Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

PRINCIPIOS GENERALES A CONSIDERAR EN LA ELABORACIÓN DE UNA LEY DE PROTECCIÓN DE DATOS PERSONALES

Gustavo Adolfo BELLO MARTÍNEZ

SUMARIO: I. *Antecedentes*. II. *Características particulares de los datos personales*. III. *Origen de los principios*. IV. *Primer principio: las bases de datos personales deben ser procesadas justa y legalmente; y su procesamiento debe cumplir con ciertas condiciones mínimas*. V. *Segundo principio: los datos personales deben ser obtenidos para uno o varios propósitos definidos y legales, y no pueden ser procesados de una forma incompatible con estos propósitos originales*. VI. *Tercer principio: los datos personales deben ser adecuados y no excesivos con relación a los propósitos definidos por los cuales son procesados*. VII. *Cuarto principio: los datos personales deben ser correctos y, cuando sea necesario, actualizados*. VIII. *Quinto principio: los datos personales no deben mantenerse más allá de lo necesario para cumplir con los propósitos para los cuales fueron procesados*. IX. *Sexto principio: el controlador de los datos personales debe establecer y mantener las medidas técnicas y organizacionales adecuadas para evitar el procesamiento ilegal o no autorizado de los datos personales, así como para evitar la pérdida, destrucción o daño accidental a los mismos.* X. *Séptimo principio: los datos personales no se deben transferir a países que no protejan, al menos con la misma seguridad, los datos personales.* XI. *Recomendaciones específicas para México*. XII. *Glosario.* XIII. *Referencias*.

Como se ha señalado anteriormente, es necesario complementar la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) con regulación específica de protección de datos per-

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

sonales. Este capítulo tiene por objeto presentar una serie de principios a considerar en un proyecto de Ley de Protección de Datos Personales. Al final, se presenta una serie de recomendaciones específicas para México respecto al tema.

La regulación de los datos personales ha creado sus propios tecnicismos. Por ello, al final se incluye un pequeño glosario con los principales conceptos utilizados en este documento (en cursivas).

I. Antecedentes

Desde hace varias décadas los países económicamente más desarrollados (los países de la Unión Europea y los de la Organización para la Cooperación y el Desarrollo Económicos-OCDE) han promulgado leyes para proteger la privacidad en relación a los datos personales. Estas leyes tienen los siguientes objetivos:

1. Prevenir y eliminar violaciones a las garantías individuales con respecto a la privacidad, tales como el almacenamiento y tratamiento ilegal o incorrecto de los datos personales o la transmisión no autorizada de dichos datos; y
2. Evitar que estas regulaciones dificulten el flujo de la información, necesaria para el eficiente funcionamiento de los mercados y para el adecuado desarrollo de la economía.

La legislación de estos países ha conciliado dos objetivos que en apariencia son contradictorios, pero que la evidencia internacional demuestra que son complementarios. Así, permitir que los datos personales, relevantes para las actividades económicas, tengan un valor en el mercado, fomenta su protección por parte de los tenedores de los mismos. Asimismo, incrementa la confianza de los particulares en el buen uso de los datos, lo que permitirá la conformación de mejores bases de datos.

En México existe un vacío regulatorio respecto a la protección de los datos personales, lo que ha generado:

a) Un abuso en el *procesamiento de la información y los datos personales* por parte de los *controladores de los datos*;
b) Indefensión por parte de los *sujetos de los datos*;
c) Incapacidad del Estado mexicano para remediar esta situación.

Lo anterior genera condiciones que propician un círculo vicioso.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

1. Los datos personales en México son considerados como un bien público.
2. Esto hace que, ante la falta de regulación, casi ningún controlador de datos esté dispuesto a invertir en la protección/calidad de los datos personales.
3. Como resultado de ello, los sujetos de los datos no tienen suficiente incentivos[1] para mantener cierta veracidad en su información personal.
4. Debido a ello, algunos controladores de datos personales abusan de los sujetos de los datos para mantener sus bases de datos.
5. Los sujetos de los datos responden, en la medida posible, con datos personales de dudosa veracidad (falsa o de rápida obsolescencia).

Naturalmente, una de las soluciones directas para resolver este círculo vicioso es la regulación de los datos personales. Lo importante es elegir la alternativa regulatoria que —considerando su impacto— permita resolver la problemática de la manera más eficiente. En este sentido, quien proponga la regulación deben considerar:

a) La problemática, de forma integral;
b) Los objetivos a alcanzar, mediante la expedición de la regulación;
c) Las facultades/restricciones jurídicas del Estado para regular en esta materia;
d) Las alternativas regulatorias, que son los diferentes enfoques mediante los cuales se pueden lograr los objetivos determinados;
e) La implementación, y así verificar si el Estado prevé las instituciones, recursos y procedimientos necesarios para ejecutar la regulación;
f) El impacto esperado, mediante la definición y descripción de los costos y beneficios derivados de la regulación. Esto incluye la identificación de los agentes involucrados en la regulación, así como la forma en que los costos y beneficios serán distribuidos entre ellos; y,
g) Las acciones regulatorias, que son el conjunto de derechos y obligaciones definidos en la regulación y que servirán de instrumentos para lograr los objetivos establecidos por los reguladores.

1 Excepto en el caso de la información cubierta por el *Buró de Crédito*, la cual se encuentra regulada por la Ley para Regular las Sociedades de Información Crediticia, publicada en el *Diario Oficial de la Federación*, el 15 de enero de 2002.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

II. Características particulares de los datos personales

Es necesario señalar algunas características particulares de los datos personales:

— Los datos personales son información;
— La información pierde su valor si ésta no es veraz (falsa u obsoleta);
— La falta de información veraz incrementa los costos de transacción en la economía (de los agentes económicos).
— Teniendo esto en cuenta, se infiere que:
— Los datos personales, por sí mismos o cruzando algunos de ellos, generan información;
— La información tiene un valor;
— Ese valor está relacionado con la veracidad de la información; y,
— La economía, en su conjunto, requiere de información veraz.

Los países con regulación específica respecto de la protección de los datos personales han tenido que tomar una de las siguientes posturas.

1. La autoridad decide restringir (y hasta prohibir), bajo directivas y códigos estrictos, la recolección, el almacenamiento, el manejo, la transmisión y la publicación de datos personales.
2. La autoridad establece reglas que protegen los datos (prohíben el procesamiento de datos sensibles) pero que al mismo tiempo permiten el flujo de información. Detrás de esta lógica hay dos preceptos:
   a) Al permitir el flujo regulado de la información entre diferentes agentes económicos autorizados, los datos personales adquieren un valor.
   b) Dado que adquieren un valor, los datos dejan de considerarse como un bien público. Con ello, la gente cuida aquello que tiene un valor en el mercado y busca mantenerlos correctos y actualizados (eso determina el valor del dato en el mercado).

Las dos posturas tienen sus seguidores (Alemania tiene reglas restrictivas *vs*. Estados Unidos que cuenta con reglas que facilitan el flujo). Es importante que los reguladores definan qué postura es la que más conviene a México y la determinación de las condiciones para lograr ese objetivo.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

III. ORIGEN DE LOS PRINCIPIOS

Estos principios son resultado de una vasta experiencia internacional.[2] Diferentes países, con diferentes tradiciones jurídicas y grados de desarrollo heterogéneos, han experimentado, en algunos casos por varios siglos, en el tratamiento que se le debe dar a los datos personales.[3] Sería ineficiente (y arrogante) pretender una elaboración, desde cero, de estos principios. Dada la poca experiencia mexicana en el tema y la premura para regular este tema, se propone analizar los principios para que los reguladores definan la manera en que la regulación propuesta se apegará (o no) a ellos.

En éste y en todos los principios, es pertinente recordar que el Estado puede ser un controlador de datos, y que debe sujetarse a los mismos principios que cualquier otro controlador de datos,[4] bajo la supervisión de una institución con suficiente independencia para poder tomar sus decisiones de forma adecuada.

IV. PRIMER PRINCIPIO: LAS BASES DE DATOS PERSONALES DEBEN SER PROCESADAS JUSTA Y LEGALMENTE; Y SU PROCESAMIENTO DEBE CUMPLIR CON CIERTAS CONDICIONES MÍNIMAS

En este principio se establecen tres requisitos:

1. Cumplir con las condiciones mínimas de procesamiento;
2. Que el procesamiento sea legal; y,
3. Que el procesamiento sea apropiado.

1. *Condiciones mínimas de procesamiento*

Para el procesamiento de cualquier dato personal debe cumplirse alguna de las siguientes condiciones:

2 Al final se enuncian los documentos que han servido de referencia para identificar estos principios.

3 Villar del (2001) es una sobresaliente investigación sobre la protección de datos en América y la Unión Europea.

4 Ninguno de los países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) establece un régimen más laxo para los controladores públicos de datos personales. De hecho, la mayoría de ellos establece disciplinas más estrictas para los mismos.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

A. El sujeto de los datos ha dado su consentimiento[5] para el procesamiento; o,
B. El procesamiento es necesario[6] para:
   a) La ejecución de un contrato en el que el sujeto de los datos es parte;
   b) Que, a solicitud del sujeto de los datos, se tomen los pasos requeridos para establecer una relación contractual;
   c) Cumplir con cualquier obligación legal a que es sujeto el controlador de los datos, además de las establecidas en relaciones contractuales;
   d) Proteger los intereses vitales del sujeto de los datos. En este caso específico, se debe considerar si la (calidad de) vida del sujeto de los datos está en serio riesgo o sujeta a un grave daño irreversible;
   e) La administración de justicia;
   f) El ejercicio de cualquier función conferida por o bajo cualquier disposición jurídica de carácter general; o,
   g) El ejercicio de cualquier función de naturaleza pública desarrollada en el interés público;[7]

Por la naturaleza de los *datos personales sensibles*, el procesamiento específico de estos datos debe cumplir con, al menos, una de las siguientes condiciones:

A. El sujeto de los datos ha dado su consentimiento explícito[8] para el procesamiento de dichos datos;
B. El procesamiento es necesario para:
   a) Proteger los intereses vitales del sujeto de los datos o de cualquier otra persona, en caso de que no se pueda obtener el consentimiento del sujeto de los datos;

5 El consentimiento debe ser obtenido libre de coacción y basado en información veraz y clara. El consentimiento debe ser comprobable.

6 ¿En quién radica la facultad de definir si es necesario? Hay diferentes enfoques, algunos países lo acotan a una supervisión *ex ante* de los controladores; eso implica una enorme carga de trabajo para la institución responsable de la protección de los datos personales. Otros países prefieren una supervisión *ex post*, lo que se complementa con fuertes sanciones (y compensaciones para el sujeto) en caso de un error por parte de los controladores.

7 Por ejemplo, la prevención de un crimen.

8 El consentimiento explícito debe ser claro y acotado. Debe cubrir detalles específicos del procesamiento, sobre los datos a ser procesados, el propósito del procesamiento y sobre los resultados a ser revelados. Numerosos países han establecido estándares técnicos obligatorios para regular la obtención de consentimientos (tanto regulares como explícitos).

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

b) Proteger los intereses vitales de una persona diferente al sujeto de los datos e irrazonablemente se ha retenido dicho consentimiento;
c) Funciones relevantes de administración de justicia; o
d) Ejecutar funciones establecidas por o bajo otras leyes;[9] o

C. La información personal sensible ha sido hecha pública deliberadamente por el sujeto de los datos.

2. *Procesamiento legal*

No todos los marcos regulatorios establecen explícitamente que es un procesamiento legal.[10] El procesamiento legal se refiere a que sus propósitos y métodos se apegan a las siguientes características:

a) No son contradictorios ni opuestos a ninguna ley aplicable; y,
b) Existe justificación legal que permita realizar este procesamiento.

Se presentan dos casos donde estas características son evidentes. El primero se refiere a obligaciones de confidencialidad entre controlador y sujeto de los datos personales. En el caso de información médica o bancaria hay obligaciones legales y explícitas de confidencialidad. La regulación relevante establece restricciones explícitas para que dicha información pueda ser utilizada con un propósito diferente para el cual se autorizó el procesamiento de la misma, sin el consentimiento manifiesto del sujeto de los datos. Obviamente, un procesamiento ilegal será aquel que no observe estas restricciones legales.

El segundo caso se refiere a las facultades legales de la autoridad para solicitar información. Dependencias y entidades públicas cuentan con facultades explícitas para procesar datos personales, pero esa misma facultad las limita a procesarlos de la forma establecida en la regulación correspondiente.

3. *Procesamiento apropiado*

Este requerimiento se refiere a que todas y cada una de las etapas del procesamiento deben ser apropiadas y que además sean apropiadas las consecuencias del procesamiento para el sujeto de los datos.

9 Un ejemplo sería el procesamiento de datos para verificar la existencia o ausencia de un trato discriminatorio.

10 Algunos países prefieren definir procesos ilegales. Lo importante es que la restricción sea a favor de los sujetos de los datos.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

El procesamiento adecuado debe considerar lo siguiente:

A. La forma en que se obtuvieron/recolectaron los datos debe ser apropiada. Se debe evitar que el sujeto de los datos sea engañado o confundido respecto a los objetivos del procesamiento de sus datos personales. De igual forma, el consentimiento debe ser apropiado (comprobable, claro y certero).
B. La información entregada a los sujetos de los datos debe ser apropiada. Alguna de la información a incluir es:
   a. La identidad del controlador de los datos y la de su representante ante la entidad responsable de la protección de los datos personales;
   b. El propósito o propósitos para los cuales se recolecta la información;
   c. Las consecuencias del procesamiento de la información para el sujeto de los datos (obvias y no obvias);
   d. Potenciales revelaciones de información; y,
   f. En caso de que la información haya sido proporcionada por otro diferente al sujeto de los datos, se debe informar tanto al sujeto de los datos personales así como al que transfirió la información.

Esta información debe ser entregada dentro de un plazo razonable.[11]

V. Segundo principio: los datos personales deben ser obtenidos para uno o varios propósitos definidos y legales, y no pueden ser procesados de una forma incompatible con estos propósitos originales

En este principio se deben considerar los siguientes aspectos:

1. El controlador de los datos debe hacer explícitos al sujeto de los datos los propósitos del procesamiento de los datos personales.
   A. En el caso de autoridades, también deben hacer explícitas sus facultades para recabar dicha información.
   B. Los propósitos (y las facultades, en caso de autoridades públicas) deben hacerse explícitos antes que inicie el procesamiento de los datos.
   C. Si se modifican los propósitos del procesamiento de los datos, se debe recabar el consentimiento del sujeto.

11 Algunos países establecen un plazo definido que corre desde la recolección, transferencia de los datos personales e información. Otros, lo dejan más abierto.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

a) No es válida una notificación simple al sujeto; es necesario su consentimiento.
b) Le debe quedar claro al sujeto de los datos las implicaciones de los nuevos propósitos de procesamiento de los datos.
c) No puede proceder si no se tiene este consentimiento.

2. Los propósitos deben ser legales y claros para el sujeto de los datos.
3. El procesamiento siempre debe ser acorde a los propósitos.
4. Los propósitos puedes ser generales, y los usos más específicos pero siempre en la misma línea.[12]

VI. Tercer principio: los datos personales deben ser adecuados y no excesivos con relación a los propósitos definidos por los cuales son procesados

Este principio busca que los controladores sean proporcionales y equitativos al recabar los datos personales. Para cumplir con este principio se requiere que los controladores de datos sólo requieran la cantidad mínima de información necesaria para cumplir con los objetivos originales del procesamiento de datos. Si los controladores requieren información adicional para un subconjunto de sus sujetos (esto es, no para todos), el controlador podría requerirla para este grupo es específico, pero sería incorrecto recabar un dato que sólo sería ocupado para un grupo.

Tampoco sería aceptable que los controladores recabarán información que consideraran que en futuro podría, de alguna forma aún indeterminada, serles útil. Esto es diferente a recabar información que tendría un propósito determinado pero que no tiene certeza sobre la ocurrencia de dicho evento.[13]

VII. Cuarto principio: los datos personales deben ser correctos y, cuando sea necesario, actualizados

Sin embargo, los controladores no serán responsables por los datos personales incorrectos y entregados de esa forma por los sujetos de los

12 Por ejemplo, un particular puede autorizar a un tenedor de datos la inclusión de sus datos personales con fines de mercadotecnia. Así no tendrá que solicitar autorización cada vez que intente incluir al particular en una lista de clientes potenciales.

13 Por ejemplo, un registro de información médica que los empleadores conservarían para el tratamiento de potenciales accidentes laborales.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

datos, a menos que exista una obligación jurídica del controlador de los datos de verificar la información entregada por el sujeto. Sin embargo, si el controlador tiene una duda razonable sobre la exactitud de los datos, debe establecer un procedimiento de alerta en su propia base de datos. De la misma forma, si un sujeto detecta una información que a su parecer sea incorrecta, y mientras se define la veracidad o no de la información, el controlador estará obligado a anexar al dato en discusión los puntos de vista del sujeto del dato.

Para calificar sobre la necesidad de mantenerlos actualizados, los controladores deben verificar:

Si la obsolescencia del dato registrado causa algún daño al sujeto de los datos;

— Si causa algún daño al controlador de los datos;
— Si causa algún daño a un tercero relacionado con el dato; y
— Si la información obsoleta podría impactar, en alguna forma, la obtención de un beneficio o de una responsabilidad por cualquiera de los involucrados.

En caso de que alguna respuesta sea positiva, es evidente que será necesario actualizar los datos.

VIII. Quinto principio: los datos personales no deben mantenerse más allá de lo necesario para cumplir con los propósitos para los cuales fueron procesados

Los controladores serán responsables de depurar los datos personales en su responsabilidad y destruir los datos que ya no utilicen. En este sentido, se puede establecer una caducidad determinada de los datos personales, y si después de "n" años, no ha habido un nuevo registro, el dato se pueda eliminar de la base activa de datos.

De la misma forma, se debe establecer que aquellos controladores que dejen de operar puedan deshacerse de sus bases de datos de una forma adecuada (si es destrucción, que esta sea total; si es transferencia, que esta sea bajo principios claros y ciertos, que no vulneren los derechos de los sujetos ni la seguridad de las bases de datos).

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

IX. Sexto principio: el controlador de los datos personales debe establecer y mantener las medidas técnicas y organizacionales adecuadas para evitar el procesamiento ilegal o no autorizado de los datos personales, así como para evitar la pérdida, destrucción o daño accidental a los mismos

El primer concepto a definir de este principio es que se entiende por "adecuadas". Para auxiliar en este punto las autoridades regulatorias presentan algunas sugerencias:

A. Se debe considerar el estado de la tecnología y el costo de implementar dicha tecnología. En todo momento se debe asegurar que el nivel de seguridad es apropiado para:

   a) El daño que podría surgir de una violación a la seguridad; y,
   b) La naturaleza de los datos a proteger.

B. El controlador de los datos debe asegurarse (y será responsable) de la confiabilidad de su personal que tendrá acceso a los datos bajo su resguardo.

Además, se debe buscar que los sistemas sean adecuados tanto en el diseño, su infraestructura y en su operación.

Es relevante que la Ley contemple la posibilidad de establecer regulación secundaria que permita determinar si el grado de seguridad es el adecuado. Algunas naciones han establecido estándares técnicos para medir la confiabilidad y seguridad del sistema.[14]

X. Séptimo principio: los datos personales no se deben transferir a países que no protejan, al menos con la misma seguridad, los datos personales

La OCDE ha establecido las *Directrices de la OCDE para la Protección de la Privacidad de los Datos Personales y sus Flujos Transfronterizos*. Las directrices de la OECD constituyen estándares mínimos para los países miembros los cuáles se pueden complementar con medidas adicionales para la protección de la privacidad y las libertades individuales. Los

14 En México debería contemplarse en el reglamento respectivo la posibilidad de establecer normas oficiales mexicanas al respecto.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

objetivos que se establecen en las directrices se pueden perseguir de diferentes maneras dependiendo de los instrumentos legales y las estrategias con los que cuenten los países para su implementación. Por su importancia, se transcriben las directrices relacionados al flujo transfronterizo de los datos personales.

Principios básicos de aplicación internacional

1. Los países miembros deben tomar en consideración las implicaciones que tienen el procesamiento interno y la re-exportación de datos personales sobre otros países miembros.
2. Los países miembros deben tomar las medidas razonables y adecuadas para asegurar que el flujo transfronterizo de datos personales, incluyendo el tránsito a través de un país miembro, sea ininterrumpido y seguro.
3. Un país miembro debe evitar restringir los flujos transfronterizos de datos personales entre sí mismo y otros países miembros, excepto cuando estos últimos no han observado adecuadamente las directrices o cuando la re-exportación de los datos puede infringir su legislación doméstica sobre privacidad. Asimismo, puede imponer restricciones sobre categorías de datos personales que debido a su naturaleza están reguladas específicamente en su legislación doméstica sobre privacidad y para las cuáles los otros países miembros no tienen protección equivalente.
4. Los países miembros deben evitar desarrollar leyes, políticas o prácticas bajo el nombre de protección de privacidad y libertades individuales que puedan crear obstáculos al flujo transfronterizo de datos personales que excedan los requerimientos de protección. Este principio intenta balancear los intereses de protección de privacidad contra los de flujos libres transfronterizos de datos personales. Se deben eliminar las barreras artificiales al flujo de los datos desde el punto de vista de protección de privacidad y libertades individuales.

XI. Recomendaciones específicas para México

1. La Ley de Transparencia y una Ley de Protección de los Datos Personales deben ser instrumentos complementarios. Por esta razón

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

debe cuidarse que no existan contradicciones o traslape entre ambos ordenamientos.

2. El ámbito de la Ley de Protección de los Datos Personales no debe acotarse por el controlador de los datos (público o privado) o por la naturaleza de los datos (regulares, financieros, gubernamentales). Ese tipo de lagunas generan incongruencias y vulnerabilidad del sistema de protección de datos (las áreas grises o casos especiales socavan la protección general). En este sentido se recomienda que los principios (líneas generales) de la protección de datos se establezca en la Ley y abarquen todas las materias.
3. El punto anterior se refleja y determina el diseño institucional que deberá adoptarse para la protección de los datos personales. En este sentido, deben mantenerse una congruencia entre la salida de los datos (Ley de Acceso) y la entrada de algunos de estos datos (Ley de Protección de los Datos Personales) por ello, debe buscarse que el Instituto Federal de Acceso a la Información Pública (IFAI) sea el que opere como autoridad responsable de la protección de los datos personales. Cuando se pensó en el diseño, facultades y presupuesto del IFAI se tomaron en cuenta esas tareas. Por ello, sería un error de operación y un malgasto crear una nueva institución.
4. Se debe establecer un derecho a la indemnización por el inadecuado tratamiento de los datos personales. Esto permitiría alinear la necesidad de la sociedad de contar con una protección efectiva con los incentivos de los controladores de evitar pagar indemnizaciones. Los controladores harían lo posible por mantener sus sistemas trabajando adecuadamente y le permitirán a la autoridad poder establecer un enfoque de vigilancia *ex post* con fuertes sanciones en caso de incumplimiento, lo cual hará más efectiva y menos costosa la supervisión por la autoridad.
5. Existe un amplio consenso entre los expertos en la materia que un elemento fundamental para el adecuado funcionamiento de las sociedades contemporáneas reside en los flujos de información, e incluso la creación de mercados de información.
6. Aspectos tan cruciales como la creación de nuevas empresas, la investigación científica o la toma de decisiones en general, dependen de contar con sistemas de información. El problema de la legislación es por ello asegurar la protección del derecho a la vida privada

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

sin inhibir los flujos de información. La Ley de Protección de Datos Personales debe adoptar un enfoque regulatorio denominado *opt-in* que pone los controles al momento de crear los bancos de datos. Esto eleva significativamente los costos y crea, por la vía legislativa, obstáculos innecesarios a la creación de bases de datos y en general de los mercados de información en México. La consecuencia inmediata sería menoscabar seriamente la eficiencia y la competitividad de la economía de nuestro país.

La experiencia internacional demuestra que el *opt in* contribuyó a que surgiera un mercado negro de bases de datos. Los costos prohibitivos fueron el incentivo idóneo para que se crearan y transmitieran inadecuadamente bases de datos, lo cual generó incertidumbre y un gran descontento por los sujetos de los datos. Por otro lado, las empresas de mercadotecnia directa emigraron a países con una regulación más laxa o hasta inexistente.[15] Esta situación y la Directiva de Protección de Datos Personales 95/46/CE del Parlamento Europeo han obligado a algunos países, tal como España, a promover una nueva Ley de Datos. En suma, este enfoque regulatorio añade costos significativos a la creación de bases de datos y establece límites para su uso. Esto impide el uso de economías de escala en la generación de bases de datos inhibiendo su efecto positivo sobre el conjunto de la economía.

Un enfoque regulatorio distinto, más moderno, consistiría en proteger los datos personales al momento de "bajar" la información, es decir, al momento de su distribución, difusión o comercialización. Conforme a este enfoque cualquier persona puede solicitar a las empresas que recolecten los datos que los modifiquen o eliminen de sus bases de datos. Este enfoque, conocido como *opt-out*, permitiría no inhibir la creación de bases de datos y de los mercados de información, al mismo tiempo que garantizar una protección eficiente de la privacidad de las personas.

7. Es necesario subrayar que la experiencia internacional muestra de manera contundente que un flujo eficiente de datos personales beneficia a los consumidores, a los oferentes de bienes y servicios y a la

15 Por ejemplo, en el caso de España las bases de datos emigraron a Marruecos, donde se carecía de una legislación específica. En el caso de Alemania, los datos emigraron a Holanda, donde se han establecido todas las empresas de mercadeo directo que sirven al mercado alemán (de donde desaparecieron).

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

eficiencia en general de la economía. La intervención de legislador en materia de datos personales debe responder a diversos objetivos. El primero de ellos es asegurar el derecho a la privacidad de las personas y el derecho de éstas de tener acceso y corregir sus datos personales. Pero otros, no menos importantes, se refieren a propiciar un sano flujo de información en la economía y establecer un marco regulatorio adecuado para la creación de sociedades de información. Por ello, se debe buscar que la Ley de Protección de Datos Personales:

a) Atienda a todos los objetivos de la Ley;
b) No limite las posibilidades de promoción directa de bienes y servicios, lo que restringiría al propio consumidor en su posibilidad de elegir entre diferentes opciones.
c) Evite la aparición de mercado negro de los datos personales: dada la innegable necesidad del flujo de la información para que las actividades económicas se desarrollen eficientemente, es muy probable que los agentes económicos busquen adquirir bases de datos. Una Ley que se proponga eliminar este flujo de información sería la primera promotora del mercado negro de datos personales.
d) Evite la emigración de las empresas de bases de datos: la experiencia internacional demuestra que las empresas de bases de datos se establecerían en un país con menores barreras al flujo de la información. Por un lado, la Ley no lograría su objetivo de proteger los datos personales, ya que los habría empujado fuera de sus fronteras manteniéndolos fuera de su alcance; por el otro lado, habría propiciado la emigración de esos negocios al extranjero (muy probablemente a algún país de Centroamérica o del Caribe), debilitando innecesariamente a una industria en desarrollo; y, elevaría el costo de la información, haciéndola inaccesible para pequeñas y medianas empresas, disminuyendo las posibilidades de desarrollo económico y de eficiencia del mercado, haciendo más lentos e imperfectos a los mercados mexicanos.

XII. GLOSARIO

Controlador de los datos. Es la persona u organización que recolecta, procesa, transfiere, datos personales.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

Dato personal. La información concerniente a una persona física, identificada o identificable.

Datos personales sensibles. Son aquellos que se refieren al origen racial o étnico del sujeto de los datos; a su ideología u opiniones políticas; a sus creencias o convicciones religiosas, filosóficas o similares; a sus características físicas, morales o emocionales; a su vida afectiva y familiar; a sus estados de salud físicos o mentales; a su vida sexual; a la comisión o supuesta comisión de una ofensa judicial; a los procesos judiciales de ofensas o supuestas ofensas judiciales, la eliminación de dichos procesos judiciales o las sentencias de cualquier corte referente a los procesos judiciales enfrentados por el sujeto de los datos.

Procesamiento de la información y los datos personales. Obtener, mantener, o realizar cualquier operación con los datos personales o información derivada de ellos, incluyendo:

— La organización, adaptación o modificación de la información o datos personales;
— La recuperación, consulta o uso de las información o los datos personales;
— La revelación de información o datos personales mediante la transmisión, divulgación o mediante cualquier otra forma de publicación; o,
— Vinculación, combinación, obstrucción, anulación o destrucción de la información o datos personales.

Sujeto de los datos. Es la persona física a quien se refieren los datos personales. En algunos países, tales como el Reino Unido o España, se establece que dicha persona debe estar viva. Con ello, los datos de un difunto han dejado de ser personales.

XIII. REFERENCIAS

CONSEJO EUROPEO, *Directiva 95/46/CE del Parlamento Europeo y del Consejo Europeo 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*, Unión Europea.

FRAASE, Michael, *Information Eclipse: Privacy & Access in America*, Arts & Farces, 1998.

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas

Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx https://biblio.juridicas.unam.mx/bjv Libro completo en: https://goo.gl/jqYbUH

KLUWER LAW INTERNATIONAL, *A Business Guide to Changes in European Data Protection Legislation*, 2000.

MICHAEL, James, *Privacy and Human Rights: An International and Comparative Study, With Special Reference to Developments in Information Technology*, Dartmouth Co., 1994.

NUGTER, A. C. M., *Transborder Flow of Personal Data Within the EC. A Comparative Análisis*, Kluwer International Law, 1991.

OCDE, *Principios de la OCDE para la Protección de la Privacidad de los Datos Personales y sus Flujos Transfronterizos*, OECD.

ROTENBERG, Marc. *The Privacy Law Sourcebook - United States Law, International Law, and Recent Developments*, Electronic Privacy Information Center, 1999.

SMITH, Robert Ellis, *Compilation of State and Federal Privacy Laws*, Privacy Journal, 2002.

SOLOVE, Daniel J., ROTENBERG, Marc, *Information Privacy Law*, Aspen Publisher, 2003.

VILLAR, Rafael DEL, DÍAZ DE LEÓN, Alejandro; y GIL HUBERT; Johanna, *Regulación de protección de datos y de sociedades de información: una comparación de países seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea*, Banco de México, 2001.

Legislaciones consultadas

Reino Unido
Chile
Argentina
Canadá
Brasil
Perú
España (vigente y derogada)

DR © 2004. Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas