoridades organizadoras de la 31ª y 32ª Conferencias Internacionales la coordinación de un Grupo de Contacto, integrado por las Autoridades de Protección de Datos y Privacidad que así lo deseen, que se encargará de:

   a. la promoción y difusión de Propuesta Conjunta entre entidades privadas, expertos y organismos públicos nacionales e internacionales como base para un futuro trabajo para la elaboración de un Convenio universal vinculante, y en particular entre las instituciones y organizaciones mencionadas en la Declaración de Montreux; y

   b. explorar e informar sobre otras formas en que la propuesta conjunta podría utilizarse como base para el desarrollo de la comprensión y la cooperación internacionales sobre protección de datos y la privacidad, particularmente en el contexto de permitir las transferencias internacionales de datos personales, que tendrán lugar de un modo que proteja los derechos y libertades de los individuos.

5. Solicitar al Grupo de Contacto:

   a. coordinar su labor con el Grupo director sobre la representación en reuniones de organizaciones internacionales, eb. informar de cualquier avance relevante a la 32ª Conferencia Internacional, para garantizar una atención continua al tema de la presente resolución.

Nota explicativa

La 30ª Conferencia Internacional de Autoridades Protección de Datos y Privacidad adoptó la Resolución relativa a la urgente necesidad de proteger la privacidad de estándares internacionales sobre privacidad y protección de datos personales, presentada conjuntamente por las autoridades de protección de datos de Suiza y España y respaldada por otras veinte autoridades.

En esta Resolución, la Conferencia recuerda que diversas Declaraciones y Resoluciones adoptadas durante los últimos diez años tienen por objeto reforzar el carácter universal del derecho a la protección de datos de carácter personal y de la privacidad, y realizan un llamamiento para el desarrollo de un convenio universal para la protección de las personas con respecto al tratamiento de datos personales.

Además, la Resolución indica que la Conferencia Internacional considera el derecho a la protección de datos y a la privacidad como un derecho fundamental de las personas, con independencia de su nacionalidad o residencia, al tiempo que constata que las diferencias persistentes en materia de protección de datos y respeto de la privacidad en

el mundo, y especialmente debido al hecho de que muchos Estados no han aprobado todavía leyes adecuadas, perjudican los intercambios de datos personales y la puesta en práctica de una protección de datos efectiva y global.

Por ello, la Resolución expresa la convicción de la Conferencia de que el reconocimiento de estos derechos pasa por la adopción de un instrumento legislativo universal y vinculante, que haga uso, consagre, y complemente los principios comunes de protección de datos y de respeto a la privacidad enunciados en los diferentes instrumentos existentes, y que refuerce la cooperación internacional entre autoridades de protección de datos. En ese sentido, la Resolución expresa el apoyo de la Conferencia Internacional a los esfuerzos del Consejo de Europa para impulsar los derechos fundamentales a la protección de datos y a la privacidad e invita a los Estados, sean o no miembros de la organización, a ratificar el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional, al tiempo que confirma su apoyo a las acciones llevadas a cabo por APEC, la OCDE y otros foros regionales e internacionales con vistas a desarrollar herramientas efectivas que fomenten unos mejores estándares internacionales de privacidad y protección de datos.

La Resolución mandató a la Agencia Española de Protección de Datos, como Autoridad organizadora de la 31ª Conferencia Internacional, a crear un Grupo de Trabajo compuesto por las autoridades de protección de datos interesadas, con el objetivo de elaborar y presentar una Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal.

La Resolución incluye una lista de criterios que deben presidir el proceso de elaboración de esta Propuesta Conjunta y, en particular, que debe desarrollarse fomentando una amplia participación de entidades y organizaciones tanto públicas como privadas, con el fin de lograr el más amplio consenso institucional y social.

De acuerdo con este mandato, la Agencia Española de Protección de Datos estableció el Grupo de Trabajo a que se refiere la Resolución y ha promovido y coordinado los trabajos destinados a la elaboración de una la Propuesta Conjunta para la Redacción de Estándares Internacionales.

La Agencia Española de Protección de Datos dirigió invitaciones a participar en el Grupo de Trabajo a todas las Autoridades de Protección de Datos y Privacidad acreditadas ante la Conferencia Internacional. Las Autoridades mencionadas en el Anexo 2* manifestaron su voluntad de formar parte de este grupo de trabajo y consecuentemente se unieron.

El Grupo de Trabajo se ha reunido en los meses de Enero y Junio de 2009. La primera de estas reuniones acordó la metodología de redacción de la Propuesta Conjunta y el alcance material de su contenido, en tanto que la segunda debatió una versión avanzada de borrador de propuesta con vistas a su posterior remisión a la 31ª Conferencia Inter-

nacional. Según los criterios y metodología expuestos por la Resolución de Estrasburgo y acordados por el Grupo de Trabajo, la Agencia Española de Protección de Datos ha llevado a cabo una intensa actividad, elaborando sucesivos documentos de trabajo en cuya redacción se han incorporado las contribuciones de Autoridades de Protección de Datos y Privacidad y otras entidades públicas relacionadas con la protección de datos, así como de expertos procedentes de empresas, la profesión jurídica, el mundo académico y organizaciones internacionales y no gubernamentales.

En particular, el Grupo de Trabajo ha elaborado la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con Tratamiento de Datos de Carácter Personal que resultan comunes a los diferentes texto legales, directrices o recomendaciones de alcance internacional que han recibido un amplio consenso en sus respectos ámbitos geográficos, económicos o legales de aplicación.

La Propuesta Conjunta se ha elaborado asumiendo que todos estos principios y enfoques comunes aportan elementos de valor en la defensa y la mejora de la privacidad e información personal, con el objetivo de ampliarlos mediante soluciones y disposiciones específicas que podrían aplicarse independientemente de las diferencias que puedan existir entre los diferentes modelos existentes de protección de datos y privacidad.

Autoridades que conformaron el grupo de trabajo

COMISARIO FEDERAL DE PROTECCIÓN DE DATOS (Alemania), COMISARIO DE PROTECCIÓN DE DATOS Y LIBERTAD DE INFORMACIÓN DE BERLÍN (Alemania), COMISARIO DE PROTECCIÓN DE DATOS DE SCHLESWIG-HOLSTEIN (Alemania), COMISIÓN DE PROTECCIÓN DE DATOS (Austria), COMISIÓN DE PROTECCIÓN DE LA PRIVACIDAD (Bélgica), COMISIÓN DE LA INFORMÁTICA Y LAS LIBERTADES (Burkina-Fasso), COMISARIO DE PRIVACIDAD (Canadá), COMISARIO DE ACCESO A LA INFORMACIÓN (Canadá), SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, COMISARIO DE INFORMACIÓN (Eslovenia), AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (España), AGENCIA CATALANA DE PROTECCIÓN DE DATOS (España), AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID (España), AGENCIA VASCA DE PROTECCIÓN DE DATOS (España), COMISIÓN NACIONAL DE LA INFORMÁTICA Y LAS LIBERTADES (Francia), COMISARIO DE PRIVACIDAD PARA LA PROTECCIÓN DE DATOS (Hong Kong), COMISARIO DE PROTECCIÓN DE DATOS (Irlanda), GARANTE PARA LA PROTECCIÓN DE LOS DATOS PERSONALES (Italia), COMISARIO DE PRIVACIDAD (Nueva Zelanda), COMISIÓN DE PROTECCIÓN DE DATOS (Países Bajos), COMISIÓN NACIONAL DE PROTECCIÓN DE DATOS (Portugal), COMISARIO DE INFORMACIÓN (Reino Unido), OFICINA PARA LA PROTECCIÓN DE DATOS PERSONALES (República Checa), COMISARIO FEDERAL DE PROTECCIÓN DE DATOS (Suiza)

Notas

Para una mayor información sobre el desarrollo de los trabajos preparatorios de este documento, puede visitarse la página web de la Agencia Española de Protección de Datos, www.agpd.es, donde puede encontrarse un Memorándum explicativo y otra documentación de interés.

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales

Prólogo

El desarrollo del tratamiento automático de datos, que permite la transmisión de enormes cantidades de ellos en segundos a través de las fronteras nacionales y, naturalmente, a través de los continentes, ha hecho que sea necesario considerar la protección de la intimidad en relación a los datos personales. Se ha introducido, o se van a introducir en breve, legislación para la protección de la intimidad en aproximadamente la mitad de los países miembro de la OCDE (Austria, Canadá, Dinamarca, Francia, Alemania, Luxemburgo, Noruega, Suecia y los Estados Unidos han aprobado legislación; Bélgica, Islandia, Países Bajos, España y Suiza han elaborado proyectos de ley) para impedir lo que se considera que son vulneraciones de derechos humanos fundamentales, tales como el almacenamiento ilícito de datos personales, exactos o inexactos, o el abuso o la revelación no autorizada de los mismos.

Por otra parte, existe el peligro de que las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de datos personales; circulación que se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones. Las restricciones a esta circulación podrían ocasionar graves trastornos en importantes sectores de la economía, tales como la banca y los seguros.

Por este motivo, los países miembro de la OCDE han considerado necesario elaborar Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos. Representan un consenso sobre principios básicos que pueden incorporarse a la legislación nacional existente o servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella.

Las Directrices, en forma de Recomendación del Consejo de la OCDE, fueron elaboradas por un grupo de expertos gubernamentales, bajo la presidencia de Su Señoría el Magistrado M. D. Kirby, presidente de la Comisión Australiana de Reforma Legislativa. La Recomendación fue adoptada y entró en vigor el 23 de septiembre de 1980.

Las Directrices van acompañadas de un Memorándum Explicativo, con la finalidad de proporcionar información acerca del debate y de los razonamientos que subyacen en su planteamiento.

Recomendación del consejo relativa a las directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales (23 de septiembre de 1980)

EL CONSEJO,
Considerando los artículos 1(c), 3(a) y 5(b) del Convenio sobre la Organización para la Cooperación y Desarrollo Económicos de 14 de diciembre de 1960;
RECONOCIENDO:
que, si bien pueden variar las legislaciones y políticas nacionales, los países miembro tienen un interés común en proteger la intimidad y las libertades individuales, y en reconciliar los valores fundamentales en oposición, tales como la intimidad y la libre circulación de información;
que el tratamiento automático y la circulación transfronteriza de datos personales crean nuevas formas de relación entre los países y precisan la elaboración de normas y prácticas compatibles;
que la circulación transfronteriza de datos personales contribuye al desarrollo económico y social;
que la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza;
RESUELTO
a fomentar la libre circulación de información entre los países miembro y a evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembro;

RECOMIENDA
1. Que los países miembro tengan en cuenta en su legislación nacional los principios relativos a la protección de la intimidad y de las libertades individuales expuestos en las Directrices que se contienen en el Anejo a esta Recomendación, que forma parte integrante de las mismas.
2. Que los países miembro procuren retirar o evitar la creación, en aras de la protección de la intimidad, los obstáculos injustificados a la circulación transfronteriza de datos personales;

3. Que los países miembro cooperen en la implantación de las Directrices expuestas en el Anejo, y
4. Que los países miembro lleguen a un acuerdo, en cuanto sea posible, respecto a los procedimientos concretos de consulta y cooperación para la aplicación de estas Directrices.

Anejo a la Recomendación del Consejo de 23 de septiembre de 1980 .
Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales

Primera parte. Generalidades

Definiciones

1. A los efectos de estas Directrices:
   a) por "controlador de datos" se entenderá la parte que, conforme a la legislación nacional, sea competente para decidir acerca del contenido y la utilización de los datos personales, con independencia de si tales datos se recogen, almacenan, tratan o se divulgan por dicha parte o por un mandatario en nombre suyo;
   b) por "datos personales" se entenderá toda información correspondiente a una persona identificada o identificable (el sujeto de los datos), y
   c) por "circulación transfronteriza de datos personales" se entenderá los movimientos de datos personales a través de fronteras nacionales.

Ámbito de las Directrices

2. Estas Directrices son de aplicación a los datos personales, tanto del sector público como del privado, que, a causa de la manera en que hayan sido tratados, o por su índole o por el contexto en el cual se utilicen, presenten un peligro para la intimidad y las libertades individuales.
3. Estas Directrices no debieran interpretarse en el sentido de que impiden:
   a) la aplicación, a diferentes categorías de datos personales, de distintas medidas de protección según su índole y el contexto en el cual se recojan, almacenen, traten o divulguen;
   b) la exclusión, respecto a la aplicación de las Directrices, de datos personales que evidentemente no contienen ningún riesgo para la intimidad ni para las libertades individuales, o
   c) la aplicación de las Directrices sólo al tratamiento automático de datos personales.

4. Las excepciones a los Principios que se contienen en las Partes II y III de estas Directrices, incluso las correspondientes a la soberanía y seguridad nacionales y al orden público, deberían:

a) ser tan escasas como sea posible, y
b) darse a conocer al público.

5. En el caso particular de los países federales, la observancia de estas Directrices puede verse afectada por la división de poderes dentro de la Federación.
6. Estas Directrices deberían considerarse como criterios mínimos susceptibles de suplementarse con medidas adicionales para la protección de la intimidad y las libertades individuales.

Segunda parte. Principios básicos de aplicación nacional

Principio de limitación de la recogida
7. Debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

Principio de calidad de los datos
8. Los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.

Principio de especificación de la finalidad
9. Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.

Principio de limitación de uso
10. Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo:

a) con el consentimiento del sujeto de los datos, o
b) por imperativo legal.

Principio de salvaguardas de seguridad
11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.

Principio de apertura
12. Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.

Principio de participación individual
13. La persona debería tener derecho a:

a) recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma;

b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;

c) que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, y

d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.

Principio de responsabilidad
14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

Tercera parte. Principios básicos de aplicación internacional: libre circulación y restricciones legítimas

15. Los países miembro deberían tomar en consideración las consecuencias implícitas para los demás países miembro del tratamiento nacional de los datos personales y de su reexportación.
16. Los países miembro deberían adoptar todas las medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura, de los datos personales, incluso el tránsito a través de algún país miembro.
17. La circulación transfronteriza de datos personales entre dos países miembro no debería restringirse, salvo en el caso de que el segundo país aún no haya observado sustancialmente estas Directrices o cuando la reexportación de tales datos soslayase su legislación nacional sobre la intimidad. Cualquier país miembro también podrá imponer restricciones respecto a ciertas categorías de datos personales para las cuales su legislación nacional sobre la intimidad incluya normativas específicas en vista de la índole de tales

datos y para las cuales otro país miembro no proporcione protección equivalente.
18. Los países miembro deberían evitar la elaboración de leyes, políticas y prácticas en aras de la protección de la intimidad y de las libertades individuales, que creen obstáculos a la circulación transfronteriza de datos personales que superarían las necesidades de tal protección.

Cuarta parte: Implantación nacional

19. Al implantar nacionalmente los principios expuestos en las Partes II y III, los países miembro deberían establecer procedimientos o instituciones jurídicas, administrativas u otras para la protección de la intimidad y de las libertades individuales respecto a los datos personales. Los países miembro deberían, en particular, procurar:

a) adoptar legislación nacional adecuada;
b) fomentar y apoyar la autorregulación, ya sea en forma de códigos de conducta o de otro modo;
c) prever medios razonables para que las personas ejerciten sus derechos;
d) prever las sanciones y recursos suficientes en caso de incumplimiento de las medidas con las cuales se implanten los principios expuestos en las Partes II y III, y
e) asegurar que no haya discriminación injusta contra los sujetos de los datos.

Quinta parte. Cooperación internacional

20. El país miembro, previa solicitud, deberían dar a conocer a los demás países miembro los detalles de la observancia de los principios expuestos en estas Directrices. Los países miembro deberían también asegurar que los procedimientos para la circulación transfronteriza de datos personales y para la protección de la intimidad y de las libertades individuales, sean sencillos y compatibles con los de los demás países miembro que cumplan estas Directrices.
21. Los países miembro deberían establecer procedimientos para facilitar:

1. el intercambio de información correspondiente a estas Directrices y ayuda mutua en las cuestiones de procedimiento e investigación implicadas.

22. Los países miembro deberían encaminarse hacia la elaboración de principios, nacionales e internacionales, que rijan el Derecho aplicable en el caso de circulación transfronteriza de datos personales.

Memorándum explicativo

Introducción

Una particularidad de los países miembro de la OCDE en el último decenio ha sido la elaboración de leyes para la protección de la intimidad, las cuales propenden a asumir diferentes formas en distintos países, y en muchos de ellos están todavía en vías de elaboración. Las disparidades en la legislación pueden crear obstáculos a la libre circulación de información entre los países. Tal circulación se ha incrementado en gran medida en los últimos años y seguramente seguirán creciendo a resultas de la introducción de nueva tecnología informática y de comunicaciones.

La OCDE, que viene desarrollando actividad en este campo desde hace algunos años, ha decidido afrontar los problemas de la legislación nacional divergente y en 1978 pasó instrucciones a un Grupo de Expertos para que elabore Directrices sobre normas básicas que rijan la circulación transfronteriza y la protección de datos personales y la intimidad, a fin de facilitar la armonización de la legislación nacional. El Grupo ya ha finalizado su labor.

Las Directrices son de índole amplia y recogen el debate y la labor legislativa que ha venido produciéndose durante varios años en los países miembro. El Grupo de Expertos, que elaboró las Directrices, ha considerado imprescindible publicar un Memorándum Explicativo anejo. Su finalidad es la de explicar y ampliar las Directrices y los problemas básicos de la protección de la intimidad y de las libertades individuales. Dirige la atención a cuestiones clave que han surgido en el debate de las Directrices y puntualiza los motivos de la elección de soluciones en particular.

En la primera parte del Memorándum se proporciona información general sobre los antecedentes en la esfera de interés que perciben los países miembro. En ella se explica la necesidad de intervención internacional y se resume la labor llevada a cabo, hasta ahora, por la OCDE y ciertos otros organismos internacionales. Concluye con una lista de los principales problemas con que se ha topado el Grupo de Expertos en su labor.

La Parte II tiene dos apartados. El primero de ellos contiene comentarios acerca de ciertas particularidades generales de las Directrices y en el segundo se dan comentarios detallados respecto a subapartados individuales.

Este Memorándum es un documento informativo, elaborado para explicar y describir en general la labor del Grupo de Expertos y está subordinado a las propias Directrices. No puede variar el sentido de las Directrices, pero se proporciona para ayudar en su interpretación y aplicación.

I. Antecedentes generales

Los problemas

1. El decenio de 1970-79 puede describirse como un período de actividades de investigación y legislación intensas concernientes a la protección de la intimidad respecto a la recogida y uso de datos personales. Numerosos informes oficiales indican que los problemas se toman en serio a nivel político y, al propio tiempo, que la tarea de equilibrar intereses contrapuestos es delicada y que es improbable que pueda conseguirse de una vez y para siempre. El interés público ha tendido a centrarse en los riesgos y resultados implícitos asociados al tratamiento informático de datos personales y algunos países han optado por promulgar leyes que traten exclusivamente de ordenadores y de actividades asistidas por los mismos. Otros países han preferido un planteamiento más general de las cuestiones de protección de la intimidad, con independencia de la determinada tecnología de tratamiento de datos implicada.

2. Los remedios en estudio son principalmente salvaguardas para la persona que impidan la invasión de su intimidad en el sentido clásico, esto es, abuso o revelación de sus datos personales íntimos, pero se han hecho evidentes otras necesidades de protección más o menos íntimamente relacionadas. Dos ejemplos al azar son las obligaciones que tienen los que llevan constancia escrita de informar al público en general acerca de las actividades que tienen que ver con el tratamiento de datos y los derechos de los sujetos de los mismos a hacer que se suplementen o modifiquen los datos que les correspondan. Hablando en general, viene habiendo una tendencia a ampliar el concepto tradicional de la intimidad ("el derecho a que le dejen a uno en paz") y a identificar una síntesis más compleja de intereses que quizá se puedan calificar más correctamente de intimidad y libertades individuales.

3. Por lo que se refiere a los problemas jurídicos del tratamiento automático de datos (TAD), la protección de la intimidad y de las libertades individuales constituye quizás el aspecto de debate que está más extendido. Entre los motivos de tal interés están el uso ubicuo de ordenadores para el tratamiento de datos personales, las posibilidades vastamente extendidas de almacenamiento, contrastación, vinculación, selección y acceso a los datos personales, y la combinación de la informática con la tecnología de telecomunicaciones, que puede poner los datos personales simultáneamente a disposición de miles de usuarios en lugares geográficamente dispersos y que permite reunir datos y la creación de redes complejas de datos nacionales e internacionales. Ciertos problemas requieren una atención urgente en particular, verbigracia, aquellos que corresponden a redes internacionales emergentes de datos, y a la necesidad de equilibrar por una parte los intereses contrapuestos de intimidad y de libertad de información por otra, a fin de permitir una plena explotación de las potencialidades de las modernas tecnologías de tratamiento de datos en la medida en que ello sea conveniente.

Actividades a escala nacional

4. Entre los países miembro de la OCDE más de un tercio han promulgado hasta ahora una o varias leyes que, entre otras cosas, están previstas para proteger a las personas frente al uso abusivo de los datos que a ellos se refieren y darles el derecho de acceso a los mismos con vistas a comprobar su exactitud e idoneidad. En los estados federales, la legislación de este género puede hallarse tanto a escala nacional como a la estatal o provincial. Tales leyes se denominan de distinta forma en diferentes países. Así, en la Europa continental en la práctica común se habla de "legislación sobre datos" o de "legislación de protección de datos" (lois sur la protection des données), mientras que en los países de habla inglesa se la conoce generalmente por "legislación de protección de la intimidad". La mayoría de las leyes se promulgaron después de 1973, y el período actual puede describirse como uno de actividad legislativa continuada o incluso ampliada. Los países que ya tienen leyes en vigor se dirigen a nuevas esferas de protección o se dedican a revisar o complementar las leyes existentes. Varios otros países están adentrándose en la cuestión y tienen proyectos de ley pendientes o están estudiando los problemas con miras a elaborar legislación. Estos esfuerzos nacionales, y en no menor medida los informes y comunicaciones de investigación extensos elaborados por comisiones públicas u órganos análogos, ayudan a esclarecer los problemas y las ventajas de las diversas soluciones y los resultados implícitos de las mismas. En la fase actual, proporcionan una base sólida para la intervención internacional.

5. Los planteamientos de la protección de la intimidad y de las libertades individuales adoptados por los diversos países tienen muchas particularidades en común. Así, es posible identificar ciertos intereses o valores básicos que de ordinario se considera que son componentes elementales de la esfera de protección. Algunos principios esenciales de este orden son: fijar límites a la recogida de datos personales de acuerdo con los objetivos de quien los recoge y criterios análogos, restricción del uso de datos para ajustarse a finalidades especificadas abiertamente; crear servicios para que las personas se enteren de la existencia y contenido de los datos y hacer que se corrijan, y la identificación de las partes que sean responsables del cumplimiento de las pertinentes normas y decisiones de protección de la intimidad. Hablando en general, con las leyes para proteger la intimidad y las libertades individuales en relación a los datos personales se intenta cubrir las fases sucesivas del ciclo que comienza con la recogida inicial de datos y que finaliza con la supresión u otra medida análoga, y asegurar en la mayor medida posible la concienciación, participación y control individuales.

6. Las diferencias entre los planteamientos nacionales según se desprende actualmente de la leyes, proyectos o proposiciones de ley, se refieren a aspectos tales como el ámbito de la legislación, el acento puesto en diferentes elementos de protección, la implantación detallada de los principios amplios indicados más arriba y los mecanismos para

la ejecución forzosa. Así, las opiniones varían respecto a los requisitos para la concesión de licencias y a los mecanismos de control en forma de órganos supervisores especiales ("autoridades de inspección de datos"). Las categorías de datos delicados se definen de distintas maneras, los medios para asegurar la apertura y la participación individual varían, por poner sólo unos casos. Desde luego, las diferencias tradicionales existentes entre ordenamientos jurídicos son una causa de disparidad, tanto respecto a los planteamientos legislativos como al planteamiento detallado del marco regulador para la protección de datos personales.

Aspectos internacionales de la intimidad y de los bancos de datos.

7. Por una serie de motivos, los problemas de elaborar salvaguardas para la persona con respecto al manejo de datos personales no pueden resolverse exclusivamente a escala nacional. El tremendo incremento en la circulación transfronteriza de datos y la creación de bancos de datos internacionales (colecciones de datos previstas para su recogida y demás propósitos) ponen de relieve la necesidad de una intervención nacional concertada y al propio tiempo, de apoyar argumentos a favor de la libre circulación de información, que a menudo debe equilibrarse frente a las necesidades de protección de los datos y de restricciones a su tratamiento, colección y divulgación.

8. Un asunto básico de interés a escala internacional es el de que haya consenso respecto a los principios fundamentales sobre los cuales debe cimentarse la protección de la persona. Tal consenso obviaría o disminuiría los motivos para regular la exportación de datos y facilitaría la resolución de problemas de conflicto de leyes. Además, podría constituir un primer paso hacia la elaboración de acuerdos internaciones vinculantes más detallados.

9. Hay otros motivos por los cuales la regulación del tratamiento de datos personales debería considerarse en un contexto internacional: los principios implicados tienen que ver con valores que muchas naciones anhelan mantener y ver que sean de aceptación generalizada; pueden ayudar a ahorrar costes en el tráfico internacional de datos; los países tienen un interés común en evitar la creación de lugares en los que puedan soslayarse fácilmente las disposiciones nacionales sobre el tratamiento de datos; en efecto, a la vista de la movilidad internacional de personas, mercancías y actividades comerciales y científicas, las prácticas de aceptación común con respecto al tratamiento de datos pueden ser ventajosas, aún cuando no haya implicado directamente ningún tráfico transfronterizo de datos.

Actividades internacionales pertinentes

10. Existen varios acuerdos internacionales sobre diversos aspectos de las telecomunicaciones que, al tiempo que facilitan las relaciones y la cooperación entre países, reconocen

el derecho soberano de cada país a regular sus propias telecomunicaciones (el Convenio Internacional de Telecomunicaciones de 1973). La protección de los datos y programas informáticos ha sido investigada por, entre otros, la Organización Mundial de Propiedad Intelectual, que ha elaborado un proyecto de disposiciones modelo para la legislación nacional sobre la protección de software. Pueden hallarse acuerdos especializados dirigidos a la cooperación informativa en una serie de esferas, tales como la ejecución forzosa de la ley, servicios sanitarios, estadísticas y servicios judiciales (verbigracia, con respecto a la toma de pruebas).

11. Hay una serie de acuerdos internacionales en los que se trata, de una forma más general, sobre las cuestiones que están debatiéndose actualmente, a saber, la protección de la intimidad y la libre divulgación de la información. Entre ellos se encuentran el Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950 y el Pacto Internacional sobre Derechos Civiles y Políticos (Naciones Unidas, 19 de diciembre de 1966).

12. Sin embargo, en vista de la insuficiencia de los instrumentos nacionales existentes referidos al tratamiento de datos y a los derechos individuales, una serie de organismos internacionales han llevado a cabo estudios detallados de los problemas implicados a fin de hallar soluciones más satisfactorias.

13. En 1973 y 1974, la Comisión de Ministros del Consejo de Europa adoptó dos acuerdos relativos a la protección de la intimidad de las personas frente a los bancos electrónicos de datos en los sectores privado y público, respectivamente. En ambos acuerdos se recomienda que los gobiernos de los estados miembro del Consejo de Europa adopten medidas para dar efectividad a una serie de principios básicos de protección referidos a la obtención de datos, la calidad de los mismos y los derechos de las personas a ser informadas acerca de los datos y de las actividades de tratamiento de los mismos.

14. Posteriormente, el Consejo de Europa, siguiendo instrucciones de su Comisión de Ministros, comenzó a elaborar un Convenio internacional de protección de la intimidad en relación al tratamiento de datos en el extranjero y al transfronterizo. También inició una labor relativa a normas modelo para bancos de datos médicos y normas de conducta para los profesionales del tratamiento de datos. La Comisión de Ministros adoptó el Convenio con fecha 17 de septiembre de 1980. Con él se pretende establecer principios básicos de protección de datos de ejecución forzosa por los países miembro, para reducir las restricciones a la circulación transfronteriza de datos entre las partes contratantes a base de reciprocidad, para conseguir la cooperación entre las autoridades nacionales de protección de datos y crear una Comisión Consultiva para la aplicación y desarrollo permanente del Convenio.

15. La Comunidad Europea ha llevado a cabo estudios acerca de los problemas de armonización de las legislaciones nacionales dentro de la Comunidad, en relación a la circulación transfronteriza de datos y las posibles desvirtuaciones competitivas, los

problemas de la seguridad y confidencialidad de los datos y la índole de la circulación transfronteriza de los mismos. Una subcomisión del Parlamento Europeo celebró a principios de 1978 una audiencia pública sobre el tratamiento de datos y los derechos de la persona. Su labor ha dado por resultado un informe presentado al Parlamento Europeo en la primavera de 1979. El informe, que el Parlamento Europeo adoptó en mayo de 1979, contiene un acuerdo sobre la protección de los derechos de la persona de cara a los avances técnicos en el tratamiento de datos.

Actividades de la OCDE

16. El programa de la OCDE acerca de la circulación transfronteriza de datos se deriva de unos estudios de utilización de la informática en el sector público que se iniciaron en 1969. Un Grupo de Expertos, el *Data Bank Panel*, analizó y estudió diferentes aspectos de la cuestión de la intimidad, verbigracia, en relación a la información digital, la administración pública, la circulación transfronteriza de datos y los resultados implícitos de la política en general. A fin de recabar pruebas de la índole de los problemas, el *Data Bank Panel* organizó un Simposio en Viena en 1977, que proporcionó opiniones y experiencia procedentes de una diversidad de sectores interesados, incluidos gobiernos, industria, usuarios de redes internacionales de comunicación de datos, servicios de tratamiento y organismos intergubernamentales.

17. Se elaboraron una serie de principios rectores dentro de un marco general para una posible intervención internacional. En estos principios se reconocía: a) la necesidad de una circulación de información continua e ininterrumpida entre los países, b) los legítimos intereses de los países en impedir los traslados de datos que sean peligrosos para su seguridad o contrarios a su legislación sobre el orden público y la decencia o que infrinjan los derechos de sus ciudadanos, c) el valor económico de la información y la importancia de proteger el "comercio de datos" mediante normas aceptadas de competencia leal, d) las necesidades de salvaguardas de seguridad para reducir al mínimo las infracciones de datos patrimoniales y el uso indebido de la información personal y e) la relevancia de un compromiso entre los países para fijar los principios esenciales de la protección de la información personal.

18. A principios de 1978 se creó dentro de la OCDE un nuevo Grupo de Expertos *ad hoc* sobre las Trabas a la Circulación Transfronteriza de Datos y Protección de la Intimidad, al que se encargó la elaboración de directrices sobre normas básicas que rijan la circulación transfronteriza y la protección de datos personales y de la intimidad, a fin de facilitar la armonización de las legislaciones nacionales, sin perjuicio de que se establezca en fecha posterior un Convenio internacional. Esta labor iba a ser llevada a cabo en estrecha colaboración con el Consejo de Europa y la Comunidad Europea y finalizarse para el 1º de julio de 1979.

19. El Grupo de Expertos, bajo la presidencia de Su Señoría el Magistrado Kirby, de Australia, y con la asistencia del Dr. Peter Seipel (Consultor), produjo varios proyectos y

debatió diversos informes que contenían, vebigracia, análisis comparativos de diferentes enfoques de la legislación en este campo. Se interesó en particular por la serie de cuestiones clave, que se exponen a continuación:

a) La cuestión de los hechos específicos, delicados

Surgió la cuestión de si las Directrices deberían ser de índole general o si deberían estructurarse para atender a diferentes órdenes de datos o actividades (verbigracia, informes comerciales). En efecto, probablemente no es posible identificar una serie de datos que se consideren delicados universalmente.

b) La cuestión del tratamiento automático de datos (TAD)

Es dudoso el argumento de que el TAD sea la causa principal de preocupación e, incluso, su impugnación.

c) La cuestión de las personas jurídicas

Algunas de las legislaciones nacionales, lo que de ninguna manera significa la totalidad de ellas, protegen los datos correspondientes a las personas jurídicas, de forma análoga a los datos correspondientes a las personas físicas.

d) La cuestión de recursos y sanciones

Los planteamientos de los mecanismos de control varían considerablemente: verbigracia, los planes de actuación que implican supervisión y concesión de licencias por autoridades constituidas especialmente podrían compararse a aquellos otros que implican cumplimiento voluntario por los que llevan constancia escrita y dependencia de los recursos judiciales tradicionales ante los tribunales.

e) La cuestión básica de los mecanismos o de la implantación

elección de principios esenciales y de su adecuado grado de detalle presenta dificultades: verbigracia, es debatible la medida en que las cuestiones de seguridad de los datos (protección de datos frente a injerencia no autorizada, incendio e incidencias análogas) debería considerarse como parte del complejo de la protección de la intimidad. Pueden diferir las opiniones respecto a los plazos para la retención de los datos o los requisitos para la supresión de los mismos, y lo mismo reza para con los requisitos de que los datos sean pertinentes a finalidades concretas. En particular, es difícil trazar una línea divisoria clara entre el grado de principios u objetivos básicos y el grado inferior de las cuestiones de "mecanismos", que deberían dejarse para la implantación nacional.

f) La cuestión de elección del Derecho aplicable

Los problemas de elección de jurisdicción, elección de Derecho aplicable y reconocimiento de sentencias extranjeras han resultado ser complejos en el contexto de la circulación transfronteriza de datos. Sin embargo, ha surgido la cuestión de si debería intentarse en esta fase proponer soluciones de carácter no vinculante en las Directrices, y en qué medida.

g) La cuestión de excepciones
Análogamente, pueden variar las opiniones respecto a la cuestión de excepciones. ¿Son acaso necesarias?. De serlo, ¿deberían preverse categorías de excepciones en particular o deberían formularse límites generales a las excepciones?.
h) La cuestión de parcialidad
Finalmente, hay un conflicto inherente entre la protección de datos personales y la libre circulación transfronteriza de los mismos. Se podrá poner el acento en la una o en la otra, y los intereses en la protección de la intimidad pudieran ser difíciles de distinguir respecto a otros intereses correspondientes al comercio, la cultura, la soberanía nacional y así sucesivamente.

20. Durante su labor, el Grupo de Expertos mantuvo estrechos contactos con los órganos homólogos del Consejo de Europa. Se puso todo empeño en evitar diferencias innecesarias entre los textos producidos por las dos organizaciones; así, el conjunto de principios básicos de protección es análogo en muchos aspectos. Por otra parte, existe una serie de diferencias. De entrada, las Directrices de la OCDE no son vinculantes jurídicamente, mientras que el Consejo de Europa ha producido un convenio que será vinculante jurídicamente entre los países que lo ratifiquen. Esto, a su vez, significa que la cuestión de las excepciones ha sido tratada por el Consejo de Europa con mayor detalle. En cuanto al ámbito de aplicación, el Convenio del Consejo de Europa trata primordialmente sobre el tratamiento automático de datos personales, en tanto que las Directrices de la OCDE son de aplicación a los datos personales que impliquen peligros para la intimidad y las libertades individuales, con independencia de los métodos y mecanismos que se empleen al efecto. Por lo que se refiere al grado de detalle, los principios básicos de protección propuestos por las dos organizaciones no son idénticos y la terminología empleada difiere en algunos aspectos. El marco institucional para la cooperación continuada se trata con mayor detalle en el Convenio del Consejo de Europa que en las Directrices de la OCDE.
21. El Grupo de Expertos también mantuvo cooperación con la Comisión de las Comunidades Europeas, según lo requerido por su mandato.

II. Las directrices

A. Objeto y ámbito

Generalidades

22. En el Preámbulo de la Recomendación se expresan los asuntos básicos de interés que reclaman intervención. En la Recomendación se afirma el compromiso de los países miembro de proteger la intimidad y las libertades individuales y respetar la circulación transfronteriza de datos personales.

23. Las Directrices expuestas en el Anejo a la Recomendación constan de cinco partes. En la I Parte se contiene una serie de definiciones y se especifica el ámbito de las Directrices, con la indicación de que representan criterios mínimos. En la II Parte se contienen ocho principios básicos (Apartados 7 al 14) correspondientes a la protección de la intimidad y de las libertades individuales a escala nacional. En la III Parte se trata sobre los principios de aplicación internacional, esto es, aquellos principios que se refieren principalmente a las relaciones entre los países miembro.

24. En la IV Parte se trata, en términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores y se especifica que estos principios deberían aplicarse de forma no discriminatoria. La V Parte tiene que ver con cuestiones de asistencia mutua entre los países miembro, principalmente a través del intercambio de información y la evitación de procedimientos nacionales incompatibles para la protección de datos personales. Concluye con una remisión a las cuestiones de Derecho aplicable que pueden surgir cuando la circulación de datos personales implique a varios países miembro.

Objetivos

25. La esencia de las Directrices consta de los principios expuestos en la II Parte del Anejo. Se recomienda a los países miembro que observen esos principios con vistas a:

a) conseguir la aceptación entre ellos de ciertos criterios mínimos de protección de la intimidad y de las libertades individuales con respecto a los datos personales;

b) reducir al mínimo las diferencias entre sus normas y prácticas nacionales pertinentes;

c) garantizar que en la protección de los datos personales toman en consideración los intereses mutuos y la necesidad de evitar ingerencias indebidas en la circulación de datos personales entre ellos, y

d) eliminar, en cuanto sea posible, los motivos que podrían inducirles a restringir la circulación transfronteriza de datos personales por causa de los posibles riesgos asociados a esa circulación.

Tal y como se manifiesta en el Preámbulo, hay implicados dos valores básicos imprescindibles: la protección de la intimidad y de las libertades individuales y el fomento de la libre circulación de datos personales. Con las Directrices se intenta equilibrar ambos valores entre sí. En tanto que se aceptan ciertas restricciones a la libre circulación transfronteriza de datos personales, se pretende reducir la necesidad de tales restricciones y, por tanto, reforzar la idea de la libre circulación de información entre los países.

26. Finalmente, las IV y V Partes de las Directrices contienen principios con los que se pretende garantizar:

a) medidas nacionales eficaces para la protección de la intimidad y de las libertades individuales;

b) la evitación de prácticas que impliquen una discriminación desleal entre las personas, y

c) las bases para una continuada cooperación internacional y procedimientos compatibles en toda normativa sobre la circulación transfronteriza de datos personales.

Grado de detalle

27. El grado de detalle de las Directrices varía según dos factores principales, a saber: a) la extensión del consenso alcanzado relativo a las soluciones propuestas y b) el conocimiento y la experiencia disponibles que indiquen las soluciones que hayan de adoptarse en esta fase. Verbigracia, el Principio de Participación Individual (Apartado 13) trata concretamente sobre diversos aspectos de la protección del interés de la persona, mientras que la disposición respecto a problemas de elección de Derecho aplicable y cuestiones conexas (Apartado 22) meramente establece un punto de partida para una elaboración gradual de planteamientos comunes detallados y de acuerdos internacionales. En su conjunto, las Directrices constituyen un marco general para intervenciones concertadas por los países miembro: los objetivos propuestos en las Directrices pueden alcanzarse de distintas maneras, según los instrumentos y las estrategias jurídicos que prefieran los países miembro para su implantación. En conclusión, hay necesidad de un estudio continuado de las Directrices, tanto por los países miembro como por la OCDE.

Siempre y cuando se adquiera experiencia, pudiera ser conveniente desarrollar y reajustar las Directrices en consecuencia.

Países que no sean miembros

28. La Recomendación va dirigida a los países miembro, lo cual se hace ver en varias disposiciones que están restringidas expresamente a las relaciones entre los países miembro (véanse los Apartados 15, 17 y 20 de las Directrices). Sin embargo, el reconocimiento generalizado de las Directrices es conveniente y nada de lo que se exponga en ellas

debería interpretarse en el sentido de que se impide la aplicación de las Disposiciones oportunas a los países que no sean miembros. En vista del incremento en la circulación transfronteriza de datos y de la necesidad de garantizar soluciones concertadas, se hará todo lo posible para poner las Directrices en conocimiento de los países que no sean miembros y de los organismos internacionales competentes.

Perspectiva reguladora más amplia

29. Se ha señalado anteriormente que la protección de la intimidad y de las libertades individuales constituye uno de los muchos aspectos jurídicos parcialmente coincidentes que están implicados en el tratamiento de datos. Las Directrices constituyen un nuevo instrumento, además de otros, que tienen que ver con instrumentos internacionales que rigen tales cuestiones como derechos humanos, telecomunicaciones, comercio internacional, propiedad intelectual y diversos servicios de información. De surgir la necesidad, los principios expuestos en las Directrices podrían desarrollarse aún más dentro del marco de las actividades emprendidas por la OCDE en la esfera de políticas de información, informática y comunicaciones.

Convenio Número 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Los Estados miembros del Consejo de Europa, signatarios del presente Convenio,
CONSIDERANDO
que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.
REAFIRMANDO
al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras.
RECONOCIENDO
la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos,
CONVIENEN
en lo siguiente:

Capitulo I
Disposiciones generales

Artículo 1. Objeto y fin

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Artículo 2. Definiciones

A los efectos del presente Convenio:
a) «Datos de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»);
b) «fichero automatizado» significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado;
c) por «tratamiento automatizado» se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión;
d) autoridad «controladora del fichero» significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

Artículo 3. Campos de aplicación

1. Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.
2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulteriorhacer saber mediante declaración dirigida al Secretario general del Consejo de Europa:

a) Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de las cuales quedará depositada. No deberá sin embargo incluir en esa lista categorías de ficheros automatizados sometidas, con arreglo a su derecho interno, a disposiciones de protección de datos. Deberá, por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidas a su régimen de protección de datos categorías suplementarias de ficheros automatizados de datos de carácter personal;

b) que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica;

c) que aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.

3. Cualquier Estado que haya ampliado el campo de aplicación del presente Convenio mediante una de las declaraciones a que se refieren los apartados 2, b) o c), que ante-

ceden podrá, en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada.
4. Cualquier parte que haya excluido determinadas categorías de ficheros automatizados de datos de carácter personal mediante la declaración prevista en el apartado 2, a), anterior no podrá pretender que una Parte que no las haya excluido aplique el presente Convenio a dichas categorías.
5. Igualmente, una Parte que no haya procedido a una u otra de las ampliaciones previstas en los párrafos 2, b) y c), del presente artículo no podrá pretender que se aplique el presente Convenio en esos puntos con respecto a una parte que haya procedido a dichas aplicaciones.
6. Las declaraciones previstas en el párrafo 2 del presente artículo tendrán efecto en el momento de la entrada en vigor del Convenio con respecto al Estado que las haya formulado, si dicho Estado las ha hecho en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, o tres meses después de su recepción por el Secretario general del Consejo de Europa si se han formulado en un momento ulterior. Dichas declaraciones podrán retirarse en su totalidad o en parte mediante notificación dirigida al Secretario general del Consejo de Europa. La retirada tendrá efecto tres meses después de la fecha de recepción de dicha notificación.

Capitulo II
Principios básicos para la protección de datos

Artículo 4. Compromisos de las Partes

1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.
2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.

Artículo 5. Calidad de los datos

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;
e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Artículo 6. Categorías particulares de datos

Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Artículo 7. Seguridad de los datos

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Artículo 8. Garantías complementarias para la persona concernida

Cualquier persona deberá poder:
a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;
b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;
d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Artículo 9. Excepción y restricciones

1. No se admitirá excepción alguna en las disposiciones de los artículo 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.
2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;
b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Artículo 10. Sanciones y recursos

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

Artículo 11. Protección más amplia

Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio.

Capítulo III
Flujos transfronterizos de datos

Artículo 12. Flujos transfronterizos de datos de carácter personal y el derecho interno

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.
3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:

a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;
b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

Capítulo IV
Ayuda mutua

Artículo 13. Cooperación entre las Partes

1. Las Partes se obligan a concederse mutuamente asistencia para el cumplimiento del presente Convenio.
2. A tal fin,

a) cada Parte designará a una o más autoridades cuya denominación y dirección comunicará al Secretario general del Consejo de Europa;
b) cada Parte que haya designado a varias autoridades indicará en la comunicación a que se refiere el apartado anterior la competencia de cada una de dichas autoridades.

3. Una autoridad designada por una Parte, a petición de una autoridad designada por otra Parte:

a) Facilitará informaciones acerca de su derecho y su práctica administrativa en materia de protección de datos;
b) tomará toda clase de medidas apropiadas, con arreglo a su derecho interno y solamente a los efectos de la protección de la vida privada, para facilitar informaciones fácticas relativas a un tratamiento automatizado determinado efectuado en su territorio con excepción, sin embargo, de los datos de carácter personal que sean objeto de dicho tratamiento.

Artículo 14. Asistencia a las personas concernidas que tengan su residencia en el extranjero

1. Cada Parte prestará asistencia a cualquier persona que tenga su residencia en el extranjero para el ejercicio de los derechos previstos por su derecho interno que haga efectivos los principios enunciados en el artículo 8 del presente Convenio.
2. Si dicha persona residiese en el territorio de otra Parte, deberá tener la facultad de presentar su demanda por intermedio de la autoridad designada por esa Parte.
3. La petición de asistencia deberá hacer constar todos los datos necesarios relativos concretamente a:

a) El nombre, la dirección y cualesquiera otros elementos pertinentes de identificación relativos al requirente;

b) el fichero automatizado de datos de carácter personal al que se refiere la demanda o la autoridad controladora de dicho fichero;

c) el objeto de la petición.

Artículo 15. Garantías relativas a la asistencia facilitada por las autoridades designadas

1. Una autoridad designada por una Parte que haya recibido información de una autoridad designada por otra Parte, bien en apoyo de una petición de asistencia bien como respuesta a una petición de asistencia que haya formulado ella misma, no podrá hacer uso de dicha información para otros fines que no sean los especificados en la petición de asistencia.
2. Cada parte cuidará de que las personas pertenecientes a la autoridad designada o que actúen en nombre de la misma estén vinculadas por obligaciones convenientes de secreto o de confidencialidad con respecto a dicha información.
3. En ningún caso estará autorizada una autoridad designada para presentar, con arreglo a los términos del artículo 14, párrafo 2, una petición de asistencia en nombre de una persona concernida residente en el extranjero, por su propia iniciativa y sin el consentimiento expreso de dicha persona.

Artículo 16. Denegación de peticiones de asistencia

Una autoridad designada, a quien se haya dirigido una petición de asistencia con arreglo a los términos de los artículos 13 ó 14 del presente Convenio, solamente podrá negarse a atenderla si:

a) La petición es incompatible con las competencias, en materia de protección de datos, de las autoridades habilitadas para responder;

b) la petición no está conforme con lo dispuesto en el presente Convenio;

c) atender a la petición fuese incompatible con la soberanía, la seguridad o el orden

público de la Parte que la haya designado, o con los derechos y libertades fundamentales de las personas que estén bajo la jurisdicción de dicha Parte.

Artículo 17. Gastos y procedimientos de asistencia

1. La ayuda mutua que las Partes se concedan con arreglo a los términos del artículo 13, así como la asistencia que ellas presten a las personas concernidas residentes en el extranjero con arreglo a los términos del artículo 14, no dará lugar al pago de gastos y derechos que no sean los correspondientes a los expertos y a los intérpretes. Dichos gastos y derechos correrán a cargo de la Parte que haya designado a la autoridad que haya presentado la petición de asistencia.
2. La persona concernida no podrá estar obligada a pagar, en relación con las gestiones emprendidas por su cuenta en el territorio de otra Parte, los gastos y derechos que no sean los exigibles a las personas que residan en el territorio de dicha Parte.
3. Las demás modalidades relativas a la asistencia referentes, concretamente a las formas y procedimientos así como a las lenguas que se utilicen se establecerán directamente entre las Partes concernidas.

Capítulo V
Comité consultivo

Artículo 18. Composición del Comité

1. Después de la entrada en vigor del presente Convenio se constituirá un Comité Consultivo.
2. Cada Parte designará a un representante y a un suplente en dicho Comité. Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio tendrá el derecho de hacerse representar en el Comité por un observador.
3. El Comité Consultivo podrá, mediante una decisión tomada por unanimidad, invitar a cualquier Estado no miembro del Consejo de Europa, que no sea Parte del Convenio, a hacerse representar por un observador en una de las reuniones.

Artículo 19. Funciones del Comité

El Comité Consultivo:

a) Podrá presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio;

b) podrá presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21;
c) formulará su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, con arreglo al artículo 21, párrafo 3; d) podrá, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio.

Artículo 20. Procedimiento

1. El Secretario general del Consejo de Europa convocará al Comité Consultivo. Celebrará su primera reunión en los doce meses que sigan a la entrada en vigor del presente Convenio. Posteriormente se reunirá al menos una vez cada dos años y, en todo caso, cada vez que un tercio de los representantes de las Partes solicite su convocatoria.
2. La mayoría de los representantes de las Partes constituirá el quórum necesario para celebrar una reunión del Comité Consultivo.
3. Después de cada una de dichas reuniones, el Comité Consultivo someterá al Comité de Ministros del Consejo de Europa una memoria acerca de sus trabajos y el funcionamiento del Convenio.
4. Sin perjuicio de lo dispuesto en el presente Convenio, el Comité Consultivo fijará su reglamento anterior.

Capítulo VI
Enmiendas

Artículo 21. Enmiendas

1. Podrán proponerse enmiendas al presente Convenio por una Parte, por el Comité de Ministros del Consejo de Europa o por el Comité Consultivo.
2. Cualquier propuesta de enmienda se comunicará por el Secretario general del Consejo de Europa a los Estados miembros del Consejo de Europa y a cada Estado no miembro que se haya adherido o se le haya invitado a que se adhiera al presente Convenio, con arreglo a lo dispuesto en el artículo 23.
3. Además, cualquier modificación propuesta por una Parte o por el Comité de Ministros se comunicará al Comité Consultivo, el cual presentará al Comité de Ministros su opinión acerca de la enmienda propuesta.
4. El Comité de Ministros examinará la enmienda propuesta y cualquier opinión presentada por el Comité Consultivo y podrá aprobar la enmienda.

5. El texto de cualquier enmienda aprobada por el Comité de Ministros conforme al párrafo 4 del presente artículo se remitirá a las Partes para su aceptación.
6. Cualquier enmienda aprobada con arreglo al párrafo 4 del presente artículo entrará en vigor el trigésimo día después de que todas las Partes hayan informado al Secretario general de que la han aceptado.

Capítulo VII
Cláusulas finales

Artículo 22. Entrada en vigor

1. El presente Convenio quedará abierto a la firma de los Estados miembros del Consejo de Europa. Se someterá a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario general del Consejo de Europa.
2. El presente Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha en que cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento para quedar vinculados por el Convenio, con arreglo a las disposiciones del párrafo anterior.
3. Para cualquier Estado miembro que expresare ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de ratificación, aceptación o aprobación.

Artículo 23. Adhesión de Estados no miembros

1. Después de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera al presente Convenio mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, d), del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité.
2. Para cualquier Estado adherido, el Convenio entrará en vigor el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha del depósito del instrumento de adhesión en poder del Secretario general del Consejo de Europa.

Artículo 24. Cláusula territorial

1. Cualquier Estado podrá designar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el territorio o los territorios a los cuales se aplicará el presente Convenio.
2. Cualquier Estado en cualquier otro momento posterior, y mediante una declaración dirigida al Secretario general del Consejo de Europa, podrá ampliar la aplicación del presente Convenio a cualquier otro territorio designado en la declaración. El Convenio entrará en vigor, con respecto a dicho territorio, el día primero del mes siguiente a la expiración de un período de tres meses después de la fecha de recepción de la declaración por el Secretario general.
3. Cualquier declaración hecha en virtud de los dos párrafos anteriores podrá retirarse, en lo que respecta a cualquier territorio designado en dicha declaración, mediante notificación dirigida al Secretario general. La retirada será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción de la notificación por el Secretario general.

Artículo 25. Reservas

No podrá formularse reserva alguna con respecto a las disposiciones del presente Convenio.

Artículo 26. Denuncia

1. Cualquier parte podrá en cualquier momento denunciar el presente Convenio dirigiendo una notificación al Secretario general del Consejo de Europa.
2. La denuncia será efectiva el día primero del mes siguiente a la expiración de un período de seis meses después de la fecha de recepción dela notificación por el Secretario general.

Artículo 27. Notificaciones

El Secretario general del Consejo de Europa notificará a los Estados miembros del Consejo y a cualquier Estado que se haya adherido al presente Convenio:

a) Cualquier firma;

b) el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c) cualquier fecha de entrada en vigor del presente Convenio, conforme a sus artículos 22, 23 y 24;

d) cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual los infrascritos, debidamente autorizados al efecto, afirman el presente Convenio.

Hecho en Estrasburgo el 28 de enero de 1981 en francés y en inglés, los dos textos igualmente fehacientes, en un ejemplar único que quedará depositado en los archivos del Consejo de Europa. El secretario general del Consejo de Europa remitirá copia certificada conforme del mismo a cada uno de los Estados miembros del Consejo de Europa y a cualquier Estado invitado a la adhesión al presente Convenio.

Estados Parte

(1) Alemania, República Federal de ..... 19-6-1985 (Ratificación)
España ..... 31-1-1984 (Ratificación)
(2) Francia ..... 24-3-1983 (Aprobación)
(3) Noruega ..... 20-2-1984 (Ratificación)
Suecia ..... 29-9-1982 ®

Declaraciones y reservas

(1) Alemania, República Federal de.

Declaraciones contenidas en tres cartas del Representante Permanente de la República Federal de Alemania, fechadas el 19 de junio de 1985.
Artículo 8, párrafo b).
«La República Federal de Alemania parte del principio de que no puede darse ningún curso a una solicitud de informes, de acuerdo con lo que dispone el párrafo b) del artículo 8, si la persona afectada no está en condiciones de justificar suficientemente su petición de información.»
Artículo 12, párrafo 2.
«Refiriéndose al apartado 5 del párrafo 67 del Informe explicativo relativo al Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal, el gobierno de la República Federal de Alemania parte del principio de que el párrafo 2 del artículo 12 deja a las partes la libertad de estimar, en el cuadro de su derecho interno en materia de protección de datos, las normas prohibiendo en ciertos casos particulares la transmisión de datos de carácter personal a fin de tener en cuenta

los intereses de la persona afectada dignos de ser protegidos.»
Artículo 13, párrafo 2, apartado a).
«La Autoridad competente a nivel de la Federación es:
Der Bundesminister des Innern
Postrach 17 02 90
D-5300 Bonn 1

Las autoridades competentes a nivel de los Estados federados (Lander) serán designados tan pronto como sean posibles.»

Artículo 24, párrafo 1.
«El Convenio se aplica igualmente al Estado federado (Land) de Berlín con efecto de la fecha en la cual entrará en vigor para la República Federal de Alemania.»

(2) Francia

El Gobierno de la República Francesa desea hacer la siguiente declaración:
«Conforme a lo dispuesto en el artículo 3, párrafo 2, apartado c), aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.»

(3) Noruega

Declaración contenida en el Instrumento de ratificación depositado el 20 de febrero de 1984.
Artículo 3, párrafo 2, apartado a).
«El Convenio se aplicará a ficheros privados de carácter personal que no son utilizados ni en el sector privado ni por sociedades o fundaciones.»
Artículo 3, párrafo 2, apartado b).
«Las disposiciones del Convenio se aplicarán igualmente a informaciones referentes a las asociaciones o fundaciones.»
Artículo 24, párrafo 1.
«El Convenio no se aplicará a Svalbard.»
Artículo 13, párrafo 2, apartado a).
«La Autoridad designada en Noruega conforme a lo que dispone el artículo 13, párrafo 2, apartado a), del Convenio es:
Datatilsynet Postboks 8177 Dep. Oslo 1.»

El presente Convenio entró en vigor de forma general y para España el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo.

Protocolo Adicional al Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos

Estrasburgo, a 8 de noviembre de 2001.

Preámbulo[1]

Las Partes de este Protocolo Adicional al Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, abierto a la firma en Estrasburgo el 28 de enero de 1981 (en adelante "El Convenio");
SEGUROS de que las Autoridades de control, ejerciendo sus funciones con completa independencia, constituyen un elemento de protección efectiva de las personas con respecto al tratamiento de sus datos personales;
CONSIDERANDO
la importancia del flujo de información entre los pueblos;
CONSIDERANDO que, con el incremento del intercambio de datos personales a través de las fronteras, es necesario asegurar la afectiva protección de los derechos humanos y libertades fundamentales, y, en especial, el derecho a la privacidad, en relación con tales intercambios,
HAN ACORDADO lo siguiente:

Artículo 1. Autoridades de Control

1. Cada Parte preverá que una o más Autoridades sean responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios contenidos en los Capítulos II y III del Convenio y en el presente Protocolo.
2.
a) A tal fin, las mencionadas autoridades dispondrán, en particular, de poderes de investigación y de intervención, así como del poder de iniciar procedimientos legales o

de dirigirse a las autoridades judiciales correspondientes en relación con violaciones del derecho interno, dando así cumplimiento a los principios mencionados en el párrafo 1 del Artículo 1 del presente Protocolo.

b) Cada Autoridad de Control conocerá de las reclamaciones presentadas por parte de cualquier persona relativas a sus derechos y libertades fundamentales con respecto al tratamiento de datos personales y dentro de sus respectivas competencias.

3. Las Autoridades de Control ejercerán sus funciones con completa independencia.
4. Las Decisiones de las Autoridades de Control que den lugar a reclamaciones, pueden ser recurridas judicialmente.
5. De conformidad con las disposiciones del Capítulo IV, y sin perjuicio de las disposiciones del Artículo 13 del Convenio, las Autoridades de Control cooperarán mutuamente en la medida necesaria para el cumplimiento de sus obligaciones, y en particular a través del intercambio de cualquier información que resulte de utilidad.

Artículo 2. Transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio.

1. Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección.
2. No será de aplicación el párrafo 1 del Artículo 2 del presente Protocolo, pudiendo las Partes autorizar la transferencia de datos personales:

a) Si el derecho interno así lo establece a causa de:

Intereses concretos del afectado, o

Intereses legítimos, especialmente los de carácter público, o

b) si se prevén las suficientes garantías, que pueden resultar, en particular, de cláusulas contractuales, por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno.

Artículo 3. Disposiciones finales

1. Las disposiciones de los Artículos 1 y 2 del presente Protocolo serán contempladas por las Partes como artículos adicionales al Convenio, y en consecuencia todas las dis-

posiciones del Convenio serán de aplicación.

2. El presente Protocolo se encuentra abierto a la firma de los Estados Signatarios del Convenio. Una vez adheridos al Convenio de conformidad con las condiciones establecidas en el mismo, las Comunidades Europeas podrán firmar este Protocolo. El presente Protocolo se encuentra sujeto a su ratificación, aceptación o aprobación. Un Signatario del presente Protocolo no podrá ratificar o aprobar el mismo salvo que haya ratificado o aprobado con carácter previo o simultáneo al Convenio o se haya adherido al mismo. Los Instrumentos de ratificación y aprobación del presente Protocolo se depositarán en la Secretaría General del Consejo de Europa.

3.

a) El presente Protocolo entrará en vigor el primer día del mes siguiente al término de un período de tres meses una vez que cinco de sus Signatarios hayan expresado su consentimiento para quedar vinculados al mismo, de conformidad con las disposiciones del párrafo 2 del Artículo 3.

b) En relación con los Signatarios del presente Protocolo que expresen su consentimiento para quedar vinculado al mismo, el Protocolo entrará en vigor el primer día del mes siguiente al término del período de tres meses tras la fecha de depósito del Instrumento de Ratificación o aprobación.

4.

a) Tras la entrada en vigor del presente Protocolo, cualquier Estado que haya suscrito el Convenio puede así mismo suscribir el Protocolo.

b) La adhesión será efectiva a través del depósito por parte del Secretario General del Consejo de Europa de un Instrumento de Adhesión, que surtirá efectos el primer día del mes siguiente al término del período de tres meses después de la fecha de su depósito.

5.

a) Cualquier Parte podrá en cualquier momento denunciar el presente Protocolo mediante notificación dirigida al Secretario General del Consejo de Europa.

b) Tal denuncia será efectiva el primer día del mes siguiente al término del período de tres meses después de la fecha de recepción del tal notificación por parte del Secretario General.

6. El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, las Comunidades Europeas y cualquier otro Estado signatario del presente Protocolo acerca de:

a) Cualquier firma;

b) Depósito de cualquier Instrumento de Ratificación o Aprobación;
c) Fecha de entrada en vigor del presente Protocolo de conformidad con el Artículo 3;
d) Cualquier otro acto, notificación o comunicación relativo/a el presente Protocolo,

En fe de lo cual los infrascritos, debidamente autorizados al efecto, firman el presente Protocolo,

Hecho en Estrasburgo el 8 de Noviembre de 2001, en inglés y en francés, los dos textos igualmente fehacientes en un ejemplar único que quedará depositado en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada conforme del mismo a cada uno de los Estados miembros del Consejo de Europa, de las Comunidades Europeas y cualquier Estado invitado a adherirse al presente Convenio.

Nota

1 Traducción no oficial realizada internamente por la Agencia de Protección de Datos. Las únicas versiones vinculantes son los originales en inglés y francés custodiados por el Secretario General del Consejo de Europa. Disponible en el vínculo: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.29-cp--PROTOCOLO-ADICIONAL-CONVENIO-N-1o-108.pdf

Directrices para la regulación de los archivos de datos personales informatizados

Adoptadas mediante resolución 45/95
de la Asamblea General,
de 14 de diciembre de 1990

Los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado, con sujeción a las siguientes orientaciones:

A. Principios relativos a las garantías mínimas que deben prever las legislaciones nacionales

1. Principio de legalidad y lealtad

La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

2. Principio de exactitud

Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, asó como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados.

3. Principio de especificación de la finalidad

La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada

cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que:

a) Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados;

b) Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados;

c) El período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

4. Principio de acceso de la persona interesada

Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora especificada más abajo en el principio 8. El coste de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia.

5. Principio de no discriminación

Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

6. Facultad para hacer excepciones

Las excepciones a los principios 1 a 4 solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas.

Las excepciones al principio 5, relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación.

7. Principio de seguridad

Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

8. Supervisión y sanciones

El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados.

9. Flujo transfronterizo de datos

Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad.

10. Campo de aplicación

Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos.

B. Aplicación de las directrices a archivos de datos personales mantenidos por organizaciones intrenacionales gubernamentales

Las presentes directrices serán de aplicación a los archivos de datos personales que mantengan las organizaciones internacionales gubernamentales, sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal, y archivos para fines externos, relativos a terceros que tengan relaciones con la organización.

Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices.

Cláusula humanitaria: puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley.

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 esos datos

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea, y, en particular, su artículo 100 A,

Vista la propuesta de la Comisión ([1]),

Visto el dictamen del Comité Económico y Social ([2]),

De conformidad con el procedimiento establecido en el artículo 189 B del Tratado ([3]),

(1) Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;

(2) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos;

(3) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas;

(4) Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos;

(5) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior;
(6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;
(7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;
(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;
(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que

los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;

(10) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

(11) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;

(12) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones;

(13) Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado;

(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir,

manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;
(15) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;
(16) Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario;
(17) Considerando que en lo que respecta al tratamiento del sonido y de la imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en al artículo 9;
(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;
(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;
(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;

(21) Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal;
(22) Considerando que los Estados miembros precisarán en su legislación o en la aplicación de las disposiciones adoptadas en virtud de la presente Directiva las condiciones generales de licitud del tratamiento de datos; que, en particular, el artículo 5 en relación con los artículos 7 y 8, ofrece a los Estados miembros la posibilidad de prever, independientemente de las normas generales, condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos contempladas en el artículo 8;
(23) Considerando que los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos;
(24) Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;
(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias;
(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;
(27) Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a

riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;

(28) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados;

(29) Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona;

(30) Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;

(31) Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;
(32) Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;
(33) Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales;
(34) Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;
(35) Considerando, además, que el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;
(36) Considerando que, si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;
(37) Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección

de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales;

(38) Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención;

(39) Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; que, en todos estos supuestos, debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero;

(40) Considerando, no obstante, que no es necesario imponer esta obligación si el interesado ya está informado, si el registro o la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias;

(41) Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado;

(42) Considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter

médico únicamente pueda obtenerse a través de un profesional de la medicina;
(43) Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa;
(44) Considerando que los Estados miembros podrán verse obligados, en virtud de las disposiciones del Derecho comunitario, a establecer excepciones a las disposiciones de la presente Directiva relativas al derecho de acceso, a la información de personas y a la calidad de los datos para garantizar algunas de las finalidades contempladas más arriba;
(45) Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias;
(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;
(47) Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las perso-

nas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;
(48) Considerando que los procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva;
(49) Considerando que para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que se precisen sus límites; que los Estados miembros pueden igualmente disponer la exención o la simplificación cuando un encargado, nombrado por el responsable del tratamiento, se cerciore de que los tratamientos efectuados no pueden atentar contra los derechos y libertades de los interesados; que la persona encargada de la protección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia;
(50) Considerando que podrán establecerse exenciones o simplificaciones para los tratamientos cuya única finalidad sea el mantenimiento de registros destinados, de conformidad con el Derecho nacional, a la información del público y que sean accesibles para la consulta del público o de toda persona que justifique un interés legítimo;
(51) Considerando, no obstante, que el beneficio de la simplificación o de la exención de la obligación de notificación no dispensa al responsable del tratamiento de ninguna de las demás obligaciones derivadas de la presente Directiva;
(52) Considerando que, en este contexto, el control a posteriori por parte de las autoridades competentes debe considerarse, en general, una medida suficiente;
(53) Considerando, no obstante, que determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, o por el uso particular de una tecnología nueva; que es competencia de los Estados miembros, si así lo desean, precisar tales riesgos en sus legislaciones;
(54) Considerando que, a la vista de todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquélla; que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga su Derecho nacional, podrá emitir un dictamen o

autorizar el tratamiento de datos; que este examen previo podrá realizarse también en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas;
(55) Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva;
(56) Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;
(57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;
(58) Considerando que han de establecerse excepciones a esta prohibición en determinadas circunstancias, cuando el interesado haya dado su consentimiento, cuando la transferencia sea necesaria en relación con un contrato o una acción judicial, cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo; que en tal caso dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro; que, cuando la finalidad de un registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia sólo debería poder efectuarse a petición de dichas personas o cuando éstas sean las destinatarias;
(59) Considerando que pueden adoptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, en caso de que el responsable del tratamiento ofrezca garantías adecuadas; que, por lo demás, deben preverse procedimientos de negociación entre la Comunidad y los países terceros de que se trate;

(60) Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, y, en particular, de su artículo 8;
(61) Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores preofesionales para que elaboren códigos de conducta a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación;
(62) Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;
(63) Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa;
(64) Considerando que las autoridades de los distintos Estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones, de forma que se garantice el pleno respeto de las normas de protección en toda la Unión Europea;
(65) Considerando que se debe crear, en el ámbito comunitario, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, habida cuenta de este carácter específico, el grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva;
(66) Considerando que, por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo (4);
(67) Considerando que el 20 de diciembre de 1994 se alcanzó un acuerdo sobre un modus vivendi entre el Parlamento Europeo, el Consejo y la Comisión concerniente a las medidas de aplicación de los actos adoptados de conformidad con el procedimiento establecido en el artículo 189 B del Tratado CE;
(68) Considerando que los principios de protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios;

(69) Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste-eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento;
(70) Considerando que no es procedente que el interesado tenga que dar de nuevo su consentimiento a fin de que el responsable pueda seguir efectuando, tras la entrada en vigor de las disposiciones nacionales adoptadas en virtud de la presente Directiva, el tratamiento de datos sensibles necesario para la ejecución de contratos celebrados previo consentimiento libre e informado antes de la entrada en vigor de las disposiciones mencionadas;
(71) Considerando que la presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a tratamientos de datos personales;
(72) Considerando que la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Capítulo I. Disposiciones generales

Artículo 1. Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos

personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Artículo 2. Definiciones

A efectos de la presente Directiva, se entenderá por:

a) «datos personales»: toda información sobre una persona física idientificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Artículo 3. Ámbito de aplicación

1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

-efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

-efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Artículo 4. Derecho nacional aplicable

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento

deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Capítulo II. Condiciones generales para la licitud del tratamiento de datos personales

Artículo 5

Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales.

Sección I. Principios relativos a la calidad de los datos

Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:
   a) tratados de manera leal y lícita;
   b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
   c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
   d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
   e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.
2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo

dispuesto en el apartado 1.

Sección II. Principios relativos a la legitimación del tratamiento de datos

Artículo 7

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

Sección III. Categorías especiales de tratamientos

Artículo 8. Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.
4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Artículo 9. Tratamiento de datos personales y libertad de expresión

En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

Sección IV. Información del interesado

Artículo 10. Información en caso de obtención de datos recabados del propio interesado

Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como:

- los destinatarios o las categorías de destinatarios de los datos,
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Artículo 11. Información cuando los datos no han sido recabados del propio interesado

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- las categorías de los datos de que se trate,
- los destinatarios o las categorías de destinatarios de los datos,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

Sección V. Derecho de acceso del interesado a los datos

Artículo 12. Derecho de acceso

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:
-la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

-la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

-el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

Sección VI. Excepciones y limitaciones

Artículo 13. Excepciones y limitaciones

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una

disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

Sección VII. Derecho de oposición del interesado

Artículo 14. Derecho de oposición del interesado

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

Artículo 15. Decisiones individuales automatizadas

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre

que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Sección VIII. Confidencialidad y seguridad del tratamiento

Artículo 16. Confidencialidad del tratamiento

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Artículo 17. Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

-que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

-que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

Sección ix. Notificación

Artículo 18. Obligación de notificación a la autoridad de control

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.
2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

-cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o

-cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:

-hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

-llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos

a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.
4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 8.
5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.

Artículo 19. Contenido de la notificación

1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:

a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;

b) el o los objetivos del tratamiento;

c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;

d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;

e) las transferencias de datos previstas a países terceros;

f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.

2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.

Artículo 20. Controles previos

1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.
2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.
3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21. Publicidad de los tratamientos

1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.
2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.
3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

Capítulo III. Recursos judiciales, responsabilidad y sanciones

Artículo 22. Recursos

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. Responsabilidad

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.
2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha

responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24. Sanciones

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

Capítulo IV. Transferencia de datos personales a países terceros

Artículo 25. Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.
3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.
4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.
5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar

la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que

no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Capítulo V. Códigos De Conducta

Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

Capítulo VI. Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales

Artículo 28. Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.
Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.
2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.
3. La autoridad de control dispondrá, en particular, de:

-poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;

-poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

-capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

Artículo 29. Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo».

Dicho Grupo tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.
4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.
5. La Comisión desempeñará las funciones de secretaría del Grupo.
6. El Grupo aprobará su reglamento interno.
7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.

Artículo 30

1. El Grupo tendrá por cometido:
   a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;
   b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
   c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
   d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.
3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.
4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.
5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

Capítulo VII. Medidas de ejecución comunitarias

Artículo 31. El Comité

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.
2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:

-la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;

-el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

Disposiciones finales

Artículo 32

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a

la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.
2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.

No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.
3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.
4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 33

La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe será publicado.

La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.

Artículo 34

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Luxemburgo, el 24 de octubre de 1995.

Notas

[1] DO n° C 277 de 5. 11. 1990, p. 3 y DO n° C 311 de 27. 11. 1992, p. 30.

[2] DO n° 159 de 17. 6. 1991, p. 38.

[3] Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO n° C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO n° C 342 de 20. 12. 1993, p. 30); posición común del Consejo de 20 de febrero de 1995 (DO n° C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO n° C 166 de 3. 7. 1995).

[4] DO n° L 197 de 18. 7. 1987, p. 33.

Marco de privacidad del Foro de Cooperación Económica Asia Pacífico (APEC)

Los flujos de información son vitales para llevar a cabo negocios en una economía global. El Marco de Privacidad de APEC promueve un acercamiento flexible a la protección de la privacidad de la información en las Economías Miembro de APEC, evitando la creación de barreras innecesarias para los flujos de información.

Prólogo

Las Economías Miembro del Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) se dan cuenta del enorme potencial del comercio electrónico para expandir las oportunidades empresariales, reducir costos, incrementar la eficiencia, mejorar la calidad de vida y facilitar la participación de los pequeños negocios en el comercio global. Un marco que permita la transferencia de datos regionales beneficiará a los consumidores, a las empresas y a los gobiernos. Ministros han aprobado el Marco de Privacidad de APEC, reconociendo la importancia de desarrollar protecciones efectivas para la privacidad que eviten barreras a los flujos de información, asegurar en intercambio continuo y el crecimiento económico en la región APEC.

Parte 1. Preámbulo

Las Economías Miembro del Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) reconocen la importancia de proteger la privacidad de la información y mantener los flujos de información entre Economías de la región Asia Pacífico y entre sus socios comerciales. Como lo reconocieron los Ministros de APEC al aprobar el Programa para la Acción en el Comercio Electrónico 1998, el potencial del comercio electrónico no puede llevarse a cabo sin la cooperación del gobierno y de las empresas "para desarrollar e implementar tecnologías y políticas que establezcan confianza en cuanto a comunicación, información y sistemas de entrega seguros, protegidos y fidedignos, y que traten asuntos que incluyan la privacidad...". La falta de confianza del consumidor hacia la privacidad y seguridad de transacciones en línea y redes de información es un

elemento que puede impedir a las Economías Miembro, obtener todos los beneficios del comercio electrónico. Las Economías de APEC se dan cuenta que una parte de los esfuerzos clave para mejorar la confianza del consumidor y asegurar el crecimiento del comercio electrónico, debe ser la cooperación para balancear y promover la protección de la privacidad de la información y el libre flujo de información en la región Asia Pacífico.

Tecnologías de información y comunicación, incluyendo tecnologías móviles que se conectan a Internet y a otras rede de información, han hecho posible recopilar, almacenar y acceder a la información desde cualquier parte del mundo. Estas tecnologías ofrecen gran potencial para beneficios económicos y sociales para las empresas, los individuos y los gobiernos, incluyendo aumento en las opciones del consumidor, expansión del mercado, productividad, educación e innovación de productos. Sin embargo, mientras estas tecnologías abaratan y facilitan el recopilar, conectar y usar grandes cantidades de información, a menudo también hacen que estás actividades pasen desapercibidas para los individuos. Por consiguiente, puede ser más difícil para los individuos conservar una medida de control sobre su información personal. Como resultado de esto, los individuos se han preocupado por las dañinas consecuencias que puedan surgir del mal uso de su información. Por lo tanto, hay una necesidad de promover y hacer cumplir prácticas fidedignas de información en contextos en línea y no en línea para reforzar la confianza de los individuos y las empresas.

Como las operaciones comerciales y las expectativas de los consumidores continúan moviéndose debido a cambios en la tecnología y en la naturaleza de los flujos de información, empresas y otras organizaciones requieren entradas simultáneas y acceso a información 24 horas al día para satisfacer necesidades de la clientela y la sociedad, y proporcionar servicios eficientes y rentables. Sistemas reguladores que restringen innecesariamente este flujo o le imponen cargas, tienen implicaciones adversas para el comercio global y para las Economías. Por lo tanto, para promover y hacer cumplir prácticas éticas de información, existe la necesidad de desarrollar sistemas para proteger la privacidad de la información, que den cuenta de estas nuevas realidades en el ambiente global.

Las Economías de APEC aprueban el Marco de Privacidad de APEC basado en principios, como una herramienta importante para alentar el desarrollo de protecciones apropiadas a la privacidad de la información y para asegurar el libre flujo de información en la región Asia Pacífico.

Este Marco de trabajo, cuyo objetivo es promover el comercio electrónico en toda la región Asia Pacífico, concuerda con los valores básicos de los Lineamientos de Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 de la OCDE (Lineamientos de la OCDE)1, y reafirma el valor de la privacidad para los individuos y para la sociedad de información.

El Marco se dirige específicamente a estos conceptos base, así como a asuntos de particular relevancia para las Economías Miembro de APEC. Su distintivo acercamiento es para enfocar la atención en la protección práctica y consistente de la privacidad de la información dentro de este contexto. Al hacerlo, balancea la privacidad de la información con las necesidades empresariales y los intereses comerciales, y al mismo tiempo concede el debido reconocimiento a las diversidades culturales y de otro tipo que existan entre las Economías Miembro.

La intención del Marco es proporcionar una clara orientación y dirección a empresas dentro de las Economías de APEC, sobre asuntos comunes de privacidad y del impacto de estos asuntos en la forma en como se conducen negocios legítimos, y lo hace destacando las expectativas razonables del consumidor moderno de que las empresas reconocerán sus intereses de privacidad de forma consistente con los Principios explicados en este Marco.

Finalmente, este Marco sobre información de la protección de la privacidad fue desarrollado reconociendo la importancia de:

Desarrollar protecciones apropiadas para la información personal, particularmente contra las dañinas consecuencias de intrusiones no deseadas y del uso incorrecto de la información personal;

Reconocer el libre flujo de información como algo esencial para Economías de mercado desarrolladas y en desarrollo, para sustentar el crecimiento económico y social;

Posibilitar organizaciones globales que recopilen, accedan, usen o procesen información en Economías de APEC para desarrollar e implementar acercamientos uniformes dentro de sus organizaciones para tener acceso global y uso de la información personal;

Posibilitar agencias de seguridad para cumplir con su mandato de proteger la privacidad de la información; y,

Presentar mecanismos internacionales para promover y hacer cumplir la privacidad de la información, y mantener la continuidad de los flujos de información entre Economías de APEC y sus socios comerciales.

Parte II. Alcance

El propósito de la Parte II del Marco de Privacidad de APEC es dejar en claro el alcance de la cobertura de los Principios.

Definiciones

1. Información Personal significa cualquier información acerca de un individuo identificado o identificable.
2. Controlador de información personal significa una persona u organización que controla la recolección, posesión, procesamiento o uso de información personal. Incluye a una persona u organización que instruye a otra persona u organización para recolectar, guardar, procesar, usar, transferir o revelar información personal en su nombre, pero excluye a una persona u organización que desempeñe dichas funciones por instrucciones de otra persona u organización. También excluye a un individuo que recopile, guarde, procese o use información personal con respecto a asuntos personales, familiares o domésticos del individuo.
3. Información a disposición del público significa información personal acerca de un individuo, que él mismo hace o permite que esté disponible al público, o es obtenida o accedida legalmente desde:
registros del gobierno que están disponibles para el público;
reportes periodísticos; o
información requerida para por la ley para ser puesta a disposición del público.

Aplicación

En vista de las diferencias sociales, culturales, económicas y legales de cada Economía miembro, debe haber flexibilidad para implementar estos Principios.

Excepciones a estos Principios contenidas en la Parte II de este Marco, incluyendo aquellas relacionadas a la soberanía nacional, seguridad nacional, seguridad pública y política pública deberán:

a. ser limitadas y proporcionales para cumplir los objetivos a los que se relacionan estas excepciones; y,
b.
(i) ser dadas a conocer al público; o,
(ii) estar de acuerdo con la ley.

Parte III. Principios de privacidad de la información de APEC

I. Previniendo Daño

Reconocer los intereses del individuo para legitimar expectativas de privacidad, la protección de la información personal debe ser diseñada para prevenir el mal uso del

tal información. Además, reconocer el riesgo de que puede haber daños por el mal uso de la información personal, obligaciones específicas deben tomar en cuenta tal riesgo y medidas de saneamiento deben ser proporcionales a la probabilidad y severidad del daño amenazado por la recolección, uso y transferencia de información personal.

II. Aviso

Controladores de Información Personal deben proporcionar declaraciones claras y de fácil acceso acerca de sus prácticas y políticas por lo que respecta a la información personal, que deben incluir:

el hecho de que información personal está siendo recopilada;
los propósitos para los que se está recopilando la información personal;
los tipos de personas u organizaciones a las que se les podría revelar la información personal;
la identidad y ubicación del controlador/ director de información personal, incluyendo información de cómo contactarlos respecto a sus prácticas y manejo de la información personal;
la elección de medios que el controlador/ director de la información personal ofrece a los individuos para limitar el uso, revelación, acceso y corrección de su información.

Todos los pasos razonablemente viables deberán ser tomados para asegurar que se proporcione el aviso antes o al momento de recopilar la información personal. De lo contrario, dicho aviso deberá ser proporcionado tan pronto como sea factible.

Quizá no se apropiado que los controladores de información personal proporcionen aviso respecto a la recolección y uso de la información disponible para el público.

III. Limitación de Recolección

La recolección de la información personal deberá ser limitada a aquella información que sea relevante a los propósitos de recolección y dicha información deberá ser obtenida por medios legales y justos, y cuando sea apropiado, con consentimiento y dando aviso al individuo en cuestión.

IV. Usos de la Información Personal

La información personal recopilada sólo debe ser usada para cumplir con los propósitos de recolección y otros propósitos compatibles o relacionados, excepto:

a. con el consentimiento del individuo cuya información personal es recopilada;

b. cuando sea necesaria para proporcionar un servicio solicitado por el individuo; o,
c. por la autoridad de la ley y otros instrumentos legales, proclamas y pronunciamientos de efecto legal.

V. Elección

Cuando sea apropiado, se le deben proporcionar a los individuos mecanismos claros, prominentes, de fácil entendimiento, accesibles y asequibles para ejercitar la elección en relación a la recolección, uso y revelación de su información personal. Puede que no sea apropiado que los controladores de la información personal proporcionen estos mecanismos cuando recopilen información disponible para el público.

VI. Integridad de la Información Personal

La información personal debe ser exacta, completa y debe estar actualizada al grado necesario para los propósitos para los que será usada.

VII. Medidas de Seguridad

Los controladores de información personal deben proteger la información personal que guarden con medidas de seguridad apropiadas contra riesgos, tales como pérdida o acceso desautorizado a la información personal, o destrucción desautorizada, uso, modificación o revelación de información o cualquier otro uso incorrecto. Tales medidas de seguridad deben ser proporcionales a la probabilidad y severidad del daño obtenido, a la sensibilidad de la información y al contexto en el que es guardada y quedarán sujetas a una revisión periódica y a una nueva evaluación.

VIII. Acceso y Corrección

Los individuos deben ser capaces de:
a) obtener confirmación del controlador de información acerca de si éste posee información personal acerca de ellos
b) haberles comunicado, tras haber proporcionado pruebas suficientes de su identidad, información personal acerca de ellos;
i. dentro de un tiempo razonable;
ii. a un costo, si es que hay alguno, que no sea excesivo:
iii. de manera razonable;
iv. de forma entendible: y,

c) desafiar la exactitud de la información relacionada con ellos y, si es posible y como sea adecuado, rectificar, completar, corregir o borrar la información.

Tal acceso y oportunidad para corrección deberá ser proporcionado, excepto cuando:
(i) la carga o el gasto de hacerlo no fuera razonable ni proporcional a los riesgos sobre la privacidad del individuo en el caso en cuestión;
(ii) la información no deberá ser revelada por razones legales o de seguridad, ni para proteger información comercial confidencial; o
(iii) la privacidad de la información de personas, y no del individuo, fuera violada.

Si una solicitud bajo (a) o (b), o un desafío bajo (c) es negada, se deberán proporcionar al individuo las razones del por qué, y éste será capaz de desafiar tal negación.

IX. Responsabilidad

Un controlador de información personal deberá ser responsable de cumplir con medidas que causen efecto al Principio estipulado arriba. Cuando la información personal vaya a ser transferida a otra persona u organización, nacional o internacional, el controlador de la información personal deberá obtener consentimiento del individuo o actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con estos Principios.

Parte IV. Implementación

La Parte IV proporciona orientación a las Economías Miembro sobre la implementación del Marco de Privacidad de APEC. La Sección A se enfoca en aquellas medidas que las Economías Miembro deben considerar para implementar el Marco dentro de su país, mientras que la Sección B expone las amplias disposiciones de APEC para la implementación de los elementos transfronterizos de Marco.

A. Orientación para la implementacion interna

I. Maximizando Beneficios de Protección a la Privacidad y Flujos de Información
Las Economías deberán respetar el siguiente concepto básico al considerar la adopción de medidas diseñadas para la implementación interna del Marco de Privacidad de APEC:

Reconociendo el interés de la Economías para maximizar los beneficios económicos y sociales disponibles para sus ciudadanos y empresa, la información personal deberá

ser recopilada, guardada, procesada, usada, transferida y revelada de tal manera que se proteja la privacidad de la información individual y que les permita darse cuenta de los beneficios de los flujos de información dentro y fuera de las fronteras.

Por consiguiente, como parte de establecer o revisar sus protecciones a la privacidad, las Economías Miembro, en concordancia con el Marco de Privacidad de APEC y con cualquier protección interna a la privacidad ya existente, deberán tomar todas las medidas razonables y apropiadas para identificar y remover barreas innecesarias a los flujos de información y evitar la creación de tales barreras.

II. Haciendo efectivo el Marco de Privacidad de APEC

Hay varias opciones para hacer efectivo el Marco de Privacidad y asegurar la protección de la privacidad de los individuos, incluyendo métodos legislativos, administrativos, autorreguladores de la industria, o la combinación de estos, sobre qué derechos pueden ser ejercitados bajo el Marco. Además, las Economías Miembro deben considerar tomar medidas para establecer punto(s) de acceso o mecanismos para proporcionar información, por lo general acerca de protecciones a la privacidad dentro de su jurisdicción. En la práctica, se supone que el Marco debe ser implementado, incluyendo a través de las autoridades centrales, cuerpos conformados por varias agencias de seguridad, una red de cuerpos industriales designados, o una combinación de los anteriores, tal como las Economías Miembro lo consideren apropiado.

Como se estableció en el Párrafo 31, los medios para hacer efectivo el Marco puede diferir entre las Economías Miembro, y puede ser apropiado para las Economías individuales, el determinar que diferentes Principios de Privacidad de APEC pueden requerir diferentes medios de implementación. Cualquier acercamiento que sea adoptado en una circunstancia en particular, la meta general deberá ser adoptar compatibilidad en los acercamientos en la protección a la privacidad en la región de APEC, que es respetuosa de los requerimientos de las Economías individuales.

Las Economías de APEC son estimuladas para adoptar prácticas no discriminatorias para proteger a los individuos de violaciones a la protección de la privacidad que ocurran en la jurisdicción de esa Economía Miembro.

Discusiones con agencias de seguridad internas, seguridad, salud pública y otras agencias son importantes para identificar maneras para fortalecer la privacidad sin crear obstáculos para la seguridad nacional, seguridad pública y otras misiones de políticas públicas.

III. Educando y divulgando protecciones internas a la privacidad

Para todas las Economías Miembro, en particular aquellas en las etapas iniciales del desarrollo de sus acercamientos internos a las protecciones a la privacidad, el Marco

tiene la intención de proporcionar orientación para desarrollar sus acercamientos.
Para que el Marco tenga efectos prácticos, debe ser conocido y accesible. En consecuencia, las Economías Miembro deben:

a. divulgar las protecciones a la privacidad que proporcionen a los individuos;
b. educar a los controladores de información personal acerca de las protecciones a la privacidad de la Economía Miembro; y,
c. educar a los individuos acerca de cómo pueden reportar violaciones y cómo pueden buscarse remedios.

IV. Cooperación entre los Sectores Público y Privado

La participación activa de entidades no gubernamentales ayudará a asegurar que puedan realizarse todos los beneficios del Marco de Privacidad de APEC. En consecuencia, las Economías Miembro deben dialogar con grupos relevantes del sector privado, incluyendo grupos de privacidad y aquellos representando a consumidores y a la industria, para obtener aportes en asuntos de protección a la privacidad y cooperación para fomentar los objetivos del Marco. Además, en especial en las Economías en las que no se han establecido regímenes de protección a la privacidad en su jurisdicción interna, las Economías Miembro deben poner mucha atención al hecho de que las opiniones del sector privado sean reflejadas al desarrollar protecciones a la privacidad. En particular, las Economías Miembro deben buscar cooperación de entidades no gubernamentales en la educación pública y fomentar el envío de quejas a las agencias de seguridad de la privacidad, al igual que su continua cooperación en la investigación de esas quejas.

V. Proporcionando remedios apropiados in situaciones en las que sean violadas las protecciones a la privacidad

El sistema de protección a la privacidad de una Economía Miembro debe incluir una apropiada selección de remedios para las violaciones a la protección de la privacidad, tales como: reparación, la habilidad de detener una violación cuando esté en proceso, y otros remedios. Para determinar el rango de los remedios para las violaciones a la protección a la privacidad, un número de factores deben ser tomados en cuenta por una Economía Miembro, incluyendo:

a. el sistema particular en esa Economía Miembro para proporcionar protecciones a la privacidad (por ejemplo, poderes legislativos para hacer cumplir las leyes, que pueden incluir derechos de los individuos para ejercer acción legal, autorregulación de la industria, o una combinación de sistemas); y
c. la importancia de tener un rango de remedios acorde con la extensión actual o potencial del daño a los individuos que resulte de tales violaciones.

VI. Mecanismo para Implementación de la Cobertura Interna del Marco de Privacidad de APEC
Las Economías Miembro deben dar a conocer a APEC, la implementación interna del Marco a través de la finalización de y actualizaciones periódicas del Plan de Acción Individual (IAP) sobre Privacidad de la Información.

B. Orientación para la implementación internacional

Para tratar la implementación internacional del Marco de Privacidad de APEC y de acuerdo con las provisiones de la Parte A, las Economías Miembro deben considerar los siguientes puntos relacionados con la protección a la privacidad de la información personal:

I. Información compartida por las Economías Miembro
Las Economías Miembro son alentadas para compartir e intercambiar información, sondeos e investigación con respecto a cuestiones que tengan impacto significativo sobre la protección de la privacidad.

Para fomentar los objetivos de los párrafos 35 y 36, las Economías Miembro son alentadas a educarse unas a otras en asuntos relacionados con la protección de la privacidad y a compartir e intercambiar información sobre programas promocionales, educacionales y de entrenamiento, con el propósito de despertar la conciencia pública y mejorar el entendimiento de la importancia de la protección a la privacidad y la conformidad con leyes y normas relevantes.

Las Economías Miembro son alentadas a compartir experiencias sobre varias técnicas para investigar violaciones a protecciones a la privacidad y estrategias reguladoras para resolver disputas que involucren tales violaciones incluyendo, por ejemplo, manejo de quejas y mecanismos para la resolución alternativa de disputas.

Las Economías Miembro deben designar y dar a conocer a las otras Economías Miembro, las autoridades públicas dentro de sus jurisdicciones, que serán responsables de facilitar la cooperación transfronteriza y de compartir información acerca de la protección a la privacidad entre las Economías.

II. Cooperación Transfronteriza en Investigación y Aplicación de la Ley
Desarrollar compromisos de colaboración: Tomando en consideración compromisos internacionales ya existentes y acercamientos autorreguladores en desarrollo o ya existentes (incluyendo aquellos a los que se hace alusión en la Parte B. III, abajo) y al alcance permitido por la ley y la política interna, las Economías Miembro deben considerar desarrollar compromisos de colaboración y procedimientos para facilitar la cooperación transfronteriza para hacer cumplir las leyes de privacidad. Dichos compromisos de co-

laboración pueden tomar la forma de compromisos bilaterales o multilaterales. Este párrafo puede ser interpretado pensando en el derecho de las Economías Miembro a declinar o limitar la cooperación sobre investigaciones particulares acerca de cuestiones por motivos de que la conformidad con la solicitud de cooperación fuera inconsistente con leyes internas, políticas o prioridades, o por motivos de restricciones de recursos o basado en la ausencia de interés mutuo en la investigación en cuestión.

En el cumplimiento de leyes civiles de privacidad, los compromisos de colaboración transfronteriza puede incluir los siguientes aspectos:

a. mecanismos para notificar puntual, eficiente y sistemáticamente a las autoridades públicas designadas en otras Economías Miembro, de la investigación o de casos de privacidad en los que deba hacerse cumplir la ley, que sean objeto de conductas ilícitas o que provoquen daños a individuos de esas Economías;

b. mecanismos para compartir información necesaria de manera eficiente, para la exitosa cooperación en investigaciones de privacidad transfroterizas y en casos en los que debe hacerse cumplir la ley;

c. mecanismos para investigar asistencia en casos de privacidad en los que deba hacerse cumplir la ley;

d. mecanismos para dar prioridad a casos para cooperación con autoridades públicas en otras Economías, basada en la severidad de las violaciones a la privacidad de la información personal, el daño actual o potencial involucrado, así como otras consideraciones relevantes;

e. pasos para mantener el nivel apropiado de confidencialidad con respecto a la información intercambiada bajo compromisos de colaboración.

III. Colaboración en el Desarrollo de Reglas de Privacidad Transfronterizas

Las Economías Miembro se esforzarán para apoyar el desarrollo y reconocimiento o aceptación de reglas de privacidad transfronterizas en la región de APEC, reconociendo que las organizaciones seguirán siendo responsables de cumplir con los requerimientos locales de protección de datos, así como con todas las leyes aplicables. Tales reglas de privacidad transfronterizas deben adherirse a los Principios de Privacidad de APEC.

Para hacer efectivas las reglas de privacidad transfronterizas, las Economías Miembro se esforzarán para trabajar con depositarios apropiados para desarrollar marcos o mecanismos para el mutuo reconocimiento o aceptación de dichas reglas de privacidad transfronterizas entre las Economías.

Las Economías Miembro deberán esforzarse para asegurar que dichas reglas de privacidad transfronterizas y el reconocimiento o aceptación de mecanismos, faciliten transferencias transfronterizas responsables de datos y protecciones efectivas a la privacidad sin crear barreras innecesarias a los flujos transfronterizos de información, incluyendo cargas administrativas y burocráticas innecesarias para las empresas y los consumidores.

Artículo 8. Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

* Aprobada el 7 de diciembre de 2000, en la Cumbre de Jefes de Estado y de Gobierno de la Unión Europea.

Declaración de Santa Cruz de la Sierra*

La inclusión social, motor del desarrollo de la Comunidad Iberoamericana

1. Los Jefes de Estado y de Gobierno de los 21 países iberoamericanos, reunidos en la XIII Cumbre Iberoamericana en la ciudad de Santa Cruz de la Sierra, Bolivia, reiteramos nuestro propósito de seguir fortaleciendo la Comunidad Iberoamericana de Naciones como foro de diálogo, de cooperación y de concertación política, profundizando los vínculos históricos y culturales que nos unen, admitiendo, al mismo tiempo, los rasgos propios de cada una de nuestras múltiples identidades que nos permiten reconocernos como una unidad en la diversidad...

44. Concordamos en que la revolución informática y tecnológica abre mayores posibilidades de participación social, económica y política. Las tecnologías de la información son herramientas indispensables para la promoción del desarrollo económico y social de nuestros países Es importante evitar que la sociedad de la información genere nuevas formas de exclusión. La reducción de la brecha digital, el desarrollo de la infraestructura para la conectividad y el acceso universal deben ser objetivos fundamentales de las políticas de construcción de la sociedad de la información. Consideramos que la administración de Internet debe realizarse a través de una gestión amplia, transparente, participativa y democrática en la que intervengan los gobiernos los organismos internacionales, la empresa privada y la sociedad civil. Consideramos que junto con maximizar las ventajas que se derivan de estas innovaciones tecnológicas es necesario también evitar nuevas formas de exclusión y discriminación tecnológicas, desarrollando proyectos de cooperación en materia de tecnologías de información. Nos proponemos trabajar por estos objetivos y por la promoción de la diversidad cultural y lingüística en la próxima Cumbre Mundial de la Sociedad de la Información.

45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad...

* Dada en Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003, durante la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Versión completa de la Declaración, disponible en el vínculo: http://www.oei.es/xiiicumbredec.htm

Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana*

I. Introducción

El documento sobre desarrollos normativos y armonización, elaborado por el Grupo de Trabajo Permanente de Desarrollo Normativo de la Red Iberoamericana de Protección de Datos en la reunión celebrada en Santa Cruz de la Sierra (Bolivia) los días 3 a 5 de mayo de 2006, considera como una de las máximas prioridades en los trabajos de la Red la elaboración de una propuesta de Directrices contribuir a las iniciativas regulatorias de la Protección de Datos que surjan en la Comunidad Iberoamericana.

El establecimiento de un marco armonizado de protección de datos a nivel global ha sido el principal fundamento de la adopción de los distintos instrumentos internacionales actualmente existentes en materia de protección de datos.

Se trata así de garantizar que el desarrollo del comercio a nivel mundial resulte compatible con la protección de los derechos de las personas, especialmente en lo que se refiere a la protección de la información que les concierne.

De este modo, el establecimiento de un marco homogéneo de regulación del derecho a 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 de este derecho, garantizará el desarrollo del comercio en la zona, facilitando el intercambio de información entre los distintos operadores ubicados en los Estados Iberoamericanos y de éstos con terceros países, en particular los Estados miembros de la Unión Europea, en condiciones que no se vean restringidas como consecuencia del distinto nivel de protección del derecho fundamental a la protección de datos de carácter personal.

Así, el Preámbulo de la Recomendación del Consejo de la OCDE, relativa a las Directrices que rigen la protección de la intimidad y la circulación transfronteriza de datos de carácter personal, aprobada el 23 de septiembre de 1980, ya reconoce expresamente que "la circulación transfronteriza de datos personales contribuye al desarrollo

---

*Adoptadas por la Red Iberoamericana de Protección de Datos en el año 2007.

económico y social", pero al propio tiempo recuerda que "la legislación nacional relativa a la protección de la intimidad y de la circulación transfronteriza de datos personales puede obstaculizar tal circulación transfronteriza".

Por este motivo, la Recomendación parte del objetivo esencial de "fomentar la libre circulación de información entre los países miembro y a evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales entre los países miembros". Se pretende así que el intercambio transfronterizo de información no pueda verse limitado por la legislación nacional de protección de datos, pero al propio tiempo garantizar la adecuada protección de este derecho fundamental.

Con mayor claridad si cabe, 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, expresa esta idea en los apartados 6 a 9 de su Exposición de Motivos, indicando lo siguiente:

> (6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;
>
> (7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;
>
> (8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para

aproximar las legislaciones;
(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;"

La mayor parte de las Constituciones de los Estados que constituyen la Comunidad Iberoamericana contienen disposiciones que garantizan a la persona el derecho fundamental a la protección de sus datos personales y el "*habeas data*". Estas previsiones se completan además con las resoluciones dimanantes de los Tribunales de Justicia y, en particular de los Tribunales o Cortes Constitucionales.

Se reconoce así, a través del cauce constitucional y jurisprudencial un derecho fundamental de las personas a la protección de sus datos de carácter personal, independiente y autónomo del derecho a la intimidad, consistente en el derecho del individuo a disponer libremente de la información que le concierna.

Teniendo ello en cuenta, es preciso que los poderes públicos adopten las medidas necesarias para garantizar a las personas la salvaguarda del derecho fundamental, como garantía esencial del estado de derecho.

Sin embargo, el reconocimiento del derecho fundamental debería, como se ha señalado, complementarse con el establecimiento de un marco normativo uniforme, que permita garantizar un nivel equivalente de protección de este derecho, a través del reconocimiento normativo de los principios, derechos y deberes que lo configuran. De este modo podrá asegurarse que, encontrándose plenamente garantizado el derecho fundamental, los Estados Iberoamericanos se beneficien del enriquecimiento económico, social y cultural que puede derivarse del libre intercambio transfronterizo de la información que contiene datos de carácter personal.

El presente documento tiene por objeto delimitar esos perfiles esenciales que configuran el derecho fundamental a la protección de datos de carácter personal, con el

objeto de ofrecer a los poderes públicos de los Estados Iberoamericanos unos criterios orientativos que puedan resultar de utilidad en el desarrollo de las iniciativas normativas que puedan adoptarse, facilitando así el establecimiento de un marco homogéneo de protección que facilite el intercambio de los flujos de información entre todos ellos y desde y hacia terceros Estados que han adoptado estándares similares de protección.

2. El contenido esencial del derecho a la protección de datos personales. Criterios de armonización.

Como ya se ha señalado, la mayor parte de los derechos de los Estados Iberoamericanos reconocen, bien por referencia directa de su Constitución, bien como consecuencia de las decisiones adoptadas por sus órganos judiciales, el derecho de la persona a la protección de datos de carácter personal, esencialmente mediante el reconocimiento del recurso al "*habeas data*", mediante el cual el individuo podrá tomar conocimiento de los datos referidos al mismo y de la finalidad para la que están siendo tratados por un determinado responsable del tratamiento, pudiendo en su caso instar su rectificación, cancelación o actualización.

El ejercicio de este derecho ha dado lugar a una rica jurisprudencia que ha evolucionado hacia el reconocimiento de una serie de principios a los que deben someterse las Administraciones Públicas y las entidades privadas que tratan datos de carácter personal.

En Colombia, la Corte Constitucional a través de más de 140 sentencias ha definido el alcance y características del habeas data así como las condiciones que deben rodear el tratamiento de los datos personales consagrado en el artículo 15 de la Constitución de 1991.

Desde la primera sentencia (T 414/92) la Corte ha establecido que la persona es el titular y propietario del dato personal. Para ella es obligación de los administradores de bancos de datos administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante y no atentar contra los derechos fundamentales de las personas. La Corte Constitucional señaló, de manera general, que "*la función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*". Concretamente, ha precisado que los administradores deben: (1) Obtener previamente la autorización de la persona cuyos datos se pretende incluir en la base; (2) Notificar a la persona sobre la inclusión de sus datos en el banco e informarle que va a reportar su información en una base de datos con miras a que el titular pueda desde un comienzo ejercer sus derechos de rectificación y actual-

ización;(3) Actualizar permanente y oficiosamente la información para que ésta sea veraz, completa y no se omitan factores que pueden cambiar el buen nombre de la persona; (4) Eliminar de oficio la información negativa que ha caducado con el paso del tiempo; (5) Indemnizar los perjuicios causados por la falta de diligencia o por posibles fallas en el manejo, tratamiento o administración de datos personales; (6) Garantizar el derecho de acceso, actualización y corrección. Estos derechos implican que la persona tenga "*la posibilidad (...) de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él"; (...)si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados*". Finalmente, la Corte ha precisado que, por regla general, "*no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*".

En España, la Sentencia 292/2000, de 30 de noviembre, tras desvincular el derecho a la protección de datos del derecho a la intimidad, señala que "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso*", añadiendo que "*estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero*". Así, se concluye que "*son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele*".

En México, el derecho a la protección de datos personales se aplica en el ámbito de los ficheros públicos a nivel federal en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LAI), y cada legislatura estatal, en el marco de sus leyes de acceso a la información, incluyen capítulos ad-hoc.

Actualmente, existen dos iniciativas de reforma constitucional, la primera presentada

ante la Cámara de Senadores que adiciona el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos para reconocer al derecho a la protección de datos personales, como un derecho fundamental, mismo que fue aprobado en la anterior legislatura y fue enviado a la Cámara de Diputados para los efectos constitucionales correspondientes, estando aún pendiente su discusión y aprobación en ésta última. La segunda iniciativa se presentó el pasado 27 de marzo de 2007 de abril, que vendría a reforzar la señalada anteriormente, ya que dota al Congreso de facultades expresas para expedir la ley de la materia, esgrimiendo que es relevante no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino por los efectos esenciales que estos tienen sobre la economía nacional. *Finalmente, es de señalar que el Pleno del IFAI, en su sesión del 25 de abril de 2007, aprobó por unanimidad* que se conforme un grupo de trabajo entre el sector privado y dicho instituto, para la elaboración de un borrador de proyecto de Ley en materia de Protección de Datos Personales.

En el Perú diversa jurisprudencia del Tribunal Constitucional se ha pronunciado sobre el reconocimiento del derecho a la autodeterminación informativa que reconoce el artículo 2°, inciso 6) de la Constitución Política de 1993 y, asimismo ha señalado el objeto de este derecho, su naturaleza relacional y marcado las diferencias entre éste y otros derechos humanos como los de la intimidad, imagen e identidad personal.

Así por ejemplo, la sentencia de fecha 29 de enero recaída en el Exp. N° 1797- 2002-HD/TC, señala que *"El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución (...) por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran* muchas veces vinculadas a la protección de otros derechos constitucionales." La sentencia citada ratifica lo expresado en la sentencia recaída en el Exp. N°. 666-1996-HD/TC , precisando lo que incluye la protección del derecho a la autodeterminación informativa a través del hábeas data, señalando que comprende: *"en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la*

finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.".

Por su parte, en Europa, el derecho fundamental a la protección de datos de carácter personal ha sido expresamente reconocido como derecho fundamental y claramente diferenciado del derecho a la intimidad personal y familiar de las personas por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, cuyo artículo 8 establece lo siguiente:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Los apartados 2 y 3 de este precepto delimitan el contenido esencial que debe revestir la legislación que regule el derecho fundamental a la protección de datos de carácter personal. De este modo:

-Los datos deberán ser tratados de modo leal.

-Los datos deberán ser tratados para fines concretos.

-El tratamiento deberá efectuarse sobre la base del consentimiento del interesado o como consecuencia de algún otro fundamento legítimo y previsto legalmente.

-Toda persona tendrá los derechos de acceso, rectificación y cancelación al tratamiento.

-Deberá existir una autoridad independiente encargada de velar por la garantía del derecho.

Por otra parte, distintos instrumentos internacionales, procedentes de Organismos Supranacionales de los que son miembros todos o parte de los Estados Iberoamericanos han venido a establecer los principios básicos que configuran el derecho a la protección de datos personales.

Así, la ya citada recomendación de la OCDE delimita estos principios, enumerando como básicos los siguientes.

1. Aplicación a todo tratamiento de datos del sector público y del privado
2. Interpretación restrictiva de las posibles exclusiones a la aplicación de los principios
3. Principio de limitación de la recogida
4. Principio de calidad de los datos
5. Principio de especificación de la finalidad
6. Principio de limitación de uso
7. Principio de salvaguardas de seguridad
8. Principio de apertura
9. Principio de participación individual (Habeas data)
10. Principio de responsabilidad
11. Garantías de la circulación transfronteriza, ininterrumpida y segura, de los datos personales, entre los Estados que observen los principios
12. Establecimiento de sanciones y recursos suficientes en caso de incumplimiento.

A su vez, deben tenerse en cuenta las Directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante Resolución 45/95 de la Asamblea General de las naciones Unidas, de 14 de diciembre de 1990, que consideran como garantías mínimas que deben prever las legislaciones nacionales los siguientes principios:

1. Principio de legalidad y lealtad
2. Principio de exactitud
3. Principio de especificación de la finalidad
4. Principio de acceso de la persona interesada
5. Principio de no discriminación
6. Limitación de la facultad para hacer excepciones
7. Principio de seguridad
8. Supervisión y sanciones, a través de una autoridad que deberá ofrecer garantías de imparcialidad, independencia y competencia técnica 9. Flujo transfronterizo de datos basado en la similitud de las salvaguardas10. Campo mínimo de aplicación general a todos los archivos informatizados públicos y privados.

Junto con estos instrumentos, no debe olvidarse el análisis producido en el ámbito de la Unión Europea en cumplimiento de la Directiva 95/46/CE. La importancia de la Directiva en el ámbito supraeuropeo resulta esencial, en primer lugar, dado que se trata del texto internacional que regula con mayor precisión y detalle los principios, derechos

y deberes que configuran el derecho fundamental a la protección de datos.

Además, debe recordarse que el fundamento de la Directiva, como ya se ha indicado consiste en establecer un marco armonizado de protección del derecho a la protección de datos personales que garantice el libre flujo de información en el ámbito de la Unión Europea, favoreciendo así el comercio y el enriquecimiento derivado de los flujos de información.

Por último, no debe olvidarse que los artículos 25 y 26 de la Directiva establecen un régimen específico para los flujos transfronterizos de datos de carácter personal, exigiendo, como punto de partida, que el Estado al que se destinen los datos ofrezca un nivel adecuado de protección de datos de carácter personal. De este modo, la Directiva da cumplimiento al principio esencial de equilibrio entre la libre transmisión de información y la protección del derecho de las personas.

Por tanto, la asunción de principios que puedan considerarse "adecuados" a los previstos en la Directiva puede constituirse como un punto de partida adecuado para facilitar los flujos transfronterizos de información a ambos lados del Atlántico manteniendo unas adecuadas garantías del derecho fundamental a la protección de datos de carácter personal. No se trata así de obtener una aplicación transfronteriza de la legislación europea, sino de lograr una adecuada conciliación entre ambos.

En el ámbito Iberoamericano, deben citarse los esfuerzos realizados en el ámbito de la UNESCO y la Estrategia Latinoamericana de la Sociedad de la Información (ELAC) llevada a cabo en el seno de la CEPAL, con el objeto de lograr el diseño de mecanismos de armonización normativa en el ámbito de la privacidad y protección de datos personales.

Asimismo, debe señalarse que algunos Estados han adoptado en los últimos años iniciativas en este sentido. Así, no debe olvidarse los desarrollos normativos llevados a cabo por Argentina, que culminaron en la Adopción de la Decisión de la Comisión de 30 de junio de 2003, por la que se considera que dicho Estado garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad.

En este marco, puede resultar interesante para el análisis la actividad desarrollada por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE; en particular su Dictamen 4/2002, de 3 de octubre, sobre el nivel de protección de datos personales en Argentina.

Los diversos dictámenes aprobados en el seno del mencionado Grupo de Trabajo en relación con el nivel de protección de datos en terceros Estados han tomado como referente el documento de trabajo del Grupo sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado el 24 de julio de 1998, cuyo Capítulo 1 analiza qué debe entenderse por "protección adecuada".

A tal efecto, el documento delimita dos tipos de análisis que habrían de efectuarse sobre la legislación del Estado de destino de los datos, a fin de poder delimitar si la misma resulta adecuada: el relativo a su contenido sustantivo y el relacionado con los mecanismos y procedimientos de aplicación de la legislación sustantiva.

n cuanto al contenido sustantivo, la legislación del Estado de destino habría de contener los principios básicos de protección de datos que tradicionalmente han venido siendo reconocidos por los acuerdos y directrices internacionales adoptados en este ámbito, y que se han señalado con anterioridad, considerándose como tales los siguientes:

1. Limitación de la finalidad
2. Calidad y proporcionalidad de los datos
3. Transparencia
4. Seguridad y confidencialidad
5. Derechos de acceso, rectificación, supresión y bloqueo de los datos
6. Restricciones a la transferencia ulterior
7. Categorías especiales de datos
8. Marketing directo
9. Decisión individual automatizada

Estos principios, como mínimo, deberían aparecer recogidos en la legislación del Estado destinatario de los datos para que pudiera considerarse que el mismo ofrece un nivel adecuado de protección.

Lógicamente, para que pueda considerarse que existe un efectivo reflejo legal de estos principios en la legislación del Estado en cuestión será preciso que dicha normativa tenga un ámbito general de aplicación a los tratamientos efectuados por los sectores público y privado, de forma que no se establezcan más límites a su aplicación que los relacionados con la actividad meramente personal o familiar de quien los lleva a cabo o sean adecuadas limitaciones al derecho fundamental en el marco de actividad de una sociedad democrática.

Por otra parte, en cuanto al análisis referido a los procedimientos de aplicación de las normas sustantivas, el documento considera que la existencia de los mismos es indispensable para que un sistema de protección de datos pueda, en la práctica, otorgar un nivel adecuado de protección, dado que supone la existencia de mecanismos de control de los principios contenidos en las leyes nacionales.

Tal y como indica el documento este elemento se materializa generalmente en el establecimiento de una autoridad independiente de protección de datos y en la regulación de procedimientos adecuados que permiten a los afectado obtener la protección de sus derechos o la reparación de los perjuicios que les han sido causados.

Así, como regla general, podrá considerarse que el Estado otorga un nivel de protec-

ción adecuado en los supuestos en los que el mismo cuente con una norma reguladora de la protección de datos que contenga los principios sustantivos que se han enumerado y exista una autoridad encargada de velar por su cumplimiento, ante la cual los interesados puedan dirigir sus reclamaciones y que ostente poderes de inspección e investigación de los tratamientos.

Un último requisito esencial de dicha autoridad será su capacidad para imponer medidas que garanticen la efectividad del derecho, tales como sanciones en caso de incumplimiento o, cuando menos, la capacidad para instar a los Tribunales la imposición de esas medidas en los casos en los que del uso de sus poderes de investigación se desprenda que existe una vulneración de la normativa de protección de datos.

El análisis que se ha descrito ha permitido al Grupo dictaminar favorablemente la adecuación del nivel de Protección de Datos personales de los Estados respecto de los que posteriormente se ha adoptado una Decisión en este sentido por parte de la Comisión. Basta con analizar el ya citado Dictamen 4/2002, referido al nivel de protección de datos en Argentina, para comprobar que su estructura y análisis se fundamenta en lo establecido en el citado documento de trabajo.

3. Directrices (principios, derechos y obligaciones) que deberá contener una Ley nacional de protección de datos de carácter personal:

1. Ámbito de aplicación

1.1. Las presentes directrices serán de aplicación a todo tratamiento manual o automatizado de datos de carácter personal, entendiéndose como tales cualquier información referida a personas físicas identificadas o identificables. En consecuencia, las directrices serán aplicables a los tratamientos llevados a cabo por todas las entidades de los sectores público y privado.

1.2. No obstante, será posible excluir de las directrices el tratamiento manual o no automatizado cuando los datos objeto de tratamiento no vayan a ser incorporados a un fichero estructurado con arreglo a criterios que permitan la identificación de las personas cuyos datos son sometidos a tratamiento

1.3. Igualmente, no serán aplicables las directrices al tratamiento de datos de carácter personal, automatizado o manual, que una persona física realice para fines exclusivamente relacionados con su vida privada o familiar.

1.4. Será posible la exclusión de la aplicación de los apartados 2, 3, 4, 5, 6.1, 6.2, 6.3 y 8 de las presentes directrices mediante una Ley nacional de determinados tratamientos

de datos de carácter personal en la medida que la aplicación de las directrices pudiera suponer un riesgo para la protección de la seguridad nacional, el orden público, la salud pública o la moralidad y dicha medida resulte estrictamente necesaria y no excesiva en el ámbito de una sociedad democrática.

2. Principios relacionados con la finalidad y calidad de los datos

2.1. Tratamiento leal y lícito: los datos sólo podrán ser recabados y tratados de buena fe, con estricto respeto por la Ley y los derechos de las personas y de conformidad a lo previsto en las presentes directrices.
2.2. Limitación de la finalidad: los datos únicamente podrán ser recabados y tratados para el cumplimiento de las finalidades determinadas, explícitas y legítimas relacionadas con la actividad de quien los trate.

No podrán ser tratados para fines distintos de aquéllos que motivaron su obtención a menos que exista legitimación suficiente para ello, conforme a lo establecido en el apartado 3 de estas directrices.
2.3. Principio de proporcionalidad: Sólo podrán ser sometidos a tratamiento los datos que resulten adecuados, pertinentes y no excesivos en relación con las finalidades a las que se refiere el punto anterior.
2.4. Principio de exactitud: Los datos deberán mantenerse exactos, completos y puestos al día, respondiendo a la verdadera situación de la persona a la que se refieran.
2.5. Principio de conservación: Los datos deberán ser cancelados o convertidos en anónimos cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades que justificaron su obtención y tratamiento

3. Legitimación para el tratamiento

3.1. Los datos sólo podrán ser recabados o tratados en caso de que se hubiera obtenido el consentimiento del interesado.
3.2. No obstante la Ley podrá establecer supuestos en los que no será necesario el consentimiento del interesado para el tratamiento de sus datos personales, atendiendo a las circunstancias que concurran en cada supuesto y, en todo caso, siempre que dicha excepción no perjudique los derechos fundamentales del interesado. En particular, la Ley podrá permitir el tratamiento de los datos sin contar con el consentimiento del interesado cuando el mismo se realice en el marco de una relación jurídica o por una Administración en el ejercicio de las potestades que le hayan sido atribuidas.

3.3. Los datos que revelen la ideología, afiliación sindical, religión o creencias del afectado sólo podrán ser tratados con su consentimiento, a menos que aquél los hubiera hecho

manifiestamente públicos.
3.4. Los datos relacionados con la salud, el origen racial y la vida sexual del afectado únicamente podrán ser recogidos y tratados en los supuestos mencionados en el párrafo anterior o cuando una Ley así lo disponga.
3.5 En todo caso las presentes directrices no obstaculizarán el adecuado tratamiento médico del interesado ni la atención de una urgencia vital del mismo.

4. Transparencia e información al interesado

4.1 El interesado del que se recaben los datos deberá ser informado al tiempo de su recogida de la identidad del responsable del tratamiento, los fines para los que los datos vayan ser tratados y el modo en que podrá hacer efectivos los derechos a los que se refieren los apartados 5 y 6 de estas directrices, así como de cualquier otra información necesaria para garantizar un tratamiento lícito de los datos. Esta obligación solamente quedará exceptuada si el interesado hubiera sido ya informado con anterioridad de estas circunstancias.
4.2. Cuando los datos no hayan sido obtenidos del interesado deberá informarse al mismo de los extremos previstos en el párrafo anterior en un plazo prudencial de tiempo y, en todo caso, con anterioridad a que los datos sean comunicados a un tercero.

5. Derechos de acceso, rectificación y cancelación de los interesados

El interesado cuyos datos sean objeto de tratamiento podrá, a través de procedimientos claros, expeditos y gratuitos o sin gastos excesivos:
5.1 Recabar del responsable del tratamiento confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos.
5.2. Recabar del responsable del tratamiento información, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos.
5.3. Exigir, en su caso, la rectificación o cancelación de los datos que pudieran resultar incompletos, inexactos, inadecuados o excesivos, con arreglo a lo previsto en las presentes directrices.
5.4. Exigir que se notifique a los terceros a quienes se hayan comunicado los datos de toda rectificación o cancelación efectuado conforme al párrafo anterior.

6. Otros derechos de los interesados

Además de los derechos a los que se refiere el apartado anterior, los interesados tendrán los siguientes:
6.1. No verse sometidos a decisiones con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad o conducta. No obstante, será posible la adopción de dichas decisiones cuando se verifiquen en el marco de una relación jurídica libremente aceptada por el interesado, en que se concede al mismo la posibilidad de efectuar alegaciones acerca del resultado de la valoración.
6.2. Oponerse al tratamiento de sus datos, en supuestos no excluidos en virtud de la Ley, como consecuencia de la concurrencia de una razón excepcional y legítima derivada de su concreta situación personal.
6.3. Oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable vaya a llevar a cabo un tratamiento para actividades vinculadas con la publicidad y la prospección comercial.
6.4. Recabar el auxilio de los tribunales y de las autoridades a las que se refiere el apartado 9 de estas directrices en caso de considerar que el tratamiento de sus datos se está llevando a cabo con conculcación de las mismas.
6.5. Ser indemnizados por cualquier daño o lesión que hubieran sufrido en sus bienes o derecho como consecuencia del tratamiento de datos llevado a cabo con conculcación de lo dispuesto en estas directrices.

7. Seguridad y confidencialidad en el tratamiento

7.1. Deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.
7.2. Quienes intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

8. Limitaciones a la transferencia internacional de datos

8.1. Como regla general sólo podrán efectuarse transferencias internacionales de datos al territorio de Estados cuya legislación recoja lo dispuesto en las presentes directrices.
8.2. No obstante la Ley podrá establecer supuestos en que, excepcionalmente, sea posible la transferencia internacional de datos a otros Estados, atendiendo a las circunstancias

que concurran en cada supuesto. En todo caso, deberán tenerse en cuenta los derechos e intereses del afectado y, en particular, si el mismo ha prestado su consentimiento a la transferencia en cuestión.

8.3. Fuera de los supuestos mencionados en los dos párrafos anteriores, sólo será posible la transferencia internacional de datos en caso de que se obtenga la autorización de la autoridad a la que se refiere el apartado 9, para lo cual será necesaria la aportación por parte del exportador de garantías suficientes para asegurar que el importador cumplirá en todo caso lo dispuesto en estas directrices.

9. Autoridades de control

9.1. La garantía del cumplimiento de estas directrices deberá quedar sujeto al control de una o varias autoridades de protección de datos. Las autoridades podrán tener personalidad propia o encontrarse integradas en la Administración Pública o en un Organismo Público preexistente. Igualmente podrán tener como función exclusiva el cumplimiento de las normas de protección de datos o ejercer tal competencia junto con otras atribuidas por su legislación.

La organización territorial del Estado no podrá suponer un obstáculo para que las garantías derivadas de la existencia de la o las autoridades de protección de datos sean reales y efectivas en relación con todos los tratamientos llevados a cabo tanto por el sector público como por el privado.

9.2. Las autoridades de protección de datos deberán actuar con plena independencia e imparcialidad, no pudiendo estar sometidas en el ejercicio de sus funciones al mandato de ninguna autoridad pública. Deberán establecerse mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.

9.3 Las autoridades deberá tener como mínimo las siguientes competencias:

-Conocer de las reclamaciones que les sean dirigidas por los interesados, en particular en cuanto al ejercicio de los derechos a los que se refiere el apartado 5 de estas directrices.

-Realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de las directrices, pudiendo acceder a los datos que sean objeto de un tratamiento y recabar toda la información necesaria para el cumplimiento de su misión de control.

-Adoptar las medidas que resulten necesarias para evitar la persistencia en el incumplimiento de las directrices.

-Mantener un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer los derechos

reconocidos en las presentes directrices. La solicitud de inscripción se realizará mediante modelos simplificados y basados en estándares técnicos, respetando el principio de neutralidad tecnológica, utilizándose siempre que ello sea posible técnicas o medios electrónicos.

-Autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados cuya legislación no recoja lo dispuesto en las presentes directrices.

-Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.

-Dictaminar los proyectos de disposiciones normativas que puedan afectar al derecho fundamental a la protección de datos personales.

-Divulgar a los individuos y a los poderes públicos el contenido del derecho fundamental a la protección de datos personales.

-Cooperar con las autoridades de protección de datos para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre si y prestarse el debido auxilio mutuo cuando se requiera.

10. Sanciones

10.1. El incumplimiento de las disposiciones que reflejen lo previsto en estas directrices deberá ser sancionado conforme a la legislación interna. La capacidad para la imposición de las correspondientes sanciones podrá corresponder a la autoridad de protección de datos, a la que se refiere el apartado 9 o a los órganos judiciales.

10.2 En todo caso, las autoridades de protección de datos deberán tener capacidad suficiente para recurrir a las vías judiciales que resulten competentes para lograr la adopción de las medidas necesarias para garantizar el cumplimiento de estas directrices y, en particular, la imposición de las sanciones que correspondiesen.

10.3. Si las autoridades de protección de datos fueran directamente competentes para la imposición de sanciones, sus resoluciones deberán ser recurribles ante los Tribunales de Justicia.

Sentencia del Tribunal Constitucional Español 292/2000

En esta materia la sentencia del Tribunal Constitucional de España SCT 292/2000 se erige como un pilar fundamental para comprender la autonomía e independencia del derecho a la protección de datos personales.

A manera de contexto, la litis de la Sentencia 292/2000 del 30 de noviembre del 2000,1 versa sobre el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra los artículos 21.1 y 24.1 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal del 13 de diciembre de 1999.2

De manera paralela en que la Sentencia se pronuncia sobre la inconstitucionalidad de estas disposiciones, en medio de sus razonamientos se van sentado las bases jurídicas que tajantemente reconocen como un derecho fundamental a la protección de datos de carácter personal.

Dada su importancia, a continuación se reproducen dichos argumentos.

> 4. Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.
>
> Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6)…
>
> 5...
>
> Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la

libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del

acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre,

FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.3

Los aspectos centrales de la Sentencia 292/2000 del Tribunal Constitucional español son los siguientes:

El derecho fundamental a la protección de datos persigue garantizar a cualquier persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

El objeto de protección del derecho fundamental a la protección de datos no se reduce a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales.

> El derecho a la protección de datos atribuye a su titular una haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos que se traducen en el derecho a que se requiera el previo consentimiento para la obtención y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho de acceder, rectificar y cancelar dichos datos.

Es así como el derecho a la protección de datos personales se desliga totalmente del derecho a la intimidad para constituirse como un derecho fundamental y autónomo.

Dicho reconocimiento conlleva dotar al titular de los datos con un as de facultades para ejercer el mismo y que, a su vez, se traducen en deberes u obligaciones de hacer a quien posee o trata los mismos (sea el propio Estado, particulares o terceros).

Notas

1 Disponible en el sitio oficial de Internet del Tribunal Constitucional de España en el vínculo: http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467

2 El artículo 21 señala que la Comunicación de datos entre Administraciones públicas: 1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Por su parte el artículo 24 dispone otras excepciones a los derechos de los afectados: 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

3 Disponible en el sitio oficial de internet del Tribunal Constitucional de España.

Decreto por el que se adiciona un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos*

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos. Presidencia de la República.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, EN USO DE LA FACULTAD QUE LE CONFIERE EL ARTÍCULO 135 DE LA CONSTITUCIÓN GENERAL DE LA REPÚBLICA Y PREVIA LA APROBACIÓN DE LA MAYORÍA DE LAS HONORABLES LEGISLATURAS DE LOS ESTADOS, DECLARA ADICIONADO UN SEGUNDO PÁRRAFO AL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

Artículo Único. Se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

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

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que proceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión...

---

* Publicado en el Diario Oficial de la Federación el 01 de junio de 2009.

ARTÍCULO TRANSITORIO

Artículo Único. El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

México, D.F., a 21 de abril de 2009.- Dip. Cesar Horacio Duarte Jaquez, Presidente.- Sen. Gustavo Enrique Madero Muñoz, Presidente.- Dip. Margarita Arenas Guzman, Secretaria.- Sen. Gabino Cué Monteagudo, Secretario.- Rúbricas.

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia, expido el presente Decreto en la Residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a veintiocho de mayo de dos mil nueve.- Felipe de Jesús Calderón Hinojosa.- Rúbrica.- El Secretario de Gobernación, Lic. Fernando Francisco Gómez Mont Urueta.- Rúbrica.

Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos*

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos. Presidencia de la República.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, EN USO DE LA FACULTAD QUE LE CONFIERE EL ARTÍCULO 135 DE LA CONSTITUCIÓN GENERAL DE LA REPÚBLICA Y PREVIA LA APROBACIÓN DE LA MAYORÍA DE LAS HONORABLES LEGISLATURAS DE LOS ESTADOS, DECLARA ADICIONADA LA FRACCIÓN XXIX-O AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

Artículo Único.- Se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I. a XXIX-N...

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.

XXX...

TRANSITORIOS

Primero. El presente Decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo. El Congreso de la Unión deberá expedir la ley en la materia en un plazo no mayor de 12 meses, contados a partir de la entrada en vigor del presente Decreto.

Tercero. En tanto el Congreso de la Unión expide la ley respectiva a la facultad que

---

* Publicado en el Diario Oficial de la Federación el 30 de abril de 2009.

se otorga en este Decreto, continuarán vigentes las disposiciones que sobre la materia hayan dictado las legislaturas de las entidades federativas, en tratándose de datos personales en posesión de particulares.

México, D. F., a 24 de marzo de 2009.- Sen. Gustavo Enrique Madero Muñoz, Presidente.- Dip. César Horacio Duarte Jáquez, Presidente.- Sen. Gabino Cue Monteagudo, Secretario.- Dip. María Eugenia Jiménez Valenzuela, Secretaria.- Rúbricas."

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia, expido el presente Decreto en la Residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a veinticuatro de abril de dos mil nueve.- Felipe de Jesús Calderón Hinojosa.- Rúbrica.- El Secretario de Gobernación, Lic. Fernando Francisco Gómez Mont Urueta.- Rúbrica.

Acuerdo de asociación económica, concertación política y cooperación entre la comunidad Europea y sus Estados Miembros y los Estados Unidos Mexicanos

Este Acuerdo también denominado Tratado de Libre Comercio con la Unión Europea (en adelante, TLCUE), tiene por finalidad fortalecer las relaciones entre las Partes sobre la base de la reciprocidad y del interés común. Para tal fin, el Acuerdo institucionalizará el diálogo político, fortalecerá las relaciones comerciales y económicas a través de la liberalización del comercio de conformidad con las normas de la OMC y reforzará y ampliará la cooperación.*

En materia de protección de datos personales, las Partes firmantes se comprometen a lo siguiente:

Artículo 41. Cooperación en materia de protección de datos
1. Visto el artículo 51, las Partes convienen en cooperar en materia de protección de los datos de carácter personal con vistas a mejorar su nivel de protección y prevenir los obstáculos a los intercambios que requieran transferencia de datos de carácter personal.
2. La cooperación en el ámbito de la protección de datos de carácter personal podrá incluir asistencia técnica a través de intercambios de información y de expertos, y de la puesta en marcha de programas y proyectos conjuntos".

Artículo 51. Protección de los datos
1. Las Partes convienen en garantizar un grado elevado de protección respecto al tratamiento de los datos de carácter personal y de otra índole, de conformidad con las normas adoptadas por los organismos internacionales competentes en la materia y por la Comunidad.
2. A tal efecto, las Partes tendrán en cuenta las normas contempladas en el anexo que forma parte integrante del presente Acuerdo.*

---

* Artículo 2 del TLCUE. Disponible en el vínculo: http://www.economia.gob.mx/pics/pages/5200_5208_1_base/dof2.pdf

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales

Las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales, tienen por objeto constituirse en propuestas y sugerencias específicas que le permitan a la Administración Pública Federal lograr una eficaz protección de los datos personales en su posesión.

Esta Recomendaciones promueven la adopción de medidas de seguridad de índole administrativa, física y técnica necesarias que garanticen la confidencialidad, integridad y disponibilidad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, con base en estándares de seguridad internacionales.

Para lograr lo anterior, las dependencias y entidades federales deberán tomar en consideración los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya sea que provengan de la acción humana o de las condiciones físicas y ambientales, por lo que se establecen distintos niveles de seguridad aplicables a cada categoría o tipo de datos, alojados en los sistemas de datos personales;

Lineamientos de Protección de Datos Personales*

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Instituto Federal de Acceso a la Información Pública.

El Pleno del Instituto Federal de Acceso a la Información Pública, con fundamento en lo dispuesto por los artículos 37 fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y 2 fracción III, 47 y 62 fracciones I y II de su Reglamento, y:

Reconociendo que el respeto a la dignidad de la persona es un valor central de los Estados democráticos que tienen como fundamento la búsqueda de la justicia, la libertad, la igualdad, la seguridad y la solidaridad, y que es a partir de la afirmación de dicha dignidad que existen y se legitiman todos los derechos;

Considerando que en nuestro país, fue voluntad del legislador plasmar en la Constitución Política de los Estados Unidos Mexicanos el derecho a la vida privada también denominada por la doctrina intimidad, como límite a la intromisión del Estado en el ámbito de la persona, al plasmar en su artículo 16 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 del procedimiento", por lo que el derecho a la intimidad tiene dos facetas principales: una que tutela la inviolabilidad del hogar, de las comunicaciones y de las relaciones familiares, y otra que consagra el derecho del individuo a desarrollarse libremente como tal;

Observando que los artículos 6o. y 7o. Constitucionales establecen como límite a la manifestación de las ideas y a la libertad de imprenta respectivamente, el ataque a los derechos de tercero y el respeto a la vida privada, la libertad de expresar o publicar pensamientos encuentra entonces una restricción cuando con ello se menoscabe a la persona. Asimismo, el artículo 6o. consagra el derecho a la información, el cual será garantizado por el Estado, que para efectos de la regulación que en el presente instrumento se emite, se interpreta como el derecho del individuo a tener acceso a la información sobre sí mismo que obra en bancos de datos y a que sus datos no sean manejados de manera indebida;

Reconociendo que a nivel internacional se configura la existencia del derecho humano a la vida privada, por el cual: "ninguna persona puede ser objeto de injerencias ar-

*Publicados en el Diario Oficial el 30 de septiembre de 2005.

bitrarias en su vida privada, su familia, 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". Lo anterior se establece en los siguientes instrumentos internacionales, los cuales por virtud del artículo 133 Constitucional constituyen Ley Suprema de la Unión: la Declaración Universal de los Derechos Humanos -artículo 12-; el Pacto Internacional de Derechos Civiles y Políticos -artículo 17-; la Declaración Americana de los Derechos y Deberes del Hombre -artículo V-; la Convención Americana sobre Derechos Humanos -artículo 11-, y la Convención sobre los Derechos del Niño -artículo 16-;

Recordando que en el marco jurídico vigente en México existen diversas disposiciones que regulan las consecuencias de los ataques o invasiones a la vida privada de las personas en el orden administrativo, civil, penal y de responsabilidad patrimonial del Estado, por lo que existe un acervo jurídico que brinda protección al individuo frente a injerencias ilegales en su vida privada;

Admitiendo que la sociedad de la información, fundada en el avance vertiginoso de la tecnología, ofrece al individuo ventajas diversas que contribuyen a mejorar su calidad de vida y, en el caso del Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste, pero que, al mismo tiempo, una mala utilización de las herramientas tecnológicas puede convertirse en un factor de amenaza a la privacidad y seguridad de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo, ya que las nuevas tecnologías facilitan ilimitadas posibilidades para mover un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;

Reconociendo que como consecuencia de lo anterior, y a efecto de lograr un uso racional y ético de las tecnologías, en el concierto de las naciones se ha legislado en materia de protección de datos personales, por lo cual los individuos gozan de un nuevo derecho denominado a la autodeterminación informativa, como garantía del ciudadano en las modernas sociedades frente al desafío del tratamiento electrónico de sus datos, entendida la garantía como la facultad del individuo de decidir quién, cuándo y bajo qué circunstancias utiliza sus datos personales, tanto en el sector público como en el privado;

Atendiendo a la evolución que ha ocurrido de la noción tradicional de intimidad o vida privada limitada al derecho de impedir interferencias ajenas, o al derecho a ser dejado solo, hasta el derecho de mantener el control de la propia información y de determinar la forma de construcción de la propia esfera privada, por lo que el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la persona en las sociedades democráticas;

Tomando en cuenta que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es obligatoria únicamente para los poderes públicos del Estado

Federal, y tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de sus titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado;

Reconociendo que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública Federal implica recabar datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de licitud, calidad, de información al titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transmisión; principios que no limitan la utilización de la informática en el ámbito público, sino que se trata de hacerla compatible con los derechos de los ciudadanos;

Distinguiendo la importancia de que las personas tengan conocimiento de la información que de ellos obra en los archivos del Gobierno Federal a efecto de hacer uso del derecho de acceso y corrección de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman, se creará un nueva aplicación informática de acceso al público denominada "Sistema Persona";

Considerando que la Administración Pública Federal debe proteger rigurosamente los datos personales, apegándose en forma escrupulosa a la regulación en la materia, sin que ello se constituya en pretexto u obstáculo que menoscabe el Estado de Derecho o impida el acceso a la información gubernamental y la rendición de cuentas, de manera que los ciudadanos puedan valorar el desempeño de los sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que ante una solicitud de acceso a información gubernamental en la que se requieran datos personales contenidos en un Sistema de datos personales, en cada caso, las dependencias y entidades deberán determinar la procedencia de otorgar acceso a aquellos datos que no se consideran como confidenciales, por ubicarse en los supuestos establecidos por los artículos 7, 12 y 18 último párrafo de dicha Ley, y

Resaltando que en el ámbito del Poder Ejecutivo Federal, el Instituto Federal de Acceso a la Información Pública es el garante de la protección de las personas respecto del tratamiento dado a la información que les concierne, a efecto de evitar injerencias a su vida privada, y que los principios contenidos en el capítulo IV del Título I de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental requieren de un desarrollo para su adecuada observancia, ha tenido a bien expedir los siguientes:

Lineamientos de protección de datos personales

Capítulo I. Disposiciones generales

Objeto y ámbito de aplicación

Primero. Los presentes Lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la Administración Pública Federal en el ejercicio de sus atribuciones.

Elementos de los datos personales

Segundo. A efecto de determinar si la información que posee una dependencia o entidad constituye un dato personal, deberán agotarse las siguientes condiciones:

1) Que la misma sea concerniente a una persona física, identificada o identificable, y

2) Que la información se encuentre contenida en sus archivos.

Definiciones

Tercero. Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en los artículos 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2 de su Reglamento, y las referidas en los Lineamientos expedidos por el Instituto, publicados en el Diario Oficial de la Federación el 25 de agosto de 2003 y 6 de abril de 2004, se entenderá por:

I. Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales.

II. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

III. Sistema "Persona": Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

IV. Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.
V. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.
VI. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.
VII. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión.
VIII. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.
IX. Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

Sistema de datos personales
Cuarto. Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a) Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.
b) Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II. Principios rectores de la Protección de los Datos Personales

Principios de la protección de datos personales
Quinto. En el tratamiento de datos personales, las dependencias y entidades deberán observar los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión.

Licitud
Sexto. La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima.

Calidad de los datos
Séptimo. El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

Acceso y corrección
Octavo. Los sistemas de datos personales deberán almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto.

De Información
Noveno. Se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

Seguridad
Décimo. Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Custodia y cuidado de la información
Undécimo. Los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

Consentimiento para la transmisión
Duodécimo. Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el Lineamiento Vigésimo segundo.

Capítulo III. Del Tratamiento

Del Tratamiento exacto, adecuado, pertinente y no excesivo

Decimotercero. A efecto de cumplir con el principio de calidad a que se refiere el Lineamiento Séptimo, se considera que el tratamiento de datos personales es:

a) Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;

b) Adecuado: Cuando se observan las medidas de seguridad aplicables;

c) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y

d) No excesivo: Cuando la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Corrección de oficio

Decimocuarto. En caso de que los Responsables, Encargados o Usuarios detecten que hay datos personales inexactos, deberán de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Conservación de los datos

Decimoquinto. Los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos o contables, deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los Lineamientos Generales para la organización y conservación de archivos de las Dependencias y Entidades de la Administración Pública Federal, teniendo en cuenta los siguientes plazos:

a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron;

b) El establecido por las disposiciones aplicables;

c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y

d) El señalado en los casos de transmisión.

Condiciones técnicas

Decimosexto. Los datos personales sólo podrán ser tratados en sistemas de datos personales que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Información al Titular de los datos
Decimoséptimo. En el momento en que se recaben datos personales, la dependencia o entidad deberá hacer del conocimiento al Titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente:

a) La mención de que los datos recabados serán protegidos en términos de lo dispuesto por la Ley;
b) El fundamento legal para ello, y
c) La finalidad del Sistema de datos personales.

Modelo de leyenda para informar al Titular de los datos
Decimoctavo. Sin perjuicio de que las dependencias y entidades elaboren sus propios formatos para informar al Titular de los datos lo establecido por el Lineamiento anterior, podrán utilizar el siguiente modelo:

Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de datos personales (indicar nombre)*, con fundamento en* (indicar) *y cuya finalidad es* (describirla)*, el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Federal de Acceso a la Información Pública* (www.ifai.org.mx)*, y podrán ser transmitidos a* (indicar)*, con la finalidad de* (indicar)*, además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es* (indicar)*, y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es* (indicar). *Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación* (incluir fecha).

Otros medios para recabar los datos
Decimonoveno. Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el Decimoséptimo de los presentes Lineamientos.

Disociación de datos Vigésimo. La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse al Titular de éstos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la Ley de Información Estadística y Geográfica, así como las demás disposiciones aplicables.

Tratamiento de datos por terceros
Vigésimo primero. Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

Capítulo IV. De la transmisión

Transmisión sin consentimiento del Titular de los datos
Vigésimo segundo. Las dependencias y entidades podrán transmitir datos personales sin el consentimiento del Titular de los datos, en los casos previstos en el artículo 22 de la Ley. Asimismo, deberán otorgar acceso a aquellos datos que no se consideran como confidenciales por ubicarse en los supuestos establecidos por sus artículos 7, 12 y 18 último párrafo.

Transmisión con el consentimiento del Titular de los datos
Vigésimo tercero. Para los efectos del artículo 21 de la Ley, y en los casos no previstos por el artículo 22 de la Ley, las dependencias y entidades sólo podrán transmitir datos personales cuando:

a) Así lo prevea de manera expresa una disposición legal, y
b) Medie el consentimiento expreso de los titulares.

Consentimiento
Vigésimo cuarto. Para la transmisión de los datos, el consentimiento del Titular de los mismos deberá otorgarse por escrito incluyendo la firma autógrafa y la copia de identificación oficial, o bien a través de un medio de autenticación. En su caso, las dependencias y entidades deberán cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas.

El servidor público encargado de recabar el consentimiento del Titular de los datos para la transmisión de los mismos, deberá entregar a éste, en forma previa a cada transmisión, la información suficiente acerca de las implicaciones de otorgar, de ser el caso, su consentimiento.

Informes sobre la transmisión
Vigésimo quinto. Las transmisiones totales o parciales de sistemas de datos personales que realicen las dependencias y entidades en el ejercicio de sus atribuciones, deberán ser notificadas por el Responsable al Instituto en los términos establecidos por el Cuadragésimo de los presentes Lineamientos.

Requisitos del Informe
Vigésimo sexto. El informe a que hace referencia el Lineamiento anterior deberá contener al menos, lo siguiente:

I. Identificación del Sistema de datos personales, del transmisor y del destinatario de los datos;

II. Finalidad de la transmisión; así como el tipo de datos que son objeto de la transmisión;

III. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transmisor y destinatario;

IV. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al Instituto, y

V. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión.

Capítulo V. De la Seguridad de los Sistemas de Datos Personales

Medidas de seguridad
Vigésimo séptimo. Para proveer seguridad a los sistemas de datos personales, los titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

I. Designar a los Responsables;

II. Proponer al Comité de Información, la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos;

III. Proponer al Comité la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y

IV. Proponer al Comité la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Acciones sobre seguridad
Vigésimo octavo. En cada dependencia o entidad, el Comité coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Reserva de la información
Vigésimo noveno. La documentación generada para la implementación, administración

y seguimiento de las medidas de seguridad administrativa, física y técnica tendrá el carácter de información reservada y será de acceso restringido.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales así como del contenido de éstos.

Resguardo de sistemas de datos personales físicos

Trigésimo. El Responsable deberá:

a) Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados y Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico, y

c) Informar al Comité los nombres de los Encargados y Usuarios.

Sitio seguro para sistemas de datos personales automatizados

Trigésimo primero. Las dependencias y entidades deberán:

I. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;

II. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales debiendo registrarse para ello en una bitácora;

III. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en estos Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

IV. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los Usuarios que utilizan datos personales, considerando al menos las siguientes actividades:

a) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y

b) Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.

V. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;

VI. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia; y

VII. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Seguridad en la red

Trigésimo segundo. En relación con los aspectos de seguridad al utilizar la red de comunicación donde se transmitan datos personales, es necesario establecer:

I. Procedimientos de control de acceso a la red que consideren perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los Sistema de datos personales;

II. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los Sistema de datos personales.

Documento de seguridad

Trigésimo tercero. Las dependencias y entidades, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Requisitos del documento de seguridad

Trigésimo cuarto. El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios;

II. Estructura y descripción de los sistemas de datos personales;

III. Especificación detallada del tipo de datos personales contenidos en el sistema;

IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;

V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, las cuales deberán incluir lo siguien-

te:

a) Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales;

b) Actualización de información contenida en el Sistema de datos personales;

c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;

d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;

e) Procedimiento de notificación, gestión y respuesta ante incidentes; y

f) Procedimiento para la cancelación de un Sistema de datos personales. El contenido del documento deberá actualizarse anualmente.

Registro de incidentes

Trigésimo quinto. El Encargado deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Accesos controlados y bitácoras

Trigésimo sexto. En cada acceso a un Sistema de datos personales deberá guardarse como mínimo:

I. Datos completos del Responsable, Encargado o Usuario;

II. Modo de autenticación del Responsable, Encargado o Usuario;

III. Fecha y hora en que se realizó el acceso, o se intentó el mismo;

IV. Sistema de datos personales accedido;

V. Operaciones o acciones llevadas a cabo dentro del Sistema de datos personales; y

VI. Fecha y hora en que se realizó la salida del Sistema de datos personales.

Operaciones de acceso, actualización, respaldo y recuperación

Trigésimo séptimo. En las actividades relacionadas con la operación de los sistemas de datos personales tales como el acceso, actualización, respaldo y recuperación de información, las dependencias y entidades deberán llevar a cabo en forma adicional, las siguientes medidas:

I. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, Encargados o Usuarios de los sistemas de datos personales;

II. Llevar control y registros del Sistema de datos personales en bitácoras que con-

tengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad;
III. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de datos personales;
IV. Mecanismos de auditoría o rastreabilidad de operaciones; V. Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del Sistema de datos personales según su perfil de usuario;
VI. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;
VII. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;
VIII. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;
IX. Garantizar que durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accesados, reproducidos, alterados o suprimidos sin autorización;
X. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;
XI. En los casos en que la operación sea externa, convenir con el proveedor del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;
XII. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;
XIII. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente respecto de medidas técnicas establecidas en los presentes Lineamientos y en su caso, remitirlos al Organo Interno de Control, y
XIV. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el capítulo II de los presentes Lineamientos.

Estas medidas deberán ser integradas como anexos técnicos al documento de seguridad mencionado en el Lineamiento Trigésimo tercero.
Recomendaciones sobre estándares mínimos de seguridad
Trigésimo octavo. El Instituto emitirá anualmente las recomendaciones sobre los

estándares mínimos de seguridad, aplicables a los sistemas de datos personales que se encuentren en poder de las dependencias y entidades de la Administración Pública Federal y determinará en su caso, el nivel de protección que amerite la naturaleza de los datos personales.

Capítulo VI. Del Sistema "Persona"

Del Sistema "Persona"
Trigésimo noveno. Para dar cumplimiento a lo dispuesto por el artículo 23 de la Ley, el Instituto pondrá a disposición de las dependencias y entidades el Sistema "Persona".

Cuadragésimo. Los Responsables deberán registrar e informar al Instituto, dentro de los primeros diez días hábiles de enero y julio de cada año, lo siguiente:

a) Los sistemas de datos personales;
b) Cualquier modificación sustancial o cancelación de dichos sistemas, y
c) Cualquier transmisión de sistemas de datos personales de conformidad a lo dispuesto por los Lineamientos Vigésimo quinto y Vigésimo sexto de los presentes Lineamientos.

Datos del registro
Cuadragésimo primero. El registro de cada Sistema de datos personales deberá contener, los siguientes datos:

a) Nombre del sistema;
b) Unidad administrativa en la que se encuentra el sistema;
c) Nombre del responsable del sistema;
d) Cargo del Responsable;
e) Teléfono y correo electrónico del Responsable;
f) Finalidad del sistema, y
g) Normatividad aplicable al sistema.

El Instituto otorgará al Responsable un folio de identificación por cada Sistema de datos personales registrado.

Vínculo al Sistema "Persona"
Cuadragésimo segundo. Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema "Persona", a efecto de dar cumplimiento a lo establecido en los artículos 48 y Sexto transitorio del Reglamento de la Ley.

Capítulo VII. Del Instituto

Supervisión de la Protección
Cuadragésimo tercero. Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste, el acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley, su Reglamento y los presentes Lineamientos.

Irregularidades
Cuadragésimo cuarto. En caso de que el Instituto determine que algún servidor público pudo haber incurrido en responsabilidades por el incumplimiento de los presentes Lineamientos, lo hará del conocimiento del Órgano Interno de Control correspondiente, a efecto de que determine lo conducente, con base en el capítulo de Responsabilidades y Sanciones establecido en el Título IV de la Ley, así como en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Transitorios
Primero. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.
Segundo. Los formatos y mecanismos mediante los cuales se recaben datos personales y se informe a los Titulares de los mismos sobre la finalidad del Sistema de datos personales, deberán ser elaborados o modificados en términos del Lineamiento Décimo Séptimo y deberán comenzar a utilizarse, a más tardar el día 31 de marzo de 2006.

En tanto, y a más tardar dentro de los 20 días hábiles siguientes a la entrada en vigor de los presentes Lineamientos las dependencias y entidades que recaben datos personales deberán entregar a los Titulares de los mismos un documento por separado en el que se informen los propósitos para los cuales éstos se recaban.
Tercero. El cumplimiento de las disposiciones contenidas en el capítulo V de los presentes Lineamientos deberá efectuarse a más tardar en diciembre de 2006, incluido el documento de seguridad a que se refiere el Lineamiento Trigésimo tercero.
Cuarto. La primera actualización del Sistema "Persona" por parte de las dependencias y entidades a que se refiere el Lineamiento Cuadragésimo, deberá llevarse a cabo dentro de los primeros diez días hábiles de marzo de 2006.
Quinto. Las primeras recomendaciones sobre las medidas de seguridad que se mencionan en el Lineamiento Trigésimo octavo, serán emitidas por el Instituto a más tardar en el mes de mayo de 2006.
Sexto. Se dejan sin efecto las disposiciones contenidas en los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar

al Instituto el listado de sus sistemas de datos personales, publicados el 20 de agosto de 2003 en el Diario Oficial de la Federación.

Así lo acordó por unanimidad el Pleno del Instituto Federal de Acceso a la Información Pública, en sesión celebrada el día veintisiete de julio de dos mil cinco, ante el Secretario de Acuerdos.

La Comisionada Presidenta, María Marván Laborde.- Rúbrica.- Los Comisionados: Horacio Aguilar Alvarez de Alba, Alonso Gómez-Robledo Verduzco, Juan Pablo Guerrero Amparán, Alonso Lujambio Irazábal.- Rúbricas.- El Secretario de Acuerdos, Francisco Ciscomani Freaner.- Rúbrica.
(R.- 218575)

Guía para la elaboración de un documento de seguridad. Instituto Federal de Acceso a la Información Pública Gubernamental

Introducción

En toda organización, la información es un activo que, al igual que sus instalaciones, capital humano y recursos financieros, debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la propia organización.

De esta manera, la gestión de la seguridad de la información, como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organización afronta.

Para lograr lo anterior, es necesario llevar a cabo una correcta administración de riesgos a fin de que éstos puedan ser asumidos, mitigados, transferidos o evitados de manera eficiente, sistemática y estructurada, que se adapte a los cambios que se produzcan en el entorno y en la información.

Es justamente el avance vertiginoso de las tecnologías de la información el que posibilita la recolección y almacenamiento de grandes volúmenes de información en pequeños dispositivos y facilita su transmisión por medios remotos a grandes distancias en cuestión de segundos. Lo anterior incluye el tratamiento de información relativa o concerniente a personas físicas, cuya protección es una atribución del Instituto Federal de Acceso a la Información Pública, en su calidad de órgano garante de la protección de datos personales en el ámbito del Poder Ejecutivo Federal.

En la Administración Pública Federal el riesgo de sufrir la pérdida de información personal, sea ésta producto de la voluntad de un agente pernicioso o bien resultado del caso fortuito, siempre está presente. Las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas (por ejemplo, el acceso no autorizado a información del estado de salud de un individuo por personas ajenas al tratamiento de dicho paciente).

Es por ello que no resulta conveniente escatimar recursos y esfuerzos en el establecimiento de controles para la protección de la información frente a acciones o situaciones

no deseadas, pues de esa manera, además de garantizar la continuidad de la operación de los sujetos obligados, se protege a los individuos a los que se refiere dicha información.

A efecto de que las dependencias y entidades de la Administración Pública Federal puedan conocer el tipo de controles a que se refiere el párrafo anterior, éstos deben estar documentados y ser difundidos para el conocimiento de todos los involucrados en el tratamiento de la información.

Al respecto, el Trigésimo tercero de los Lineamientos establece la obligación de que las dependencias y entidades expidan un documento de seguridad que contenga las medidas de seguridad administrativa, física y técnica aplicables a la protección de sistemas de datos personales, ya que dejar constancia por escrito de dichas medidas de seguridad permite identificar los roles, actividades y responsabilidades de los servidores públicos o terceros contratados que dan tratamiento a información personal, así como una ágil verificación de los controles implementados para el aseguramiento de ésta.

Por lo anterior, el Instituto Federal de Acceso a la Información Pública, conforme la facultad prevista en el artículo 37, fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, pone a su disposición la presente Guía para la elaboración de un Documento de seguridad que tiene por objeto garantizar en la Administración Pública Federal la correcta documentación de los controles de seguridad mínimos indispensables que deben considerarse según lo previsto en el Trigésimo cuarto de los Lineamientos.

El modelo propuesto en esta Guía no es limitativo. Los sujetos obligados, tomando en cuenta factores como el tamaño y estructura de la organización, objetivos, clasificación de la información, requerimientos de seguridad y procesos, entre otros aspectos relativos a su contexto, pueden prever y aplicar medidas de seguridad adicionales como aquellas que desde 1980 han trascendido para conformar el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2005 (anterior ISO/IEC 17799:2005), lo cual se determina en razón de los activos que poseen los sujetos obligados y los riesgos a los que dichos activos están expuestos.

En ese sentido, el modelo que se presenta pretende brindar a las dependencias y entidades homogeneidad en la redacción, organización y contenido para que los Comités de Información, conjuntamente con el área de tecnologías de la información y los responsables de los sistemas de datos personales, elaboren su propio Documento de seguridad en el que describan las medidas de seguridad administrativa, física y técnica implementadas para la protección de los sistemas de datos personales que custodian.

1. Terminología

1.1 Abreviaturas

APF Administración Pública Federal.
DOF Diario Oficial de la Federación.
IFAI Instituto Federal de Acceso a la Información Pública.
LFTAIPG Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

1.2 Conceptos básicos

Para la aplicación de la Guía para la elaboración de un Documento de seguridad (en adelante Guía), se deberán considerar las definiciones contenidas en los artículos 3 de la LFTAIPG1 y 2 de su Reglamento2; así como lo previsto en el Tercero de los Lineamientos de Protección de Datos Personales3 (en adelante Lineamientos), las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales4 (en adelante Recomendaciones) y los conceptos que se señalan en el presente apartado.

1.2.1 Documento de seguridad
Concepto. Documento elaborado por el sujeto obligado que contiene las medidas de seguridad administrativa, física y técnica aplicables a sus sistemas de datos personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen. El documento tiene como propósito identificar el universo de sistemas de datos personales que posee cada dependencia o entidad, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Dicho documento deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la presentación de un servicio tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

Marco jurídico
El Capítulo V de los Lineamientos establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes (físicos, electrónicos o ambos) en los que residen dichos datos y dependiendo

del nivel de protección que tales datos requieran (bajo, medio o alto) conforme a la naturaleza de los mismos.

En el mismo sentido, el Trigésimo tercero de los Lineamientos establece que las dependencias y entidades deberán expedir un Documento de seguridad que contenga las medidas administrativas, físicas y técnicas aplicables a los sistemas de datos personales y que dicho documento será de observancia obligatoria.

En cuanto al contenido mínimo del Documento de seguridad, el Trigésimo cuarto de los Lineamientos señala lo siguiente:

Requisitos del documento de seguridad

Trigésimo cuarto. El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios;

II. Estructura y descripción de los sistemas de datos personales;

III. Especificación detallada del tipo de datos personales contenidos en el sistema;

IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;

V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, las cuales deberán incluir lo siguiente:

a) Procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales;

b) Actualización de información contenida en el Sistema de datos personales;

c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;

d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;

e) Procedimiento de notificación, gestión y respuesta ante incidentes; y

f) Procedimiento para la cancelación de un Sistema de datos personales.

1.2.2 Tipos de seguridad: administrativa, física y técnica

Es importante aclarar las diferencias que existen entre las medidas de seguridad administrativa, física y técnica para que el sujeto obligado cuente con estos elementos teóricos al momento de elaborar su Documento de seguridad. A continuación se agrupan los temas que corresponden a cada tipo de seguridad tomando como base el estándar internacional ISO/IEC 27002:2005 que se refiere a mejores prácticas sobre seguridad de la información:

a) Las medidas de seguridad administrativa son aquellas que deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

Política de seguridad. Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del sujeto obligado.

Cumplimiento de la normatividad. Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable al sujeto obligado, los derechos de propiedad intelectual, la protección de datos personales y la privacidad de la información personal.

Organización de la seguridad de la información. Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.

Clasificación y control de activos. Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.

Seguridad relacionada a los recursos humanos. Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.

Administración de incidentes. Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

Continuidad de las operaciones. Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

b) Las medidas de seguridad física atañen a las acciones que deben implementarse para contar con:

Seguridad física y ambiental. Establecimiento de controles relacionados con los perímetros de seguridad física y el entorno ambiental de los activos, con el fin de prevenir accesos no autorizados, daños, robo, entre otras amenazas. Se enfoca en aspectos tales como los controles implementados para espacios seguros y seguridad del equipo.

c) Las medidas de seguridad técnica son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

Gestión de comunicaciones y operaciones. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

Control de acceso. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

Adquisición, desarrollo, uso y mantenimiento de sistemas de información. Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

1.2.3 Tipo de soportes: físicos y electrónicos

Es importante explicar la diferencia entre un soporte físico y un soporte electrónico debido a que las medidas de seguridad que el sujeto obligado implemente para cada sistema de datos personales están estrechamente relacionadas con el tipo de soportes utilizados.

Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el Instituto:

Soportes físicos. Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados a mano o a máquina, fotografías, placas radiológicas, carpetas, expedientes, entre otros.

Soportes electrónicos. Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

El Decimoséptimo y el Trigésimo de los Lineamientos hacen mención de los conceptos arriba señalados cuando se alude a los tipos de soportes, medios de almacenamiento o formatos (físicos o electrónicos) en los cuales residen los datos personales del sistema que custodia el sujeto obligado.

Una vez explicado lo anterior, es preciso señalar que el sujeto obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en:

i. Soporte físico;
ii. Soporte electrónico, o
iii. Ambos tipos de soportes.

1.2.4 Nivel de protección que requieren los datos personales

Para que el sujeto obligado pueda identificar las medidas de seguridad que resultan aplicables a cada uno de sus sistemas, debe considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido: básico, medio o alto, como a continuación se señala:5

1. Nivel de protección básico:

a) Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
b) Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

2. Nivel de protección medio:

a)Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
b) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
c) Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

d) Datos de transito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

3. Nivel de protección alto:

a) Datos ideológicos: Creencia religiosa, ideología, afiliación política y sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros.
b) Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros.
c) Características personales: Tipo de sangre, ADN, huella dactilar u otros análogos.
d) Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
e) Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.
f) Origen: Étnico y racial.

Los niveles de protección señalados definen el mayor o menor grado de confidencialidad, disponibilidad e integridad que el sujeto obligado debe asegurar de acuerdo con la naturaleza de los datos contenidos en los sistemas de datos personales que custodia, de conformidad con las siguientes definiciones:

La confidencialidad es asegurar que la información no sea accedida por (o divulgada a) personas o procesos no autorizados.

La integridad es garantizar la exactitud y la confiabilidad de la información y los sistemas de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

La disponibilidad es que las personas o procesos autorizados accedan a los activos de información cuando así lo requieran.

1.2.5 Tipo de transmisiones de datos personales y Modalidades para la transmisión

Una transmisión de datos personales implica la entrega total o parcial de sistemas de datos personales a cualquier persona distinta del titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras o bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.6

En el ámbito de la APF, existen tres tipos de transmisiones que se pueden llevar a cabo dependiendo de quién sea el destinatario:

a) Interinstitucionales: Transmisiones de datos a dependencias y entidades de la APF, entidades federativas y municipios;

b) Internacionales: Transmisiones a gobiernos u organismos internacionales, y
c) Con entes privados u organizaciones civiles públicas o privadas.

Para implementar las medidas de seguridad aplicables a las transmisiones citadas, debe considerarse la modalidad por la cual se envían los datos personales a los destinatarios, pudiendo hacerse mediante el traslado de soportes físicos, mediante el traslado físico de soportes electrónicos o el traslado sobre redes electrónicas. Cada una de estas modalidades se caracteriza por lo siguiente:

a) Traslado de soportes físicos: En esta modalidad los datos personales se trasladan en medios de almacenamiento inteligibles a simple vista que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo del traslado de soportes físicos es cuando una dependencia envía por correspondencia oficios o formularios impresos.

b) Traslado físico de soportes electrónicos: En esta modalidad se trasladan físicamente para entregar al destinatario los datos personales en archivos electrónicos contenidos en medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos. Ejemplo de ello es cuando una dependencia entrega a otra por mensajería oficial un archivo electrónico con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, entre otros.

c) Traslado sobre redes electrónicas: En esta modalidad se transmiten los datos personales en archivos electrónicos mediante una red electrónica. Por ejemplo, cuando un archivo electrónico con un listado de beneficiarios se envía de una dependencia a otra por Internet.

1.2.6 Diferencias entre identificar, autenticar y autorizar en el control de acceso

El control de acceso es una medida de seguridad que permite el acceso únicamente a quien está autorizado para ello y una vez que se ha cumplido con el procedimiento de identificación y autenticación. En ese sentido, cabe precisar el significado de los siguientes conceptos:

Identificar consiste en tomar conocimiento de que una persona es quien dice ser. Lo anterior se logra, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (login).

Autentificar (o autenticar) a una persona se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona,

(ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo).

Autorizar se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos.

Es importante que el sujeto obligado identifique las diferencias entre estos conceptos pues cada uno de ellos implica la implementación de medidas de seguridad distintas pero relacionadas entre sí. Ejemplo de lo anterior es cuando se implementan medidas de seguridad en capas en el control de acceso, como las siguientes:

a) Mostrar una identificación oficial para acceder a las instalaciones del sujeto obligado en un punto de revisión (control de acceso en el perímetro exterior).

b) Una vez adentro de sus instalaciones, una segunda capa de protección se establece cuando el sujeto obligado implementa un control biométrico de huella dactilar para autenticar a la persona que fue identificada en el perímetro exterior y de este modo pueda ingresar al almacén donde se archivan los soportes físicos o el centro de datos donde residen soportes electrónicos (control de acceso en el perímetro interior).

c) Finalmente, la persona previamente identificada y autenticada, ingresa al sistema, a través de un usuario y contraseña, para realizar consultas en el mismo, pues el responsable autorizó el acceso con permiso de (sólo lectura).

Objetivos

Objetivo general

Proporcionar a las dependencias y entidades de la Administración Pública Federal los elementos mínimos con los que debe contar un Documento de seguridad.

Objetivos específicos

Explicar los conceptos que el sujeto obligado debe tomar en cuenta para la elaboración de su Documento de seguridad.

Orientar a los sujetos obligados respecto de las medidas de seguridad administrativa, física y técnica mínimas con las que debe contar un Documento de seguridad, según lo previsto en el Trigésimo cuarto de los Lineamientos.

Ofrecer una guía y un modelo para la creación de dicho documento.

Modelo de Documento de seguridad

Considerando que el Lineamiento Trigésimo Tercero del Capítulo V, "Documento de seguridad", señala que las dependencias y entidades, a través de su Comité de Información, conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales; el IFAI presenta el siguiente modelo tan solo como una referencia para el desarrollo del documento de seguridad que cada sujeto obligado debe realizar, pues deben considerarse para su elaboración las particularidades de cada sistema de datos personales, la estrategia de seguridad establecida y los riesgos que afronta cada dependencia o entidad.

El presente Modelo de Documento de seguridad para los Sistemas de Datos Personales se ha generado a partir de lo dispuesto en los Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidos por el IFAI e indica, conforme dichas disposiciones, las medidas de seguridad mínimas recomendadas para coadyuvar al cumplimiento relacionado con la integridad, confidencialidad y disponibilidad de la información.

Es importante señalar que el formato y la estructura del modelo pueden variar y que no es un modelo limitativo, sino que se pretende presentar únicamente los contenidos mínimos de un Documento de seguridad conforme lo prevé la normatividad y las mejores prácticas internacionales en la materia.

Idealmente, el sujeto obligado debe elaborar un Documento de seguridad en el que incluya todos los sistemas de datos personales bajo su custodia. No obstante, también es posible que elabore un Documento de seguridad por unidad administrativa en el que se incluyan los sistemas que opera y custodia cada una. Finalmente, la tercera opción es elaborar un documento de seguridad para cada sistema que posee el sujeto obligado.

El esquema elegido para el modelo de Documento de seguridad que aquí se presenta es el que contiene todos los sistemas de datos personales que posee y custodia el sujeto obligado, organizados por unidad administrativa.

Es recomendable que el sujeto obligado analice y documente las medidas de seguridad aplicables a cada uno de sus sistemas de datos personales considerando los ejemplos y explicaciones contenidas en las notas al pie del modelo, y sustituya con su información el texto que se encuentra en cursivas o en corchetes.

Finalmente, es importante recordar al sujeto obligado que el Documento de seguridad tiene el carácter de información reservada, de conformidad con el Vigésimo noveno de los Lineamientos de Protección de Datos Personales, por lo que deberá incluir la leyenda de clasificación correspondiente en el mismo.

DOCUMENTO DE SEGURIDAD DE
[DENOMINACIÓN DEL SUJETO OBLIGADO]

Parte 1. Catálogo de Sistemas de datos personales

A. [Denominación de la Unidad administrativa A]

A1. [Nombre del sistema A1]
Responsable:
Nombre:
Cargo:
Funciones: [Descripción de las atribuciones con relación al tratamiento de los datos personales sistema]
Obligaciones: [Descripción de las responsabilidades en cuanto al tratamiento de los datos personales del sistema]

Encargados:7
Nombre: [Nombre del Encargado 1]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Encargado 2]
Cargo:
Funciones:
Obligaciones:

Usuarios:8
Nombre: [Nombre del Usuario 1]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Usuario 2]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Usuario 3]
Cargo:
Funciones:
Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema: [Señalar el tipo de dato personales que contiene el sistema, además de listar cada uno de los datos personales recabados]9

A2. [Nombre del sistema A2]
Responsable:
Nombre:
Cargo:
Funciones:
Obligaciones:

Encargados:
Nombre: [Nombre del Encargado 1]
Cargo
Funciones:
Obligaciones:
Nombre: [Nombre del Encargado 2]
Cargo
Funciones:
Obligaciones:

Usuarios:
Nombre: [Nombre del Usuario 1]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Usuario 2]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Usuario 3]
Cargo:
Funciones:
Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:

B. [Denominación de la unidad administrativa B]

B1. [Nombre del sistema B1]
Responsable:
Nombre:
Cargo:
Funciones:
Obligaciones:

Encargados:
Nombre: [Nombre del Encargado 1]
Cargo
Funciones:
Obligaciones:
Nombre: [Nombre del Encargado 2]
Cargo
Funciones:
Obligaciones:

Usuarios:
Nombre: [Nombre del Usuario 1]
Cargo:
Funciones:
Obligaciones:
Nombre: [Nombre del Usuario 2]
Cargo:
Funciones:
Obligaciones:

Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:

Parte 2. Estructura y descripción de los sistemas de datos personales

A1. [Nombre del sistema A1]

Tipo de soporte: 10
Tipo de soporte:11
Descripción:12

Características del lugar donde se resguardan los soportes: [Describir el lugar en el que físicamente se encuentran los soportes del sistema]13

A2. [Nombre del sistema A2]

Tipo de soporte:
Tipo de soporte
Descripción:
Características del lugar donde se resguardan los soportes:14

B1. [Nombre del sistema B1]

Tipo de soporte:
Tipo de soporte
Descripción:
Características del lugar donde se resguardan los soportes:

Parte 3. Medidas de seguridad implementadas

A1. [Nombre del sistema A1]

I. Transmisiones de datos personales

1. Transmisiones mediante el traslado de soportes físicos:15

a) Deberá señalar si el envío se realiza a través de mensajero oficial, mensajero privado o correspondencia ordinaria;16

b) Deberá precisar si utiliza un sobre o paquete sellado de manera que sea perceptible si fue abierto antes de su entrega;

c) Deberá manifestar si el sobre o paquete enviado es entregado en mano al destinatario, previa acreditación con identificación oficial;

d) Deberá indicar si el remitente pide al destinatario que le informe en caso de que reciba el sobre o paquete con señas de apertura;

e) Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y

f) Deberá señalar si el remitente registra la o las transmisiones en su bitácora así como en el Sistema Persona.

2. Transmisiones mediante el traslado físico de soportes electrónicos:

a) Deberá señalar lo previsto en el numeral 1) anterior, incisos a) al f), y

b) Deberá precisar si los archivos electrónicos que contienen datos personales son cifrados antes de su envío y proporcionar detalles técnicos del cifrado tales como el tipo de algoritmo utilizado y la longitud de la llave (o clave).17

3, Transmisiones mediante el traslado sobre redes electrónicas:
a) Deberá señalar la información prevista en el inciso b) del numeral 2) anterior;
b) Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transmisiones protegidas utilizado;
c) Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones.
d) Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y
Deberá señalar si el remitente registra la o las transmisiones en su bitácora así como en el Sistema Persona.

II. Resguardo de sistemas de datos personales con soportes físicos

1. Señalar las medidas de seguridad que ha implementado el sujeto obligado para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.18
2. Señalar en un listado las personas que tienen acceso a los soportes físicos del sistema.19

III. Bitácoras para accesos y operación cotidiana

1. *Los datos que se registran en las bitácoras:20*
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;21
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:
   a. Quién es el responsable de analizarlas (si es el sujeto obligado o si es un tercero) y cada cuándo las analiza, y
   b. Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. Registro de incidentes22

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;23

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados.

2. Si el registro está en soporte físico o en soporte electrónico;

3. Cómo asegura la integridad de dicho registro, y

4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. Acceso a las instalaciones

1. Seguridad perimetral exterior (las instalaciones del sujeto obligado):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?24

Para las personas que acceden a sus instalaciones:

¿Cómo las identifica?

¿Cómo las autentifica?

¿Cómo les autoriza el acceso?

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema?25

Para las personas que acceden a dichos espacios interiores:

a) ¿Cómo las identifica?

b) ¿Cómo las autentifica?

c) ¿Cómo les autoriza el acceso?

VI. Actualización de la información contenida en el sistema

[Establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos].

Las medidas de seguridad previstas en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. Perfiles de usuario y contraseñas26

1. Modelo de control de acceso [alguno de los siguientes]:

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?

b) ¿Es discrecional (matriz de control de acceso)?

c) ¿Está basado en roles (perfiles) o grupos?

d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de datos personales:
a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:
a) ¿Quién da de alta nuevos perfiles?
b) ¿Quién autoriza la creación de nuevos perfiles?
c) ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de datos personales:
a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
c)¿Cómo se evita el acceso remoto no autorizado?

VIII. Procedimientos de respaldo y recuperación de datos

1. Señalar si realiza respaldos completos, diferenciales o incrementales;
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;27
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el sujeto obligado o un tercero).

IX. Plan de contingencia

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia del mismo.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
a) El tipo de sitio (caliente, tibio o frío);28
b) Si el sitio es propio o sub contratado con un tercero;

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio, y
d)Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

A2. [Nombre del sistema A2]29

I. Transmisiones de datos personales
II. Resguardo de sistemas de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

B1. [Nombre del sistema B1]

I. Transmisiones de datos personales
II. Resguardo de sistemas de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

Parte 4. Procedimiento para la cancelación de un sistema de datos personales
[Informar y describir el procedimiento para la cancelación de un sistema de datos personales.] 30

Datos del sistema que será cancelado:

a) Denominación
b)Folio del Sistema Persona
c) Motivo de la cancelación

Plazos y condiciones para el bloqueo del sistema:31
[Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad específica de cada sujeto obligado. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo]

Medidas de seguridad para el bloqueo y posterior supresión del sistema:
[Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema,

considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema]

Procedimiento para la supresión del sistema

[Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo]

Mecanismos para la supresión del sistema.

[Describir las técnicas para la eliminación física del sistema] 32

Parte 5. Aprobación del documento de seguridad

Responsable del desarrollo:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que elaboró el documento de seguridad]

Revisó:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que revisó el documento de seguridad]

Autorizó:

[Señalar nombre, puesto, teléfono y correo electrónico del servidor público que autorizó el documento de seguridad]

Fecha:

[Incluir la fecha de liberación del documento]

Parte 6. Anexos técnicos

[En este apartado se deberán enumerar los anexos e identificarlos con su denominación. Los anexos deberán adjuntarse en el orden en el que se enlisten en este apartado y en la parte superior de cada uno deberá estar indicado el número que le corresponde y su denominación para facilitar su identificación]

Notas

1 Publicada en el DOF el 11 de junio de 2002, disponible en http://www.ifai.org.mx/descargar.php?r=/pdf/ciudadanos/marco_normativo/leyes/&a=LFTAIPG.pdf.

2 Publicado en el DOF el 11 de junio de 2003 disponible en http://www.ifai.org.mx/descargar.php?r=/pdf/ciudadanos/marco_normativo/reglamentos/&a=reglamentoley.pdf

3 Publicados en el DOF el 30 de septiembre de 2005, disponibles en http://www.ifai.org.mx/pdf/ciudadanos/cumplimiento_normativo/datos_personales/lineamientos_protdaper.pdf

4 Disponibles en http://www.ifai.org.mx/descargar.php?r=/pdf/ciudadanos/cumplimiento_normativo/datos_personales/&a=Recomendaciones_SDP.pdf

5 Ver inciso II de las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales.*

6 Lineamiento Tercero, fracción VI de los Lineamientos de Protección de Datos Personales.

7 Se tienen que poner los datos de todos los Encargados del sistema.

8 En caso de ser muchos usuarios, se recomienda agregar la información como Anexo al Documento de Seguridad.

9 Ejemplo:

Datos de identificación (nombres, apellido paterno, apellido materno, domicilio, estado civil)

Datos laborales (correo electrónico institucional y teléfono institucional)

10 En caso de que el sujeto obligado prevea cambiar el tipo de soporte que utiliza el sistema por ejemplo de físico a electrónico o en el supuesto de que prevea en el futuro utilizar ambos tipos de soportes, deberá indicarse en este rubro.

11 Precisar si el sistema se encuentra en soportes físicos, soportes electrónicos o ambos.

12 Describir el soporte en el que se encuentran los datos por ejemplo para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

13 Para describir las características del lugar donde se resguardan los soportes, se deberá considerar lo siguiente:

a) Para soportes físicos, el sujeto obligado deberá incluir una descripción escrita con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;

b) Para soportes electrónicos, la descripción ofrecida por el sujeto obligado deberá incluir un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema. Además, deberá describir las medidas de seguridad física que ha implementado para la protección del centro de datos donde residen tales soportes, y

c) En caso de que el sistema ocupe ambos tipos de soportes, deberá presentar las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

14 En caso de que dos o más sistemas se encuentren resguardados en el mismo lugar, se puede hacer una sola descripción señalando expresamente los sistemas a los que aplica.

15 **Ejemplo de medidas de seguridad para transmisiones mediante el traslado de soportes físicos:**

1. La transmisión de datos personales mediante el traslado de soportes físicos se lleva a cabo por la vía elegida de común acuerdo entre las partes: mensajero oficial, asistente secretarial, visita personal, servicio de mensajería externo, entre otras posibles. Se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero.

2. El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo.

3. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación, además de la fecha de entrega.

4. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, el mensajero devuelve el paquete al transmisor.

5. El transmisor verifica que el mensajero haya entregado el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente.

6. Se registran estas transmisiones en el Sistema Persona.

[16] El envío por correspondencia ordinaria sólo es aceptable si los datos personales requieren de un nivel de protección básico o si los datos están disociados de sus titulares.

[17] Se recomiendan los siguientes bits de longitud considerando el nivel de protección que requieren los datos personales: nivel de protección bajo, 128 bits de longitud; nivel de protección medio, 512 bits de longitud; y nivel de protección alto, 1024 bits. Estos parámetros pueden variar de acuerdo al avance o desarrollo en tecnologías de cifrado.

[18] Por ejemplo, se espera que precise si los formatos impresos, documentos, listados o expedientes están foliados, cosidos o engargolados, si los muebles o la estantería donde residen cuentan con cerradura, si existen mecanismos para regular la temperatura y la humedad, si existen sistemas de detección y/o supresión de incendios, si cuenta con mecanismos para regular y mantener el suministro continuo de energía eléctrica, entre otras posibles medidas.

[19] En caso de ser muchas personas, se sugiere agregar el listado como Anexo al Documento de seguridad.

[20] **Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes físicos:**

El Responsable del sistema procura un estricto control y registro de:

1. Las autorizaciones emitidas para facultar el acceso a un servidor público a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas a su cargo.

2. La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido.

3. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.

4. El préstamo de expedientes es asistido por un sistema de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.

5. El sistema de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.

6. El Encargado del sistema es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes electrónicos:

1. El Responsable del sistema -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:

a) Las bitácoras de eventos ocurridos a nivel *sistema operativo* en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.

b) Las bitácoras de eventos generados a nivel *software aplicativo* del sistema de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.

c) Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio Responsable y el administrador del servidor) en su interacción con el sistema de datos personales. Entre otras, se generan bitácoras para: Archivos, servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.

d) El conjunto de bitácoras permiten registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.

e) Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

2. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con "resúmenes" creados por un algoritmo "digestor". Se cuenta con una herramienta de software que automatiza estas operaciones.

3. Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:

a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.

b) Cada semana se llevan a cabo análisis de bitácoras pero no de todas ellas. Depende de la bitácora y de las amenazas detectadas en el entorno.

4. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

[21] En caso de tener las bitácoras en soportes físicos, debe señalar si en el futuro planea incorporarlas a soportes electrónicos.

[22] En este rubro el sujeto obligado debe describir el procedimiento de atención de incidentes que tiene implementado y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

[23] **Ejemplo de procedimiento en caso de presentarse un incidente:**

a) El Encargado elabora y entrega un informe al Responsable a más tardar al día siguiente de haber ocurrido el incidente. Dicho informe precisa los soportes físicos o electrónicos afectados y, en su caso, los recuperados.

b) El incidente se registra en una hoja de cálculo anotando quién resolvió el incidente y los soportes dañados y recuperados. Dicha hoja está protegida con una contraseña de acceso. Su integridad se garantiza generando y almacenando un resumen creado por un algoritmo digestor en un servidor del centro de datos y respaldándola en un CD-R después de registrar un incidente.

c) En caso de robo o extravío de datos personales, el Responsable del sistema, al tener conocimiento del incidente, da vista al titular de la dependencia o entidad para su conocimiento y al titular del área jurídica

o aquél que tenga facultades para presentar denuncias o querellas ante el Ministerio Público para que en el ámbito de sus atribuciones, determine lo conducente.

d) A no más de 3 días naturales de haber ocurrido el incidente, el Responsable del sistema da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional.

e) En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable del sistema da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Adicionalmente, se da aviso por correo electrónico o por teléfono.

24 Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de vídeo-vigilancia, entre otras posibles medidas.

25 Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de vídeo-vigilancia, entre otras medidas.

26 En este rubro el sujeto obligado deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

27 Es deseable que precise si para almacenar dichos medios cuenta con al menos dos lugares distintos que cumplan con las condiciones de seguridad especificadas en el articulado del Capítulo V de los Lineamientos, conforme a la fracción III del Trigésimo primero de los Lineamientos; o bien, si utiliza un espacio externo seguro para guardar de manera sistemática dichos respaldos, según la fracción VIII del Trigésimo séptimo de tales Lineamientos.

28 El tipo de sitio caliente, tibio o frío se refiere a la infraestructura, el equipo y el software disponibles en el sitio alterno; por lo que a mayor disponibilidad de dichos elementos resulta una menor demora para restablecer las operaciones de uno o más sistemas. Ejemplos de lo anterior son, en cuanto a infraestructura: aire acondicionado, cableado, suministro de energía eléctrica y enlaces de comunicaciones; en cuanto al equipo: servidores, almacenamiento y periféricos, y por lo que se refiere al software: sistemas operativos, manejadores de bases de datos y aplicaciones. Por lo tanto:

i) En un sitio alterno caliente se mantienen disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal. Este tipo de sitios alternos es el más costoso pero supone tan solo unas cuantas horas para restaurar operaciones.

ii) El sitio alterno tibio cuenta con infraestructura no configurada y equipos equivalentes que pueden estar disponibles en pocas horas pero no contienen software ni datos. Este tipo de sitios alternos es el punto medio en costo y tiempo para restaurar operaciones.

iii) El sitio alterno frío cuenta con un ambiente mínimo de infraestructura y no cuenta con el equipo. Este tipo de sitios alternos es el menos costoso pero supone demora de algunos días para restablecer operaciones.

29 Se debe seguir el modelo del sistema A1 –incisos I al IX- para señalar las medidas de seguridad aplicables a cada uno de los sistemas que posea el sujeto obligado.

30 La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que la autoridad conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable

y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.

Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el sujeto obligado de estar en operación el Sistema.

La cancelación de sistemas de datos personales debe considerar lo establecido en los Lineamientos de archivos y en concordancia con ello, el sujeto obligado debe establecer un procedimiento de cancelación en su Documento de seguridad, en términos de lo que establecen el Trigésimo tercero y el Trigésimo cuarto de los Lineamientos de protección de datos, el cual deberá hacerse del conocimiento del titular de los datos.

En el Primero de los Lineamientos de archivos se establecen criterios de organización y conservación de la documentación de las dependencias y entidades de la APF con el objeto de conservar íntegros y disponibles los documentos para permitir y facilitar el acceso a la información que contengan. Dichos Lineamientos de archivo establecen además que se debe incluir la siguiente información en el Catálogo de disposición documental -un registro general y sistemático que establece los siguientes valores documentales-: (i) los plazos de conservación; (ii) la vigencia documental; (iii) la clasificación de reserva o confidencialidad, y (iv) el destino final de los documentos.

El Decimoquinto de los Lineamientos dispone que cuando se pretende dar de baja un sistema de datos personales se debe verificar en primer lugar, si el mismo tiene valores históricos, científicos, estadísticos o contables. En caso de que contenga dichos valores, los datos personales serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los "Lineamientos Generales para la organización y conservación de archivos de las dependencias y entidades de la Administración Pública Federal" -Lineamientos de Archivos-.

Dado lo anterior, dicho Catálogo de disposición documental y el procedimiento de cancelación de un sistema deben atender al valor documental de la información contenida en el mismo, de conformidad con los criterios establecidos por el sujeto obligado en consideración a la posible consulta que de los mismos se requiriera o a cualquier otra implicación jurídica que pudiera existir en razón de la normatividad aplicable. Lo anterior es así, en virtud de que la organización de los archivos de las dependencias y entidades en los que se incluyen los sistemas de datos personales debe asegurar la disponibilidad, localización y conservación de los documentos de archivo que se posean.

31 Es el periodo por el que se conservará para efectos de responsabilidades, tomando en cuenta el plazo de su prescripción conforme la normatividad aplicable.

32 Cuando el sistema almacene datos personales en soportes físicos, se recomienda incluir en el procedimiento de cancelación alguna de las técnicas conocidas para la destrucción de este tipo de soportes, como es la trituración o la incineración de documentos. Ahora bien, en caso de que almacene datos personales en soportes electrónicos, las características de la información requieren que el sujeto obligado "purgue" los archivos contenidos en los medios de almacenamiento -o bien, que destruya tales medios- toda vez que es insuficiente borrar los archivos o "darle formato" al medio de almacenamiento.

Con el fin de garantizar la efectiva destrucción de los datos contenidos en soportes electrónicos, se recomienda que el procedimiento de cancelación incluya al menos una de las siguientes técnicas:

a) Sobrescribir con un solo valor (unos o ceros) el 100% de la superficie de los medios de almacenamiento no volátil en los que residen los datos del sistema cancelado. Esta técnica es efectiva para discos duros.

b) Desmagnetización de medios magnéticos mediante una herramienta especializada conocida como desmagnetizador o "degausser". Esta técnica es efectiva para discos duros y cintas magnéticas.

c) Destrucción física de los medios de almacenamiento. La Guía para la Sanitización de Medios ("Guidelines for Media Sanitization") que fue publicada por el Instituto Nacional de Estándares y Tec-

nología (National Institute of Standards and Technology) de los Estados Unidos de América, recomienda fundir, desintegrar, desmoronar, pulverizar o incinerar los soportes electrónicos.

d) Cualquier otra técnica utilizada por el sujeto obligado que tenga por objeto la destrucción de soportes electrónicos.

Sumario sobre legislación federal y estatal en materia de protección de datos personales

A nivel federal

Sector Público	Sector Privado
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	La iniciativa de la Ley Federal de Protección de Datos de Particulares se encuentra pendiente de discusión ante el pleno de la Cámara de Diputados del Congreso de la Unión.

A nivel estatal

	Sector público	Sector Privado
Colima	Ley de Protección de Datos Personales del Estado de Colima	
Jalisco	Ley de Transparencia e Información Pública del Estado de Jalisco	Sin ley
Guanajuato	Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato	
Tlaxcala	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala	
Oaxaca	Ley de Protección de Datos Personales del Estado de Oaxaca	Sin ley
Coahuila	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila	Sin ley
Distrito Federal	Ley de Protección de Datos Personales para el Distrito Federal	Sin ley

Indice

Primera Parte
Lecturas

Segunda Parte
Legislación

Internacional

Nacional


LXI LEGISLATURA


ifai


ITAM


sdc
seminario de
derecho y
ciencia