Proyecto de Desarrollo de la Industria de las Tecnologías de la Información

ESTUDIO DE AUTORREGULACIÓN EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LAS TI

5ª. Entrega: Versión Final

CONTENIDO

Página

SEGUNDA PARTE

Recomendaciones Generales

Página

Introducción

El presente documento tiene por objeto ofrecer la perspectiva general y conclusiva del estudio "Autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI" promovido por la CANIETI con los auspicios del Prosoft 2.0, en calidad de **reporte final.** Glosando los estudios comparados y los segmentos propositivos de las entregas previas, este reporte se ha dividido en tres partes:

La *primera parte* condensa los estudios comparativos preliminares, donde se expone la situación que guarda en la actualidad la autorregulación en el ámbito de la protección de los datos personales así como sus tendencias, basados en la búsqueda o mapeo de distintos modelos que actualmente existen en el mundo o en México inclusive.

En esa sección se realizan análisis de índole terminológica de conceptos básicos del tema autorregulatorio; se comentan los modelos normativos de heterorregulación, autorregulación pura y de la autorregulación mixta o integrada existentes en materia de protección de datos personales. Y, a efecto de contar con un panorama de referencia, se analizan las particularidades de los modelos analizados en las principales economías del mundo.

Dentro de ellos, se analizan los códigos de conducta y sellos de confianza para determinar los elementos comunes de cada uno de ellos, sin dejar de considerar experiencias puntuales o exitosas de determinadas economías ni los sistemas donde la certificación se ha convertido en elemento que refuerza la credibilidad y eficacia de los distintos esquemas de autorregulación.

La *segunda parte* abarca los resultados de la fase recomendaciones sobre modelos de autorregulación a fin de incorporar a las prácticas nacionales los modelos más eficientes en el desarrollo del comercio electrónico y la economía digital, a través de una metodología que comprende la exposición de ventajas de la incorporación de los esquemas de autorregulación vinculante comparados y otros aspectos requeridos en el apartado de metodología de los Términos de Referencia en el marco de las Reglas de Operación de Prosoft-

De las fases previas (entregables parciales) se han seleccionado referencias específicas sobre la Unión Europea, de Estados Unidos, Canadá y Australia, sin soslayar las propuestas puestas a discusión recientemente en el marco del Foro de Cooperación Económica Asia-Pacifico (APEC, por sus siglas en inglés: *Asia-Pacific Economic Cooperation*) y otras que se han promovido por naciones integradas a la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

Se toman en consideración los aspectos relacionados con principios generales a seguir por los particulares y sobre los principios específicos para el ámbito de las Tecnologías de la Información (TI), así como lo que se refiere a criterios para entidades verificadoras de procesos de autorregulación en materia de protección de datos personales, con el propósito de condensar una propuesta que sirva de base en la discusión de parámetros para los mecanismos de autorregulación para el campo de la privacidad que debe elaborar la Secretaría de Economía con la coadyuvancia del Instituto Federal de Acceso a la Información y Protección de Datos (IFAIPD), de conformidad con el artículo 43 fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

En la *tercera parte*, y aunque no es un requerimiento específico de este estudio, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) de la manera más respetuosa consideró que -desde un punto de vista metodológico- podrían reunirse las propuestas generales y específicas en el marco de un anteproyecto de "parámetros" que, de acuerdo con el artículo quinto transitorio del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) publicado en el Diario Oficial de la Federación del 21 de diciembre del año 2011, deben ser emitidos dentro de los seis meses siguientes a la entrada en vigor del mismo.

Conforme al artículo 85 del Reglamento, los parámetros contendrán los mecanismos para acreditar y revocar a las personas físicas o morales certificadoras, así como sus funciones; los criterios generales para otorgar los certificados en materia de protección de datos personales, y el procedimiento de notificación de los esquemas de autorregulación vinculante.

De acuerdo con los artículos 6 y 14 de la LFPDPPP, los responsables tienen la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.

Es por ello que para la sociedad mexicana representa una oportunidad valiosa de ahondar en el uso de buenas prácticas en acatamiento del principio de responsabilidad, uno de los ocho ejes de observancia ineludible en materia de privacidad y sobre todo de ingresar a una cultura autorregulatoria.

PRIMERA PARTE

Estudio Comparado y Diagnósticos sobre los Modelos de Autorregulación sobre la Protección de Datos Personales

I.- CONCEPTOS GENERALES

El primer esfuerzo conceptual que amerita el presente trabajo, consiste en determinar qué es la *autorregulación*; y al efecto se parte del enfoque etimológico, conforme al cual la palabra proviene del latín aut(o)- *autos* "que actúa por sí mismo o sobre sí mismo", y del latín r*ēgula* (inglés *rule*, francés *regle*, italiano *regola*) "regla", y *–ā -tiōn(em)* latín "proceso de".

Así, la autorregulación (o *autorreglamentación*) se refiere a la capacidad que tiene un sujeto, o una institución, organización o asociación, de regularse a sí misma bajo controles voluntarios. En los distintos ámbitos privados, la autorregulación se constituye como la potestad de establecer reglas por parte del cada sujeto dentro de su esfera de acción, estableciendo –de manera voluntaria y quizás espontánea- normas deontológicas y códigos de autocontrol.

Para el mundo legal tradicional como el mexicano, donde son preponderantes los esquemas de *heterorregulación,* habría que señalar que la autorregulación es una noción muy amplia, pues abarca, por ejemplo, ámbitos como el bursátil, bancario, profesional, publicitario, de la radiodifusión, político, económico, tecnológico, entre otros.

Muchos de estos ámbitos, especialmente los medios de comunicación masiva como la radio, la televisión, la prensa escrita, la publicidad e Internet, ya cuentan con mecanismos de autorregulación, muchas veces relacionados con la metodología y la selección de determinados contenidos que puedan afectar severamente a la sociedad, o bien, con prácticas comerciales.

De acuerdo con la doctrina jurídica anglosajona respecto a los términos *regulation* y *self regulation*, los autores Robert Baldwin y Martin Cave analizan la autorregulación en los supuestos en que un grupo de empresas ejercen un control sobre sus propios medios o comportamiento.[1] Dichos autores examinan los aspectos vinculantes y el voluntario o no-vinculante de los instrumentos de autorregulación, el primero de carácter vinculante, donde el papel de los autorreguladores y la naturaleza gubernamental de la autorregulación puede implicar la adopción de reglas con fuerza jurídica; y el segundo, de carácter voluntario, que puede funcionar de manera informal.

Igualmente, la investigadora Julia Black[2] analiza los problemas en torno al concepto *self regulation,* manifestando que el término *self*, es utilizado con dos significados distintos para hacer referencia a un individuo o para identificar un determinado colectivo. Así, el término autorregulación describe la "disciplina de la conducta por parte de uno mismo". La autora identifica el término *regulation* con el ejercicio de funciones de mando, dirección y control por parte de sujetos privados o de instituciones públicas.

Una de las características de la autorregulación, es la autonomía privada de la voluntad; entendiéndose este concepto como el principio jurídico-filosófico que les atribuye a los individuos un ámbito de libertad, dentro del cual pueden regular sus propios intereses; permitiéndoles crear relaciones obligatorias ente ellos, que deberán ser reconocidas y sancionadas en las normas de derecho.[3]

[1] Concepto y elementos de la autorregulación. En: Http://tdx.cat/bitstream/handle/10803/7681/tmdg3de3.pdf?sequence=3 (Fecha de consulta: 3 de octubre de 2011).
[2] Black, Julia. Constitutionalising Self-Regulation *The Modern Law Review Limited*. Vol 59. 1996 p. 26. En: http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.1996.tb02064.x/pdf (Fecha de consulta: 29 de octubre de 2011)
[3] Enciclopedia Jurídica Mexicana IIJ UNAM, Ed. Porrúa México 2002 Tomo I p. 442

La autonomía privada es libertad individual que permite hacer o no hacer, otorgar al individuo una esfera de actuación; es un reconocimiento del valor jurídico de sus actos que serán vinculantes y preceptivos. El ejercicio de la autonomía privada permite la realización de "actos de autodeterminación y de autorregulación de intereses propios".[4]

Como dato doctrinal o dogmático en la materia, debe decirse que los estudiosos identifican los elementos de la autonomía de la voluntad de la siguiente manera:

1. Los individuos son libres para obligarse o para no hacerlo,
2. Los individuos son libres para discutir las condiciones del acto jurídico, determinando su contenido, respetando al orden público y las buenas costumbres,
3. Los individuos pueden escoger las normas que mejor convengan a sus intereses,
4. Las partes de un acto jurídico pueden determinar los efectos de las obligaciones, y
5. Los intereses individuales libremente discutidos concuerdan con el bien público.[5]

Cabe señalar que la autonomía también puede ser entendida como autolimitación o autovinculación de un sujeto al contenido de las manifestaciones creadas por él mismo. En este sentido, el autor Luigi Ferri indica que:

[4] José Manuel Lastra Lastra. PARADOJAS DE LA AUTONOMÍA DE LA VOLUNTAD EN LAS RELACIONES DE TRABAJO.
En http://www.juridicas.unam.mx/publica/rev/derpriv/cont/5/dtr/dtr4.htm#P105

[5] KUMMMEROV, Gert. Algunos problemas fundamentales del contrato por adhesión en el derecho privado. Universidad Central de Venezuela. Caracas, Venezuela, 1955. pp. 45 y 46. En Enciclopedia Jurídica Mexicana IIJ UNAM, Ed. Porrúa México 2002 Tomo I p. 443

> "…la autonomía privada no es expresión de una mera licitud o facultad, sino manifestación de poder y precisamente del poder de crear, dentro de los límites establecidos por la ley, normas jurídicas".[6]

Para generar modelos de autorregulación exitosos (sellos de confianza o códigos deontológicos) se debe tener presente que la regulación privada tiene una eficacia limitada a aquellos sujetos que, mediante la declaración expresa de la voluntad, deciden someterse a ella. En este sentido se requiere considerar que el resultado de la autorregulación son las normas de carácter vinculante, las cuales únicamente supeditarán a las personas que se han sometido voluntariamente, haciendo uso de su autonomía. Por lo tanto, estas normas no tienen el carácter general y no aplica a todo el conglomerado social.

Ésta característica relativa a la voluntaria aceptación de sus destinatarios, es lo que le confiere eficacia normativa ya que controlan su cumplimiento.

[6] Darnaculleta Gardella, Ma Mercè. Op. Cit. p. 464

II.- LA AUTORREGULACIÓN COMO COMPLEMENTO DE LA LEGALIDAD

Frank Kuitenbrouwer señala que la autorregulación puede servir para varios fines en relación con el proceso legislativo:

- La autorregulación puede tener la intención de evitar la legislación;
- La autorregulación puede ser usada para anticipar la legislación;
- La autorregulación puede servir para instrumentar la legislación; y
- La autorregulación también puede complementar la legislación.

Y el último de los fines señalados por dicho autor holandés, es el que parece que la Ley mexicana le otorga a la autorregulación en materia de protección de datos personales: *complementar la legalidad*[7], es decir, el integrar al régimen júridico[8] aquellas normas que *de facto* son necesarias para organizar y pactar buenas prácticas a través de códigos deontológicos, sin tener que pasar por todo el proceso legislativo, en tanto se da la coexistencia y complemenariedad de los marcos normativos.

El propósito es compensar insuficiencias y limitaciones, favoreciendo así que las actividades objeto de la autorregulación se ajusten a sus propios valores y normas, de ahí que se considere un complemento adecuado de la regulación, principalmente en sectores de especial conflictividad entre derechos fundamentales.[9]

[7] Artículo 44.- Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley.

[8] Régimen jurídico – político conformado por las leyes fundamentales de un Estado.

[9] En este sentido la investigadora Ma Mercè Darnaculleta señala que los límites y las fricciones entre derechos fundamentales, las fronteras entre lo legal y lo ético son especialmente delicadas en el ámbito de la publicidad y los medios de comunicación. Véase Darnaculleta Gardella, Ma Mercè Op. Cit. p. 438.

La interpretación de los objetivos de la autorregulación conlleva a encontrar marcos normativos dentro de los cuales interactúen los miembros de una entidad, sector o de una organización, por consiguiente los objetivos para posibilitar el uso eficiente y respetuoso del Internet es implementar medidas normativas en cada caso específico, por ejemplo la protección del comercio electrónico, o la privacidad en redes sociales.

Indudablemente el Internet es uno de los temas con mayor auge en la vida cotidiana de las personas, de ahí que la intervención tanto de la sociedad civil como de los gobiernos, ha incurrido en análisis y debates para su regulación. En este sentido se han generado mecanismos autorregulatorios aplicados de manera específica en algunos sitios web[10] como en el sector comercio, redes sociales y otros.

Por lo tanto, la problemática jurídica que impera en este ámbito donde se busca que prevalezca la libertad ha encauzado mecanismos de autorregulación. Particularmente, cada ámbito del ciberespacio es factible de regularse con el propósito de otorgar confianza a los usuarios.[11]

Los esfuerzos para regular el Internet, principalmente en el campo del comercio electrónico son, en primer lugar, justificables como una alternativa ante la sociedad de la información que carece de límites territoriales y por lo tanto jurídicos. Dicha justificación se impone cuando una nación soberana no

[10] *World Wide Web* (www), se conoce como un sistema distribuido sin un control centralizado, en LUZ Álvarez, Clara. Internet y Derechos Fundamentales. Editorial Porrúa, México 2011, p. 10

[11] "La autorregulación proporciona mecanismos para sancionar conductas contrarias a los códigos de conducta, los actores privados desarrollan medios para asegurar que los códigos de la autorregulación pasen de la letra a la acción. Las líneas de acceso directo (*hotlines)* creadas dentro del marco de ciertos códigos de conducta que permiten la denuncia de actividades contrarias a esos códigos, lo cual es un ejemplo más de los medios establecidos para garantizar la observancia de la disciplina de red."
Poullet, Yves. "Some considerations on Cyberspace Law" en UNESCO, *The International Dimensions of Cyberspace Law*, Burlington, UNESCO, 2000, P. 156. Citado por LUZ Álvarez, Clara. Op. Cit., pp. 55 y 56

puede imponer sus leyes sobre una actividad de la que se aprovecha la comunidad internacional.

Bajo estas justificaciones, se crean los códigos de conducta, con los cuales no se pretende sustituir el control legal, sino un conformar un complemento de éste al cual las partes interesadas voluntariamente acudirán de buena fe.[12]

Algunos estudiosos de la materia opinan que la autorregulación es un instrumento idóneo para contribuir a que las estructuras de gobierno puedan atender y resolver las problemáticas derivadas del Internet. En razón a ello, la especialista Clara Luz Álvarez, menciona las ventajas de la autorregulación sobre la regulación estatal para Internet, enunciando que son:

> "…su mayor prontitud, flexibilidad y eficacia; el aprovechar la experiencia acumulada de la industria; y que los recursos gubernamentales son limitados. La autorregulación permite que – si existe voluntad-, se implemente regulación más eficaz, provista de mecanismos de sanción dentro del ámbito privado."[13]

Bajo esta premisa, el Estado también interviene en el proceso de autorregulación, para complementar los aspectos legales existentes. De ahí que para nosotros el tema semántico nos podría llevar a hablar de una *corregulación o regulación cooperativa*, pues al complementarse la voluntad de los gobernados o la autoridad del gobierno, se sale del sentido estricto de la autorregulación[14] (quizás mal empleada por el legislador mexicano).

Pero más allá de digresiones académicas, la principal manifestación de la autorregulación en el mundo del Internet es la imposición, a través de

[12] http://www.uned.ac.cr/redti/documentos/regulacion.pdf (Fecha de consulta: 3 de octubre de 2011).
[13] LUZ Álvarez, Clara. Op. Cit., pp. 54 y 55.
[14] Véase más adelante la concepción australiana, que se refiere a este tema como "co-regulation".

entidades privadas o de los usuarios del ciberespacio, de "recomendaciones vinculantes"[15] para que sean consideradas y aplicadas. La pregunta radica en saber hasta dónde deben ser reconocidas por el Estado, gobierno o autoridad.

Pero si partimos del modelo previsto en la LFPDPPP, pudieran ser útiles las ideas de J. Black, quien ha desarrollado teorías acera de la autorregulación como complemento de la legalidad con la intervención estatal. Según él existen 4 modalidades:[16]

1. Autorregulación vinculante: en la que una organización o grupo de sujetos privados es designado para dictar y aplicar normas dentro de un grupo generalmente establecido directamente por los poderes públicos (*mandated self - regulation*).

2. Autorregulación aprobada: en la que los estándares son elaborados por sus destinatarios, y adoptados finalmente por los poderes públicos (*sancionated self - regulation*).

3. Autorregulación compelida: se caracteriza porque los estándares son adoptados de manera autónoma ante la amenaza de una eventual intervención normativa pública (*coerced self - regulation*).

4. Autorregulación voluntaria: no hay intervención pública dirigida a imponer o fomentar, directa o indirectamente, la autorregulación (*voluntary self - regulation*).

[15] El carácter de vinculante implica el acatamiento de tales recomendaciones, al grado de ser considerados como normas.
[16] J. Black. Constitutionalising Self- Regulation. Modern Law Review 1996. 59-1, p. 24. Citado por JIMÉNEZ Arroyo Luis; Et. Al. Autorregulación y sanciones. Editorial Nex Nova, España 2008 p. 26.

Con la idea de que el resultado de la autorregulación es un conjunto de normas de carácter vinculante, algunas de carácter jurídico con obligatoriedad general, y otras únicamente vinculan a las partes que se han sometido voluntariamente, se considera también que una de las variantes de la autorregulación es la corregulación y la autorregulación regulada, en ambos casos interviene el Estado implementando estándares o modelos a los que la industria o sector debe seguir.

El carácter vinculante como resultado de la autorregulación regulada ó regulación pública de la autorregulación, se entiende como el proceso de autorregulación con fines públicos y puede imponerse gubernamentalmente o puede surgir de forma espontánea, viniendo a cubrir la falta de implicación estatal en un determinado sector o industria.

En Alemania, los juristas han debatido sobre las aportaciones de la autorregulación a la materialización de fines y/o funciones públicas. Es en este contexto donde se ha introducido recientemente la noción de *autorregulación regulada* (*Regulierte Selbstregulierung*).[17]

Otra variante de la autorregulación ha sido reconocida como *autorregulación resolutiva,* mediante la imposición de sanciones disciplinarias y resoluciones arbitrales, las cuales son de carácter sancionador y arbitral por parte de la Administración Pública.

En este contexto, la Administración Pública utiliza las “reglas técnicas” para atribuir efectos vinculantes a la autorregulación, las cuales permiten cumplir con los fines perseguidos por una actividad profesional, se dice que son normas procedimentales que describen cómo debe realizarse una concreta

[17] Idem p. 467

actividad, y son plasmadas en normas técnicas, códigos y manuales de buenas prácticas, protocolos y procedimientos normalizados de trabajo.[18]

Asimismo, la Administración Pública utiliza "reglas éticas" para describir las conductas o comportamientos que se consideran acordes a los valores asumidos por la propia profesión, estas reglas se traducen en normas deontológicas tales como códigos éticos o códigos de buena conducta; los cuales tienen efectos habilitantes, probatorios, vinculantes o de cosa juzgada. En cuanto a sus efectos públicos, se está frente a una especie de "nueva estrategia reguladora del Estado", que incide en lo que se conoce como la autorregulación regulada[19]

En este orden de ideas, una primera conclusión es que la autorregulación es un mecanismo que no sustituye las leyes, sino que es una herramienta complementaria al marco legal para fomentar buenas prácticas.

Y en el ciberespacio, el objetivo central de la autorregulación es generar confianza en la interacción de los usuarios de Internet; y en este sentido se busca equiparar las acciones y las gestiones en un marco ético para mejorar la calidad de un servicio en el mundo del Internet.

Para lograr éstos objetivos, se han implementado los códigos de conducta o la "Netiqueta", llamada así, la etiqueta de la red o reglas de trato social asumidas por los usuarios como código social de Internet, y que se identifica como las reglas en las prácticas comunes, es decir, lo relativo al comportamiento en Internet. La palabra Netiquette se forma por las palabras

[18] Darnaculleta Gardella, Ma Mercè. Op. Cit. pp. 493 y 494

[19] Ley 22/1999 Ordenamiento Jurídico Español, en su Disposición Adicional Tercera "Promoción de la autorregulación" "Los poderes públicos promoverán el desarrollo de organizaciones de autorregulación del sector, pudiendo acudir, también, a ellas cualesquiera personas o entidades que se consideren perjudicadas". (ver p 438 de concepto y elementos de autorregulación)

"Network" y "Etiquette", la Netiquette son lineamientos para el uso responsable del Internet que incluye preceptos de urbanidad.[20]

A medida que Internet se ha desarrollado, las categorías de sitios Web han evolucionado con las normas culturales de la interacción, la Netiqueta. Cada categoría de sitios web admite todas las formas de contenido de Internet en algún grado. Ellos tienen su propia cultura. Los diversos conjuntos de reglas son las netiquettes.[21] Clara Luz Álvarez indica que "la regulación del Internet por las reglas de conducta reenvía a una concepción del Derecho más "negociado" que impuesto (…) ante todo pluralista y entonces la acción multiforme tiende a restablecer o a asegurar un equilibrio social." De ahí que éste objetivo corresponde a la equiparación de conductas en los diversos sectores en Internet.

En consecuencia, la autorregulación aplica medios de control para disciplinar la actividad estableciendo controles y límites en la red. Al respecto es recomendable el estudio que realizó el Proyecto i+Confianza en el año 2002[22] para comparar 19 marcas o sellos de confianza:

1) L@belsite (Francia)
2) Trusted Shops (Alemania)
3) Comercio Certificado (Argentina)
4) e-com-quality mark (Italia)
5) DIN Tested Website (Alemania)
6) Qweb (Italia)

[20] LUZ Álvarez, Clara. Op. Cit., pp. 54
[21] http://www.networketiquette.net/netiquette.htm (Fecha de consulta: 1 de octubre de 2011).
[22] i+Confianza es un proyecto promovido por: Asociación Española de Normalización y Certificación (AENOR), Asociación Española para el Derecho y la Economía Digital (AEDED). Real e Ilustre Colegio de Abogados de Zaragoza (REICAZ) Fundació Catalana per a la Recerca (FCR) El documento producido por este proyecto se denomina "Libro Blanco sobre los Sistemas de Autorregulación, los Sellos de Confianza en Mercados Digitales y Códigos de Buenas Prácticas". AENOR, España, Diciembre 2002.

7) Trust-e (Estados Unidos)
8) Squaretrade (Estados Unidos)
9) Webassured (Estados Unidos)
10) Consumer Trust (Singapur)
11) Health On the Net (Suiza)
12) BBBOnline Reliability (Estados Unidos)
13) BBBOnline Privacy (Estados Unidos)
14) Confiar-e (Chile)
15) [G] Garantía de Protección de Datos (España)
16) AGACE (España)
17) Bureau Veritas Web Value (Francia)
18) IQA (España)
19) Marca AENOR de Buenas Prácticas Comerciales (España)

De estos sellos, subsiste la mitad: Trusted Shop, Qweb, Trust-e, Web Assured, Hon Code, Confiar-e, [G] ahora como Confianza Online, AGACE y AENOR. BBBOnline Reliability y BBBOnline Privacy se fusionaron en Better Business Bureau, que tiene el "Business Seal for the Web"[23].

Cabe resaltar que la Asociación Mexicana de Internet, A.C. (AMIPCI)[24], ha sido una instancia fundamental para promover la autorregulación, constituyéndose como la más importante asociación encargada de otorgar los Sellos de Confianza[25], con la idea de que se constituya -no sólo como un evaluador de las políticas de privacidad y existencia física-, sino como un evaluador de procesos, incluyendo también la verificación de existencia de medidas de seguridad, receptor de quejas, enlace entre las instituciones

[23] Wwww.bbb.org/us/bbb.online-business/
[24] http://www.amipci.org.mx/
[25] https://www.sellosdeconfianza.org.mx

reguladoras y los individuos e incluso mediador en caso de quejas y conflictos.[26]

Dicha iniciativa nacional se inserta en las políticas de los Organismos Internacionales en torno a las nuevas tecnologías e Internet, los cuales trabajan en forma conjunta con el sector privado para establecer preceptos de protección y seguridad. Se trata un esfuerzo cooperativo que se ha reflejado, principalmente, en los siguientes instrumentos normativos y acciones:

1. La Organización para la Cooperación Económica en Asia-Pacifico (APEC) con la regulación de los Proveedores de los Servicios de Internet (ISP´s); se enfoca al examen de las tarifas de cobro de los ISP´s (de acuerdo a la región en la que laboren, el desarrollo, funcionalidad y condiciones de los proveedores) y lo relacionado al tráfico de los flujos de información.[27]

   El proyecto Data Privacy Pathfinder de APEC se ha ido consolidando para analizar e identificar las mejores prácticas en materia de privacidad; así como para promover nuevas reglas de privacidad transfronteriza.

2. La Unión Internacional de Telecomunicaciones (UIT), órgano de ONU, es la principal rectora internacional en materia de telecomunicaciones, la cual se encarga de analizar, especialmente, las cuestiones del sistema de nombres de dominio.[28]

[26] KRAFFT Reyes, Alfredo. Nota informativa.
[27] Regulación Jurídica de Internet En: http://www.diputados.gob.mx/cedia/sia/spe/SPE-ISS-12-06.pdf (Fecha de consulta: 27 de septiembre de 2011).
[28] Unión Internacional de Telecomunicaciones http://www.itu.int/council/C2011/index-es.html (Fecha de consulta: 4 de octubre de 2011).

3. La Organización para la Cooperación y el Desarrollo Económico (OCDE) analiza en términos generales la problemática del ciberespacio, elabora propuestas y las ofrece a los países miembros. Este organismo considera la legislación de cada Estado en lo referente a los actos ilícitos en torno al Internet, y establece estándares sobre privacidad y protección de datos personales.

   De las aportaciones de la OCDE destaca el Documento sobre Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico (1999), en el cual se propusieron "mecanismos de atención de quejas y resolución de disputas", mediante la participación de representantes de los consumidores.[29]

4. En materia de comercio electrónico en específico, los organismos internacionales que vienen promoviendo regulaciones o la armonización normativa de los países son: la Organización Mundial de la Propiedad Intelectual (OMPI- WIPO); la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI – UNCITRAL); la Organización para la Cooperación y el Desarrollo Económico (OCDE- OECD); el Área de Libre Comercio de las Américas (ALCA), y la Cámara de Comercio Internacional (CCI - ICC).

5. Por otro lado, la Red Iberoamericana de Protección de Datos [30] surge en respuesta a la necesidad de fomentar e implementar el Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los Países

[29] Establece que en el comercio electrónico debe llevarse a cabo de acuerdo con principios de privacidad que proporcionen una efectiva y apropiada protección a los consumidores. En este sentido, propone que los Estados miembros implementen medidas que promuevan las prácticas autorregulatorias para hacerlas factibles al comercio electrónico.
[30] http://www.redipd.org/ (Fecha de consulta: 4 de noviembre de 2011).

Iberoamericanos, a que elaboren una regulación normativa en esta materia a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

6. La Unión Europea[31] también ha establecido preceptos que fortalecen las actividades en torno al comercio electrónico y la protección de datos personales, en estos temas destaca la Directiva 95/46/CE en materia de protección de datos personales, el cual crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). La Directiva 1999/93/CE del Parlamento Europeo y del Consejo[32] por el que se establece un marco regulatorio para la firma electrónica.[33]

7. Otros organismos internacionales o intergubernamentales con mayor participación en Internet vinculados son: la ONU y la UNESCO, la Organización de los Estados Americanos (OEA), y la Organización para la Seguridad y Cooperación en Europa (OSCE).[34]

En todos estos organismos, sus resoluciones y acuerdos se encuentra que la autorregulación es una herramienta para fomentar la protección de datos personales.

[31] La UE Participa en el Acuerdo de WTO (World Trade Organization) sobre servicios de telecomunicaciones básicos, igualmente en el Acuerdo de ITA (International Trademark Association) sobre tarifas en materia de productos de tecnología de la información, y en el Acuerdo de WIPO (World Intellectual Property Organisation) sobre protección de la propiedad intelectual. Todos estos avances se basan en la convicción de que la Sociedad de la Información sólo puede ser global con una amplia participación de la comunidad internacional. AZNAR Gómez Hugo, y VILLANUEVA, Ernesto. Deontología y Autorregulación Informativa. Ensayos desde una perspectiva comparada. Universidad Iberoamericana (México). Fundación Manuel Buendía (México), Fundación Manuel Buendía. México p. 127.

[32] http://www.boe.es/doue/2000/013/L00012-00020.pdf (Fecha de consulta 8 de noviembre de 2011).

[33] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:258:0011:0019:ES:PDF (Fecha de consulta: 16 de noviembre de 2011).

[34] Luz Álvarez, Clara. Op. Cit., p. 46

III.- CONSIDERACIONES SOBRE LA AUTORREGULACIÓN Y SUS EFECTOS

A fin de ponderar ideas diferentes sobre el tema de la autorregulación en el ámbito de las TI, resulta importante considerar ideas como las de Henry H. Perritt, Jr., quien dice que "*mientras que las normas para proteger la privacidad personal cuando estas tecnologías se usan con gran amplitud se aceptan razonablemente bien, no existen los marcos de trabajo regulatorios para aplicar las normas, y casi nadie concuerda en cuáles son los mejores enfoques regulatorios"* Para él es importante que se sigan explorando modelos regulatorios alternativos, con énfasis en las condiciones previas para lograr una auto-regulación eficaz[35].

Sostiene además que el problema principal con la autorregulación es de índole política: los grupos de consumidores y los defensores de la privacidad están preocupados de que la autorregulación no proteja lo suficiente los intereses de los sujetos de datos. "*Suponiendo que el problema pueda solucionarse, todavía hay diversos retos legales y conceptuales para hacer eficaz la autorregulación".*

Afirma Perritt que en tanto los programas regulatorios tienen éxito en gran parte a través del cumplimiento voluntario, "también deben tener algún medio para su ejecución":

> "De otra forma, los miembros recalcitrantes de una industria no pueden sólo evitar las normas regulatorias, sino también obtener una ventaja competitiva sobre aquéllos que sí cumplen con las normas. Cualquier programa regulatorio pretende limitar la competencia en el asunto de la regulación, y como un cartel, el marco de trabajo de la autorregulación tiende a desenmarañarse por las "ovaciones".

[35] Henry H. Perritt, Jr., Profesor de la Facultad de Derecho de la Universidad Villanova Villanova, PA 19085 **http://www.law.vill.edu**

Debe considerarse su opinión en el sentido de que uno de los problemas del diseño de un esquema de autorregulación es definir los beneficios que serán eliminados por la expulsión. Dice: "*En ausencia de tal beneficio, la expulsión es una sanción ineficaz y el incumplimiento no puede ser castigado, y así, el esquema regulatorio tiende a ser ineficaz*".[36]

El holandés Frank Kuitenbrouwer, sostiene por otro lado que "*La autorregulación se ha convertido en uno de los rasgos principales de la "segunda generación" de las leyes de protección de datos en Europa, que se caracteriza por un esfuerzo por reducir las cargas administrativas para los controladores de datos personales*"[37]. Informa asimismo que los Países Bajos ofrecieron uno de los primeros ejemplos de autorregulación en este campo.

Señala que en 1974, una Comisión Real estuvo a cargo de estudiar la necesidad de legislar la privacidad. En su informe provisional, la Comisión invitó a instituciones sociales a unirse en un esfuerzo por proteger los datos. Los elementos principales de la protección de datos no sólo dependen de la reglamentación gubernamental, observaba la Comisión Real, sino pueden ser establecidas por las partes involucradas; de manera que el elemento de la autorregulación desempeñaba una función al principio del proceso

[36] Una de las propuestas recientes más interesantes de un mecanismo autorregulador es construir la autorregulación alrededor de la administración de los nombres de dominios. Promovida por David R. Johnson y David Post, este medio de auto-gobernabilidad requeriría que todos los que obtengan un dominio en la Internet cumplan con ciertas reglas elaboradas por una o más asociaciones privadas que administren el registro de los dominios. Si no se cumplen las reglas, se cancelará el dominio y se negará la participación del infractor en la Internet. Esto resolvería el problema de los incentivos y las amenazas. No resuelve otro problema que surge de la aplicación de la ley de competencia (anti-monopolio) en los Estados Unidos y en cualquier otro país. Es una violación a la ley de competencia que los competidores combinen un conjunto de términos de competencia y después ejecuten tales términos sobre sus competidores. Eso es exactamente lo que entraña la autorregulación, aunque puede ser analizada con menos rigor que un cártel que establecería los términos de la competencia en los precio.

[37] Kuitenbrouwer, Frank, Autorregulación: Algunas Experiencias en Holanda, Comentador Legal NRC Handelsblad, Ámsterdam, Holanda.

propuesto con la finalidad de la adopción de leyes para la protección de datos.

La Comisión Real finalmente elaboró un enfoque de tres niveles: 1) Autorregulación obligatoria para los usuarios individuales (la DPA establece formas separadas de autorregulación para los bancos de datos de los sectores privado y público); 2) Autorregulación opcional sobre el nivel de sector (la ley establece la elaboración preliminar de códigos de conducta por organizaciones sectoriales comerciales y profesionales, de preferencia en consulta con grupos de sujetos de datos, que pudieran presentarse a la aprobación de la Cámara de Registro); 3) Códigos de Conducta (elaborados por organizaciones sectoriales comerciales y profesionales bajo lo estipulado por la DPA han sido definidos como "un puente" entre las reglas sustantivas de la Ley de Protección de Datos (Data Protection Act, DPA) y su instrumentación a nivel operativo)

Con otro enfoque, Mary Clare Fitzgerald y Paul A. Sauder[38] señalan que:

> "…en un entorno operativo de rápida evolución, es muy apropiado que las personas que cuentan con el conocimiento y la experiencia técnicos – en este caso el sector privado – tengan la responsabilidad de lo que el Senador Maloney llamó la "regulación técnica" mientras que una dependencia regulatoria gubernamental federal adecuada – o un grupo de dependencia – tenga la supervisión amplia y facultada para enfrentarse al "área adyacente submarginal que no reconoce ninguna sanción excepto las de la legislación penal" y otros asuntos de regulación y ejecución para los que el sector del comercio electrónico es "inadecuado o incapaz de enfrentar."

Agregan que históricamente, los reguladores han podido regular por su facultad de permitir el acceso al mercado. "*Simplemente se negó la entrada o*

[38] Mary Clare Fitzgerald/Paul A. Seader, Comercio Electrónico… Su Reglamentación no está Estrechamente Relacionada con la Banca".

se confinó la entrada a actividades o funciones muy limitadas a las entidades que estaban renuentes o eran incapaces de cumplir".

Stephen Balkam,[39] señala que la autorregulación exitosa de alguna manera se reduce a incentivos y amenazas:

> "¿Cuáles son los incentivos positivos que motivarán a una industria a regularse a sí misma y cuán lejos irá el gobierno para amenazar, convencer con halagos o rogar a una industria para que ponga las cosas en orden? ¿Y en qué punto una legislatura simplemente impondrá leyes a un sector renuente y recalcitrante?"

Y agrega:

> "En mi experiencia en dos industrias diferentes pero relacionadas – la del software y la de Internet, y mi participación en una tercera, la de la televisión, diría que es muy raro que un grupo de compañías voluntariamente (en el verdadero sentido de la palabra) y sin que se le exija, decida establecer un sistema estricto de políticas autoimpuestas que costará a sus miembros tiempo y dinero establecer, administrar, promover y desarrollar. Además, podría argumentarse que para hacer esto tendría que ir contra la misión de la mayoría de las asociaciones comerciales *a menos que* hubiera una amenaza muy real y potente de que el gobierno central promulgara una legislación similar, si no peor. Sólo entonces puede una asociación de la industria legítimamente utilizar las contribuciones de sus miembros en proponer el establecimiento de un régimen autorregulador".

Desde su punto de vista, el gobierno tiene la función de reflejar las preocupaciones legítimas del público y llevar tales problemas a un público más amplio a través de audiencias, reportes publicados en la prensa y, finalmente, promulgar leyes. Frases rescatables de él son:

[39] Stephen Balkam. Clasificación de Contenido para la Internet y el Software Recreativo. Director Ejecutivo. Recreational Software Advisory Council (Consejo Asesor en Software Recreativo)

- *Creo firmemente en la buena autorregulación y el buen gobierno*. Con el marco de trabajo adecuado, las verificaciones, los balances, la vigilancia y los controles, la autorregulación es con mucho una ruta más atractiva que la promulgación de leyes por el gobierno central.
- *Pero la autorregulación es una vía difícil y requiere de tiempo, dinero y recursos para hacerla funcionar.* También requiere de una alianza saludable entre la industria, el gobierno y el público general para que tenga éxito.

Expuestas las bondades de la autorregulación, en la medida en que la globalización de las nuevas tecnologías prospera día a día, el crecimiento del flujo transfronterizo de datos y su desarrollo acerca a empresas y ciudadanos, se han expuesto problemas de control o de autocontrol en la aplicación de los sistemas autorregulatorios.

Entre los conflictos que puede presentar la autorregulación, se considera, principalmente, la insuficiencia en la protección de los datos y la falta de eficacia en el cumplimiento normativo. Por ello se afirma que la autorregulación -por sí sola- no es suficiente para alcanzar un sistema de protección jurídica adecuado para la tutela de un derecho fundamental como es la protección de los datos personales, debido a que su protección queda fuera de la intervención estatal.

Al efecto se sostiene que la autorregulación, entendida como el cumplimiento de un compromiso autoimpuesto por un sector no debe tener mayores problemas que los que emanan del cumplimiento de la legislación, considerando que la corregulación[40], al intervenir distintos agentes

[40] El concepto de corregulación aplica cuando un sector o empresa negocia este acuerdo que quiere autoimponerse con otros agentes sociales, actores o incluso con la Administración Pública. "La

negociadores en el proceso plantea problemas más extensos que pueden resumirse en: el control y el cumplimiento de los acuerdos.

Igualmente se ha llegado a decir que en al ámbito de las TI -en continuo desarrollo-, el nivel de conocimiento en estos temas se ve rebasado por las nuevas tecnologías, impidiendo así que las personas puedan acceder a mejores oportunidades de interactuar en el ciberespacio.

En se contexto se coloca como enemigo de la autorregulación el llamado "analfabetismo tecnológico", debido a que:

> "… lo tecnológico aparece enmarcado en una nueva concepción de hombre - ordenador, y dada su complejidad, aparece la figura de operador- usuario, que se obliga a estudiarse como un modelo filosófico–antropológico. Así pues, el "analfabetismo tecnológico" se relaciona directamente con el ámbito laboral, debido a que en todos los órdenes del mercado se implementan recursos tecnológicos de avanzada, principalmente, en el ámbito de la informática.[41]

corregulación combina medidas legislativas y reglamentarias vinculantes y medidas adoptadas por los agentes más interesados sobre la base de su experiencia práctica." Conceptos n p. 436

[41] http://lugospectiva.blogspot.com/2005/10/analfabetismo-informatico.html (Fecha de consulta: 3 de diciembre de 2011).

IV.- TERMINOLOGÍA Y DEFINICIONES

En el ámbito de la conceptualización[42], se puede establecer que un primer apartado sustancial que la "coadyuvancia" entre la Secretaría de Economía y el IFAIPD debe comprender, es el consenso sobre la definición de la variada gama de conceptos que se involucran en el mundo digital universal y, en particular, para las Tecnologías de la Información en México.

En otras palabras, todo parámetro que se emita en un Estado de Derecho y esté en posibilidades de ser efectivo y resista objeciones de los sectores privados involucrados, requiere de la previa afinación terminológica para que las políticas públicas y/o regulatorias encuentren un basamento uniforme y comprensible.

No se trata de impulsar un examen de las propiedades programáticas o sintácticas del vocabulario en esta materia, sino de evitar distorsiones semánticas desde el principio mismo de la construcción de enunciados con valor jurídico, como son –entre otros- los relativos a autorregulación, parámetro, sector de las TI, certificación, hardware, etc.

Esta consideración se sostiene en lo que la Comisión Federal de Mejora Regulatoria (COFEMER) ha señalado:

> "Cuando los diseñadores de las políticas regulatorias requieren analizar algún problema que se presenta en la sociedad, pueden tener diferentes visiones sobre la mejor manera de corregir dicha problemática con el uso de la regulación. El regulador puede considerar criterios o enfoques tanto de tipo **normativo** como de tipo **positivo**, así como diversos elementos que son proporcionados por la teoría de la regulación."

[42] Una base para entender los conceptos en comunicación y tecnología: http://www.scribd.com/doc/5170566/Communication-Technology

> "Por esta razón, los hacedores de las políticas públicas deben contar con criterios teóricos sólidos para enriquecer su visión en el diseño del marco regulatorio e intervenir adecuadamente en la solución de los problemas de la sociedad. La teoría de la regulación proporciona el conocimiento experto que los reguladores requieren para encontrar soluciones y generar los mayores impactos positivos hacia la sociedad. Las políticas regulatorias serán más robustas y más efectivas en la medida que las mismas sean confeccionadas con una buena **visión teórica**"[43].

En una era en la que el concepto de gobernanza regulatoria tiene un amplio sentido, *reglar la autorregulación* amerita que la terminología sea considerada un elemento indispensable de los parámetros y para ello se ensayan algunas definiciones de orden general en el presente apartado.

4.1 Autorregulación

Acerca de este concepto se ha seguido primeramente a la Comisión Europea, conforme a la cual autorregulación puede entenderse como *"cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión".*

Esta definición amplia o en *latu sensu*, abarcaría "*desde un código de protección de datos voluntario desarrollado por una pequeña asociación industrial con pocos miembros, hasta los detallados códigos de ética profesional aplicables a profesiones enteras, tales como médicos o banqueros, que suelen tener una fuerza cuasi jurídica".*[44]

[43] COFEMER. Primer Diplomado en Regulación. DIPLOMADOS COFEMER/LATIN-REG. : Lectura 2. Modulo I. Marzo, 2012

[44] Comisión Europea, *Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?*, adoptado por el Grupo

En México, de acuerdo con el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *"Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley".*

Estos esquemas de autorregulación podrán traducirse en "*códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares".*

Partiendo de lo previsto en la LFPDPPP, que dentro de cuatro modalidades de autorregulación[45] recoge la vinculante[46], entendemos que es aquella en la que una organización o grupo de sujetos privados es designado para dictar y aplicar normas dentro de un grupo generalmente establecido (o reconocido) directamente por los poderes públicos (*mandated self - regulation*).

Tanto la LFPDPPP como su Reglamento publicado en el Diario Oficial de la Federación del 21 de diciembre del año 2011, permiten que para cumplir con el principio de responsabilidad, los responsables (persona física o moral de carácter privado que decide sobre el tratamiento de datos personales) podrán valerse de estándares, mejores prácticas internacionales, políticas

de Trabajo sobre Protección de Datos de carácter personal el 14 de enero de 1998, DG XV D/5057/97 final.

[45]J. Black. Constitutionalising Self- Regulation. Modern Law Review 1996. 59-1, p. 24. Citado por JIMÉNEZ Arroyo Luis; Et. Al. Autorregulación y sanciones. Editorial Nex Nova, España 2008 p. 26.

[46] Las otras tres son Autorregulación aprobada (*sancionated self - regulation*); Autorregulación compelida (*coerced self - regulation*); y Autorregulación voluntaria (*voluntary self - regulation*).

corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines[47].

Al mismo tiempo se establece en el artículo 80 del Reglamento citado que **"**Los esquemas de autorregulación (vinculante) podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos…" Aunado a ello, el artículo 83 del mismo Reglamento autoriza que **l**os esquemas de autorregulación vinculante puedan incluir la certificación de los responsables en materia de protección de datos personales.

Pero con la finalidad de ir concibiendo un marco que sirva para darle una mayor perspectiva, se propone en seguida un esquema que permita vislumbrar todos los sentidos de la "autorregulación vinculante", basados en el modelo que reconoce que toda conceptualización jurídica debe atender aspectos sustantivos; objetivos, subjetivos, formales, materiales y, por supuesto, adjetivos.

[47] Artículo 47 del Reglamento de la LFPDPPP.

a) AUTORREGULACIÓN VINCULANTE DESDE EL PUNTO DE VISTA SUSTANTIVO

Concepto Objetivo

En Sentido Formal. Conjunto de normas que tienen por objeto complementar lo establecido en las leyes y reglamentos federales en materia de protección de datos personales en posesión de particulares, así como generar reglas o estándares que permitan armonizar los tratamientos de datos efectuados por las personas que se adhieran a los mismos y faciliten el ejercicio de los derechos de los titulares.

Desde este punto de vista, la autorregulación vinculante comprende el estudio de la estructura de los esquemas de autorregulación, tales como códigos de deontológicos, códigos de buena práctica profesional, sellos de confianza y otros mecanismos.

En Sentido Material. El estudio de los esquemas de autorregulación, de las conductas que las infringen y de las sanciones aplicables a las mismas.

Comprende el estudio de la esencia de la autorregulación, función de los códigos, sellos de confianza y demás normas autorregulatorias, teorías de la función autorregulatoria, teorías de la autorregulación, etc.

Concepto Subjetivo

El derecho del Estado de reconocer y promover esquemas de autorregulación y el derecho de los gobernados para crearlos y aplicarlos.

Bajo esta perspectiva, comprende el análisis de los fundamentos del derecho del Estado para reconocer mecanismos de autorregulación y de los particulares para establecer modelos regulatorios alternativos, sus procesos de control, evaluación, ejecución, incentivos y amenazas.

b) AUTORREGULACIÓN VINCULANTE DESDE EL PUNTO DE VISTA ADJETIVO (procedimental o procesal)

Conjunto de reglas que determinan los actos, las formas y las formalidades que deben observarse en la aprobación, reconocimiento, aplicación y ejecución de los esquemas de autorregulación para hacer factible sus fines. Contiene previsiones dirigidas a responsables, titulares de los datos, usuarios, clientes, proveedores, empleados, encargados, terceros y demás personas (particulares) involucradas en el tratamiento de datos personales.

4.2 Esquemas de Autorregulación

Toda vez que los esquemas de autorregulación vinculante solamente se enuncian de forma ejemplificativa por la ley y su reglamento, exponiéndose sus objetivos, es necesario que los parámetros definan el género (esquemas de autorregulación) y las especies:

1) Códigos deontológicos;
2) Código de buenas prácticas profesionales;
3) Sellos de confianza;
4) Políticas de privacidad;
5) Reglas de privacidad corporativas;; y
6) Otros mecanismos, que incluyan reglas o estándares específicos.

De manera somera y a manera de ejemplo, se exponen definiciones existentes sobre estos temas, con la idea de analizar la importancia que tiene el hecho de que la autoridad no defina unilateralmente los parámetros, sino en consenso con la industria.

Códigos Deontológicos. "Un código de deontología consiste normalmente en una serie de cláusulas que definen los comportamientos correctos e incorrectos de los funcionarios, previendo en algunos casos las sanciones específicas para los comportamientos incorrectos. Estas cláusulas son normativas y no le dejan prácticamente ninguna autonomía al funcionario. Se concentran en las funciones esenciales de la organización más que en los ideales éticos generales, y se inclinan a ser actos jurídicos en el sentido pleno incluso en los textos jurídicos o en las reglamentaciones"[48].

[48] BAR CENDON, Antonio, ***Responsabilidad y ética: El papel de los valores y los procedimientos legales en el mejoramiento de las normas***, Instituto Nacional de Administración Pública, "Por una

Un código de ética, por el contrario, "consiste en una serie de principios y de criterios que sirven de lineamientos al comportamiento de los funcionarios. Aunque los códigos de ética puedan variar en su contenido, incluyendo por lo general valores y principios éticos que son el fundamento de la institución que rigen, y contribuyen a resolver los dilemas a los que los funcionarios pueden verse confrontados en las decisiones a tomar en su trabajo diario"[49].

Los códigos de ética tienen como consecuencia, por lo general, una mínima carga jurídica en comparación a la ley. Se inclinan a ser sólo simples recomendaciones y no contienen mecanismos limitantes."[50]

Los códigos deontológicos, en cambio, "actúan como complemento de la regulación establecida por el Estado al fijar 'normas que promuevan proactivamente contenidos de gran calidad, lo que no debe confundirse con programas de alta cultura'".[51]

Otros conceptos a considerar son los siguientes:

> "Los códigos deontológicos se han entendido por algunos como la barrera que aleja de nosotros el peligro de la corrupción. Sin embargo, los códigos deontológicos se muestran más bien como una exigencia de la transparencia democrática, como una garantía mínima en la limpieza de los comportamientos, como una objetivación pública de las actuaciones que pueden ser calificadas como éticas".[52]

---

administración pública responsable: Conciliar democracia, eficacia y ética", México D. F., 1999, pág. 98-99. Disponible en línea: http://biblio.juridicas.unam.mx/libros/3/1317/7.pdf

[49] *Ídem.*

[50] *Ídem.*

[51] MIERES MIERES, Luis Javier, *La regulación de los contenidos audiovisuales: ¿Por qué y cómo regular?*, Instituto de Investigaciones Jurídicas, *Derecho a la información y derechos humanos*, Estudios en homenaje al maestro Mario de la Cueva, Universidad Nacional Autónoma de México, México, 2000, pág. 245. Disponible en línea: http://biblio.juridicas.unam.mx/libros/1/7/9.pdf

[52] RODRÍGUEZ ARANA, Jaime, *Ética, Política y Urbanismo*, Instituto de Investigaciones Jurídicas, "Régimen Jurídico del Urbanismo, Memoria del Primer Congreso de Derecho Administrativo

> "Un código deontológico es un conjunto de normas que establece unas pautas de comportamiento dirigido a un colectivo con el fin de guiar y regular su ejercicio profesional desde una perspectiva ética y llevar a la profesión a los niveles más altos de dignidad y prestigio social."[53]

El Poder Judicial de la Federación ha hecho mención de estos códigos en una Tesis aislada:

> CÓDIGO DE ÉTICA DEL PODER JUDICIAL DE LA FEDERACIÓN. SON INATENDIBLES LOS AGRAVIOS EN QUE SE SOSTIENE QUE LOS JUECES DE DISTRITO VIOLENTAN SUS PRINCIPIOS AL CONOCER DE UN JUICIO DE AMPARO.
>
> Del contenido del apartado de presentación del Código de Ética del Poder Judicial de la Federación, se advierte que éste se formula con el objeto de ayudar a los juzgadores federales a resolver los conflictos éticos que se presenten con motivo de su trabajo, señalándose en forma expresa que "será exclusivamente la conciencia de cada uno de ellos, el intérprete y aplicador del código"; además de que los principios, reglas y virtudes que recoge **no tienen como finalidad establecer una responsabilidad de tipo legal** para los miembros del Poder Judicial de la Federación. Asimismo, conforme a lo dispuesto en el Código Iberoamericano de Ética Judicial, el ámbito de la aplicación y obligatoriedad de las diversas codificaciones éticas en Iberoamérica responde a un tratamiento muy diversificado en cada uno de los países que los contempla, existiendo algunos, como el caso de México, en donde se confía la eficacia del código a la conciencia individual de sus destinatarios. Tales postulados llevados al ámbito del juicio de garantías y del recurso de revisión, conducen a concluir que los agravios en los que se plantea que el Juez de Distrito violentó alguno o algunos de los principios recogidos en el Código de Ética del Poder Judicial de la Federación al resolver un juicio de garantías, resultan inatendibles,

Mexicano", Universidad Nacional Autónoma de México, México, 2009, pág. 299 – 300. [Disponible en línea: http://biblio.juridicas.unam.mx/libros/6/2735/13.pdf]

[53] LOBATO PATRICIO, Julia, *Aspectos Deontológicos y Profesionales de la Traducción Jurídica, Jurada y Judicial*, Universidad de Málaga, Departamento de Traducción e Interpretación, Facultad de Filosofía y Letras, Málaga España, 2007, pág. 175. Disponible en línea: http://www.biblioteca.uma.es/bbldoc/tesisuma/17114597.pdf

> pues por una parte los alcances de esas disposiciones no pueden ser materia de examen dentro del juicio de amparo, en la inteligencia de que su aplicación e interpretación queda sólo en el ámbito estrictamente personal y deontológico de los juzgadores federales, sin que constituyan normas legales que rijan para el dictado de los fallos en dicho juicio del orden constitucional; y por otra, porque la aplicación o inaplicación de los principios éticos de independencia, imparcialidad y profesionalismo, entre otros, no puede extenderse al examen de procedencia, legalidad y/o constitucionalidad que habrán de realizar los Jueces de Distrito al resolver los juicios de amparo de su conocimiento y, por ende, tampoco habrán de ser materia de examen en el recurso de revisión que se interponga en contra de las sentencias dictadas por éstos, a fin de calificar su legalidad, pues para ello sólo es dable ceñirse a las disposiciones normativas aplicables al caso concreto, a fin de analizar la litis integrada por las partes en la revisión[54].

Para efectos de unos futuros parámetros en la materia, en este trabajo se consideran códigos deontológicos, todo acuerdo, convenio, contrato o cualquier otro instrumento celebrado por escrito, en el que se establecen **reglas y principios** que tienen como finalidad regular la conducta de los integrantes de una empresa, grupo de empresas u organización, en relación con el tratamiento y la protección de datos personales, de conformidad con la Ley, su Reglamento y las disposiciones aplicables del sector correspondiente.

Código de buenas prácticas profesionales. Al respecto se comenta que "…una ética de 'responsabilidad social empresarial' que se traduce en 'códigos de conducta' o en 'buenas prácticas laborales', asumidos como compromisos voluntarios de respeto a estándares laborales, de los mismos que vienen dando origen a campañas nacionales e internacionales que

[54] Amparo en revisión 97/2010. Maquila Mardi, S.A. de C.V. 2 de junio de 2010. Unanimidad de votos. Ponente: Francisco Javier Cárdenas Ramírez. Secretario: Alejandro Andraca Carrera.

inducen a su cumplimiento y que tienen un significativo impacto positivo en el clima de trabajo."[55]

Un código de ética profesional es el instrumento diseñado para facilitar el cumplimiento y la puesta en práctica del mandato de los Estatutos de determinado gremio de profesionistas en el que se enfatiza la ética como valor central de la profesión y su ejercicio. Su objetivo general es regular el quehacer profesional con acento en la propuesta de criterios de acción y conducta[56].

Para los efectos de los parámetros de los esquemas de autorregulación, consideramos que pueden ser reputados códigos de buena práctica profesional, todo acuerdo, convenio, contrato o cualquier otro instrumento similar celebrado por escrito, adoptados por una asociación profesional en el que se precisan los compromisos que asumen los responsables y encargados para garantizar un adecuado tratamiento y protección de datos personales, de acuerdo con la Ley, su Reglamento, las disposiciones aplicables del sector de que se trate y estos parámetros.

Políticas de privacidad. En el entorno digital, se ha dicho que estas se pueden definir "como aquellas declaraciones que hace el dueño de un sitio de Internet y que, logran explicar el uso que se le da a la información personal que un usuario de dicho sitio proporciona a través del mismo."[57] Es un conjunto de normas propuestas por un portal web, como una red social, y

[55] LÓPEZ GUÍZAR, Guillermo, *La Responsabilidad Social de las empresas y el clima laboral*, Instituto de Investigaciones Jurídicas, "Panorama Internacional de Derecho Social. Culturas y Sistemas Jurídicos Comparados", Universidad Nacional Autónoma de México, México, 2007, pág. 304. Disponible en línea: http://biblio.juridicas.unam.mx/libros/5/2458/18.pdf

[56] Véase el caso del Colegio de Psicólogos de Chile. Disponible en: http://ponce.inter.edu/cai/bv/codigo_de_etica.pdf

[57] Véase política de privacidad sitio Web PREVIRED. Disponible en línea: https://www.previred.com/pdf/politicaprivacidad.pdf

aceptadas explícitamente por cada uno de los usuarios registrados en el sito; y su objetivo base es:

> "… establecer un acuerdo entre el usuario y la página web para garantizar los derechos y las obligaciones de éste. Cada portal web se reserva el derecho de contar con una política de privacidad determinada, pero todos deben respetar unos códigos éticos que defiendan aspectos como la seguridad de los usuarios o la obligación de no enviar datos personales a terceros salvo autorización expresa. Un correcto texto de política de privacidad siempre debe estar al alcance de cualquier usuario de la web y mostrarse de manera detallada y clara. Recuerda siempre leer con detenimiento la política de privacidad de una web antes de aceptar sus normas durante el proceso de registro."[58]

Como aproximación terminológica, en este estudio se consideran políticas de privacidad, las declaraciones unilaterales hechas por un responsable (en el ámbito físico, off line u on line) en las que se explicitan los fines, usos, manejo y obligaciones que éste asume en relación con los datos personales de sus clientes o usuarios, siempre que estos se apeguen a la Ley, el Reglamento, las disposiciones aplicables del sector y estos parámetros.

Reglas de privacidad corporativas. Llamadas por sus siglas en inglés BCR[59] (binding corporate rules)[60], para la empresa Hewlett Packard (HP) las reglas corporativas vinculantes son un marco de cumplimiento de la

[58] Véase al respecto: http://www.nosologeeks.es/2010/04/30/politica-de-privacidad-definicion-seguridad-redes-sociales-facebook-tuenti/

[59] "*What are Binding Corporate Rules designed to achieve? Binding Corporate Rules (BCRs) are designed to allow multinational companies to transfer personal data from the European Economic Area (EEA) to their affiliates located outside of the EEA in compliance with the 8th data protection principle and Article 25 of Directive 95/46/EC. Applicants must demonstrate that their BCRs put in place adequate safeguards for protecting personal data throughout the organisation in line with the requirements of the Article 29 Working Party papers on Binding Corporate Rules"* United Kingndom, Information Commisioner's Office, información disponible en: http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx

[60] También "legally enforceable corporate rules for international data transfers". https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp74_en.pdf

privacidad corporativa constituido por un contrato vinculante, procesos y políticas comerciales, formación y directrices que han sido aprobados por las autoridades de protección de datos de la mayor parte de los estados miembros de la Unión Europea. "*En virtud de esta aprobación, HP puede transferir los datos personales de sus empleados y clientes europeos a otros miembros ("Datos personales de HP") del grupo global de empresas de HP, en cumplimiento de la ley de protección de datos de la UE*".[61]

Para la empresa Baxter por ejemplo, los BCR establecen los mínimos estándares a nivel mundial para la captura, uso y protección de la información de carácter personal. Da cobertura a cualquier información personal que sea capturada, almacenada, procesada, o comunicada en soporte electrónico o en papel, en relación con las operaciones de los negocios de Baxter, tales como informaciones sobre pacientes, profesionales del cuidado de la salud (ej. médicos, farmacéuticos y enfermeras), empleados o terceros asociados de negocios.

Esta Política debe ser implementada y cumplida en todos los negocios, funciones, regiones y compañías subsidiarias de Baxter, incluyendo aquellas localizadas en jurisdicciones en las cuales la protección de la privacidad provista por esta política no sea un requerimiento legal. Debido a que Baxter participa en el programa de Puerto Seguro (Safe Harbor), todas las unidades de negocio de Baxter en Estados Unidos deberán siempre seguir los Principios de Privacidad del Safe Harbor, en el manejo de la información personal, transferida desde la Unión Europea o Suiza hacia los Estados Unidos.

[61] Véase http://www8.hp.com/es/es/binding-corporate-rules.html

Además, esa política corporativa debe ser seguida y cumplida no solo internamente, sino también por todos los agentes de Baxter, personal temporal, proveedores de servicios, contratistas y consultores en su gestión y manejo de la información personal en el nombre de Baxter. El entrenamiento y puesta en conocimiento de esta política para terceros, será gestionada por el responsable de estos últimos[62].

Con la intención de aproximar un concepto que se incluya en los parámetros de los esquemas de autorregulación, se consideran reglas de privacidad corporativas, el conjunto de principios y reglas de carácter interno, adoptados por un grupo de empresas (multinacionales o no) que pertenecen a un mismo grupo económico, las cuales tienen como finalidad definir una política general y vinculante a todas sus filiales dentro y fuera del territorio nacional para garantizar un nivel adecuado de protección de datos personales de acuerdo con la Ley, su Reglamento las disposiciones aplicables del sector correspondiente y estos parámetros.

Sellos de confianza. Con el mismo objetivo conceptual, por sellos de confianza se entienden los mecanismos de autorregulación consistentes en distintivos, marcas u otros similares, cuyo uso es otorgado o licenciado a responsables y encargados de datos personales por un tercero, con el objeto de garantizar frente a los titulares el tratamiento y protección de sus datos personales de conformidad con la Ley, su Reglamento, las disposiciones aplicables del sector correspondiente y estos parámetros, mediantes servicios de verificación, auditoría, revisión o certificación.

[62] Véase Política Corporativa de Baxter, disponible en: http://www.latinoamerica.baxter.com/colombia/information/privacy/baxter_global_data_privacy_policy_spanish_web.pdf

4.3 Parámetros

Por otro lado es importante revisar el concepto de parámetros, para determinar los efectos vinculatorios (vinculantes, jurídicos, obligatorios o de referencia) que tendrían en la esfera jurídica de los particulares que se incorporen a mecanismos de autorregulación.

Esto se debe hacer para evitar que se confundan los parámetros con otras normas de la pirámide jurídica, tales como lineamientos, decretos, acuerdos, directivas, criterios, manuales, metodologías, NOM, reglas de operación, patrones, resoluciones, u otro tipo de normas que derivan de los sistemas de normalización o estandarización.

En general, un **parámetro** es un **dato** que es tomado como **necesario** para analizar o valorar una situación:

> **parámetro.**
>
> (De *para-* y *–́metro*).
>
> **1.** m. Dato o factor que se toma como necesario para analizar o valorar una situación. *Es difícil entender esta situación basándonos en los parámetros habituales.*
>
> **2.** m. *Mat.* Variable que, en una familia de elementos, sirve para identificar cada uno de ellos mediante su valor numérico[63].

Por tanto, una primera aproximación para el concepto de "parámetro" en el ámbito que nos ocupa, sería la siguiente:

> **"Parámetro**: Conjunto de normas, estándares o factores de carácter general determinados por la Secretaría de Economía, en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos, que sirven de referencia para determinar o

[63] Real Academia de la Lengua: http://buscon.rae.es/draeI/SrvltGUIBusUsual

> valorar la pertinencia y correcto desarrollo de los mecanismos y medidas de autorregulación vinculante en materia de protección de datos personales en posesión de particulares adoptados por los responsables y encargados con el fin de complementar lo dispuesto por la Ley Federal de Protección de Datos personales en Posesión de los Particulares, su Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones.
>
> Dichas normas prevén requisitos, reglas o estándares específicos para el correcto desarrollo de códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas, certificación de los responsables en materia de protección de datos personales u otros mecanismos".

Acerca de los efectos jurídicos de un "parámetro" debe señalarse que no figuran expresamente dentro de los actos administrativos de carácter general que prevé la Ley Federal del Procedimiento Administrativo, que a la letra establece:

> **Artículo 4.-** Los actos administrativos de carácter general, tales como reglamentos, decretos, acuerdos, normas oficiales mexicanas, circulares y formatos, así como los lineamientos, criterios, metodologías, instructivos, directivas, reglas, manuales, disposiciones que tengan por objeto establecer obligaciones específicas cuando no existan condiciones de competencia y cualesquiera de naturaleza análoga a los actos anteriores, que expidan las dependencias y organismos descentralizados de la administración pública federal, deberán publicarse en el Diario Oficial de la Federación para que produzcan efectos jurídicos.

Sin embargo, y dado que un parámetro expedido por SE-IFAIPD será general, este numeral abre la posibilidad hermenéutica de inscribirlo en las disposiciones "análogas". Por tanto, deberán publicarse en el Diario Oficial de la Federación.

Por otra parte se debe anticipar que conforme al artículo 69-H de la referida Ley Federal del Procedimiento Administrativo, la autoridad (SE-IFAIPD) deberá presentar su anteproyecto de parámetro a la COFEMER junto con una manifestación de impacto regulatorio (MIR) cuando menos treinta días hábiles antes de la fecha en que se pretenda emitirlo.

Para que se exima la obligación de elaborar la MIR, el anteproyecto de parámetro no debe implicar costos de cumplimiento para los particulares, lo que vemos difícil en algunos casos, pues la elaboración de un código deontológico requiere la contratación de profesionales con cierta experiencia en el mundo del derecho, buenas prácticas, estándares internacionales y privacidad; o bien se requieren hacer erogaciones como pagar una auditoría, una certificación especializada o un sello de confianza.

Para el IFAIPD parece estar claro que ese debe ser el procedimiento, pues ya inscribió ante la COFEMER este tema en su programa regulatorio 2011-2012 con el número 54[64], al lado del asunto de las reglas para el registro de mecanismos de autorregulación:

#	Dependencia	Nombre de la regulación	1er Reporte de Avance
43	IFAI	Reglamento Interior	Ver detalle
44	IFAI	REFORMAS AL REGLAMENTO DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL	
45	IFAI	LINEAMIENTOS PARA EL CUMPLIMIENTO DE OBLIGACIONES DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN GUBERNAMENTAL Y RENDICIÓN DE CUENTAS, INCLUIDA LA ORGANIZACIÓN Y CONSERVACIÓN DE ARCHIVOS RESPECTO DE RECURSOS PÚBLICOS FEDERALES TRANSFERIDOS BAJO CUALQUIER	

64 ANEXO 1. Formato de presentación de programas de mejorar regulatoria 2011-20012 de las dependencias y organismos descentralizados. http://www.cofemer.gob.mx/PMR2011-2012/Default4.aspx?val=17

		ESQUEMA AL PRESIDENTE ELECTO DE LOS ESTADOS UNIDOS MEXICANOS Y A SU EQUIPO DE COLABORADORES, ENTRE EL 2 DE JULIO Y EL 30 DE NOVIEMBRE DE 2012	
46	IFAI	LINEAMIENTOS GENERALES PARA EL ACCESO A INFORMACIÓN GUBERNAMENTAL MEDIANTE CONSULTA DIRECTA	Ver detalle
47	IFAI	LINEAMIENTOS GENERALES PARA LA CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN DE LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL	
48	IFAI	Lineamientos generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal.	
49	IFAI	Lineamientos para la organización y conservación de correos electrónicos institucionales de las dependencias y entidades de la Administración Pública Federal.	
50	IFAI	Lineamientos para el manejo de documentos clasificados.	
51	IFAI	Lineamientos de guarda y custodia de audios y versiones estenográficas.	
52	IFAI	Criterios en materia de seguridad	
53	IFAI	Criterios para medidas compensatorias.	
54	**IFAI**	**Parámetros de Autorregulación**	
55	**IFAI**	**Reglas para el registro de mecanismos de autorregulación.**	
56	IFAI	Expedición de Lineamientos que regulen el tratamiento de los datos personales que se recaban para el control de entrada y salida de visitantes a instalaciones públicas y privadas.	
57	IFAI	Expedición de Lineamientos para regular el tratamiento de los datos personales en el sector financiero.	
58	IFAI	Expedición de Lineamientos para regular el tratamiento de los datos personales en el sector salud.	
59	IFAI	Expedición de Lineamientos para regular el tratamiento de los datos personales en el sector de las telecomunicaciones.	
60	IFAI	Expedición de Lineamientos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.	
61	IFAI	Reformas a los Lineamientos de Protección de Datos Personales.	

4.4 Entorno Digital y Sector de las TI

Aunque el Reglamento de la LFPDPPP define el "entorno digital" (artículo 2 fracción III) con una perspectiva especial para el tema de la privacidad y la protección de datos, encontramos que dentro de ella se "generaliza" sobre cualquier "tecnología de la sociedad de la información" y se dan por hechos conceptos técnicos como hardware, software, etc.

Por lo amplio del concepto, se podría crear confusión si no se alcanza una definición institucional, por ejemplo, sobre qué es "sector de las TI". Dada la trascendencia de este aspecto, se ha considerado necesario proponer una definición de lo que se debe entender por sector de servicios de las TI (industria, empresas, etcétera) para los parámetros, pues se trata del universo o ámbito material del proyecto. Para lo anterior se han compulsado conceptos que pueden ser de utilidad.

a) Concepto del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Según el artículo 2 fracción III del Reglamento, el entorno digital es:

> **Artículo 2.** Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:
>
> **III. Entorno digital**: Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos;

La duda que surge con esta definición es determinar si es lo mismo sector de servicios de las TI y entorno digital, pues como se verá enseguida el sector de las TI abarca otras cuestiones.

b) Definición de las Reglas de Operación de PROSOFT

Estas reglas que se emiten anualmente definen el sector de las TI por el tipo de empresas; y al efecto se citan aquí las del 2010, 2011 y 2012.

PROSOFT 2.0		
2010[65]	**2011**[66]	**2012**[67]
XX. Sector de TI: Conjunto de industrias cuya actividad económica principal consiste en el diseño, desarrollo, producción y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos y administración de información. Este sector incluye la industria de software, servicios relacionados y producción de Medios Interactivos basados en tecnologías de Información;	**3.1.2** Actividades económicas Para efectos del presente Acuerdo se consideran empresas del sector de TI, las que realizan como actividad económica alguna de las siguientes: **a)** Desarrollo de software empaquetado **b)** Desarrollo de software de sistema y herramientas para desarrollo de software aplicativo **c)** Desarrollo de software aplicativo **d)** Servicios de consultoría de software **e)** Servicios de análisis de sistemas computacionales **f)** Servicios de diseño de sistemas computacionales	**Sector de TI:** Conjunto de industrias cuya actividad económica principal consiste en el diseño, desarrollo, producción y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos y administración de información. Este sector incluye el desarrollo de software, servicios de TI, Business Process Outsourcing (BPO) y de medios creativos digitales;

[65] Véase Reglas de Operación para el otorgamiento de apoyos del Programa para el Desarrollo de la Industria del Software (PROSOFT) para el ejercicio fiscal 2010. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5126831&fecha=30/12/2009

[66] Véase Reglas de Operación para el otorgamiento de apoyos del Programa para el Desarrollo de la Industria del Software (PROSOFT) para el ejercicio fiscal 2011. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5182928&fecha=23/03/2011

[67] Véase Reglas de Operación del Programa para el Desarrollo de la Industria del Software (PROSOFT) para el ejercicio fiscal 2012. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5226589&fecha=23/12/2011

PROSOFT 2.0		
2010[65]	**2011**[66]	**2012**[67]
	g) Servicios de programación de sistemas computacionales **h)** Servicios de procesamiento de datos **i)** Servicios de diseño, desarrollo y administración de bases de datos **j)** Servicios de implantación y pruebas de sistemas computacionales **k)** Servicios de integración de sistemas computacionales **l)** Servicios de procesamiento de datos **m)** Servicios de seguridad de sistemas computacionales y procesamiento de datos **n)** Servicios de análisis y gestión de riesgos de sistemas computacionales y procesamiento de datos **o)** Procesos de negocio basados en el uso de sistemas computacionales y comunicaciones **p)** Servicios de valor agregado de análisis, diseño, desarrollo, administración, mantenimiento, pruebas, seguridad, implantación, mantenimiento y soporte de sistemas computacionales, procesamiento de datos y procesos de negocio **q)** Servicios de capacitación, consultoría y evaluación para el mejoramiento de la capacidad humana, aseguramiento de la calidad y de procesos de las empresas del Sector de TI **r)** Servicios de administración de procesos de negocio basados en	

PROSOFT 2.0		
2010[65]	**2011**[66]	**2012**[67]
	tecnologías de información que incluyen entre otros centros de llamado, centros de contacto, administración de nóminas, carteras, cobranza, líneas de producción, entre otros **s)** Desarrollo de software embebido (embedded software) **t)** Medios interactivos basados en tecnologías de información: **i.** Desarrollo o creación de entretenimiento interactivo **ii.** Servicios especializados de diseño **iii.** Animación **iv.** Tecnologías de compresión digital **v.** Efectos visuales **vi.** Televisión interactiva, y **u)** Cualquiera otra tecnología que el Consejo Directivo determine. **3.2.** Población objetivo **a)** Las personas físicas con actividad empresarial o las personas morales del sector de TI; **b)** Los organismos, agrupamientos empresariales, empresas integradoras y asociaciones civiles, y la cámara del sector de TI; **c)** Las instituciones académicas y los emprendedores de este sector económico; **d)** Los organismos públicos, privados o mixtos sin fines de lucro entre cuyos objetivos se encuentre el desarrollo del sector de TI, y **e)** Los usuarios de TI siempre y cuando contraten	

PROSOFT 2.0		
2010[65]	**2011**[66]	**2012**[67]
	productos y/o servicios de empresas del sector de TI basadas en el país conforme a lo previsto en el numeral 3.5.5.1.	

Como se puede observar, en tres años ha variado el concepto de sector de TI para los efectos de PROSOFT, el cual debe valorar la aplicabilidad de nuevas definiciones con visión de largo aliento.

c) Definiciones del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones[68]

Este documento de la Secretaría de la Función Pública (SFP), da algunas definiciones interesantes:

> **Activo de TIC:** La información, base de datos, programa de cómputo, bien informático físico, solución tecnológica, sistema o aplicativo, relacionados con el tratamiento de la misma; que tengan valor para la Institución.
>
> **Infraestructura de TIC:** El hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar los servicios de TIC. El término infraestructura de TIC incluye todas las TIC pero no las personas, procesos y documentación asociados.
>
> **Recursos de TIC:** La infraestructura, activos, personal especializado, presupuesto y cualquier otro elemento de TIC.

[68] Véase Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y comunicaciones. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5151475&fecha=13/07/2010

Servicios: Actividades que desarrollan o coordinan las UTIC encaminadas a la satisfacción de las necesidades que en materia de TIC requieren las unidades responsables.

Sistema o aplicativo: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Software de código abierto: El software cuya licencia asegura que el código pueda ser modificado y mejorado por cualquier persona o grupo de personas con las habilidades correctas, el conocimiento es de dominio público.

d) Definiciones de PROMEXICO

Para esta institución creada en el año 2007 como Fideicomiso Público del Gobierno Federal, los rubros que se consideran en este sector[69] son:

Software. Empresas especializadas en el diseño, producción e ingeniería de programas informáticos.

Servicios de TI. Empresas dedicadas a la provisión de servicios en capacitación, mantenimiento, operación y soporte de los programas.

e) Conceptos de la Agenda Digital Nacional[70]

Este instrumento presentado por la Secretaría de Comunicaciones y Transportes en 2012, define las TIC de la manera siguiente:

Tecnologías de la Información y Comunicación (TIC): Medios de información y canales de comunicación integrados en una misma herramienta tecnológica que permiten una comunicación interactiva, capaz de generar información y compartir conocimiento.

[69] Véase Servicios de TI y Software en PROMEXICO. Disponible en: http://www.promexico.gob.mx/es_us/promexico/IT_and_Software_Services
[70] Véase http://www.agendadigital.mx/

f) Propuesta de definición

Lo primero que se tiene que concretar en el momento del ejercicio de las facultades regulatorias (o paramétricas) es si el sector de las TI es un conjunto de industrias, un grupo de actividades económicas o un tipo de empresas.

Al respecto nos parece apropiado que se les considere como un conjunto de industrias y/o empresas cuya actividad económica principal consiste en el diseño, desarrollo, producción, explotación, mantenimiento y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos, custodia y administración de información.

Pero para que esta definición sea más completa debe considerar además elementos de las Reglas de Operación de PROSOFT 2012, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de la Agenda Digital Nacional, etc., con una frase que abarque el desarrollo del software y hardware, los servicios de TI, Business Process Outsourcing (BPO), los medios creativos digitales, redes, aplicaciones o cualquier otra tecnología de la información que permiten el intercambio, custodia y/o procesamiento informatizado o por medios físicos de datos.

Por lo anterior, una definición comprehensiva sería la siguiente:

> **“Sector de las TI:** Conjunto de industrias y/o empresas cuya actividad económica principal consiste en el diseño, desarrollo, producción, explotación, mantenimiento y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos, custodia y administración de información, así como aquellas unidades económicas vinculadas al desarrollo del software y hardware, los

> servicios de TI, Business Process Outsourcing (BPO), los medios creativos digitales, redes, aplicaciones o cualquier otra tecnología de la información que permiten el intercambio, almacenamiento y/o procesamiento informatizado o por medios físicos de datos."

Un vocabulario que sirva de proemio a los parámetros, más allá del concepto de TI, deberá incluir también, definiciones *ad hoc* sobre cuestiones previstas en el Reglamento de la LFPDPPP:

- hardware,
- software,
- redes,
- aplicaciones,
- servicios o cualquier otra tecnología de la sociedad de la información intercambio o procesamiento informatizado o digitalizado de datos,
- etcétera[71].

4.5 Acreditación y Certificación

Otras nociones relevantes que deben definirse para crear un parámetro más o menos legible e interpretativo de la LFPDPPP son las que derivan de las siguientes disposiciones del Reglamento:

> **Certificación en protección de datos personales**
> **Artículo 83**. Los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales.

[71] Ver glosario de la Asociación Mexicana de Internet, A.C. (AMIPCI) en http://www.glosariodigital.com/etiquetas/amipci/

> En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley.
>
> **Personas físicas o morales acreditadas**
> **Artículo 84.** Las personas físicas o morales acreditadas como certificadoras tendrán la función principal de certificar que las políticas, programas y procedimientos de privacidad instrumentados por los responsables que de manera voluntaria se sometan a su actuación, aseguren el debido tratamiento y que las medidas de seguridad adoptadas son las adecuadas para su protección. Para ello, los certificadores podrán valerse de mecanismos como verificaciones y auditorías.
>
> El procedimiento de acreditación de los certificadores a los que refiere el párrafo anterior, se llevará a cabo de acuerdo con los parámetros que prevé el artículo 43, fracción V de Ley. Estos certificadores deberán garantizar la independencia e imparcialidad para el otorgamiento de certificados, así como el cumplimiento de los requisitos y criterios que se establezcan en los parámetros en mención.

Por el momento, una primera fuente hermenéutica para determinar el alcance de estos conceptos es la Ley Federal sobre Metrología y Normalización, publicada en el Diario Oficial de la Federación el 1 de julio de 1992, que en las fracciones I y III de su artículo 3 los define del modo siguiente:

> **ARTÍCULO 3o.-** Para los efectos de esta Ley, se entenderá por:
>
> **I. Acreditación**: el acto por el cual una entidad de acreditación reconoce la competencia técnica y confiabilidad de los organismos de certificación, de los laboratorios de prueba, de los laboratorios de calibración y de las unidades de verificación para la evaluación de la conformidad;
>
> **III. Certificación:** procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o

> lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales;

Se trata de dos conceptos que forman parte de la llamada **Evaluación de la Conformidad,** que –conforme a la misma ley citada- consiste en la determinación del grado de cumplimiento con las normas oficiales mexicanas o la conformidad con las normas mexicanas, las normas internacionales u otras especificaciones, prescripciones o características. Comprende, entre otros, los procedimientos de muestreo, prueba, calibración, certificación y verificación.

Finalmente cabe citar a la Entidad Mexicana de Acreditación, A.C. (EMA) que, en el apartado de "preguntas frecuentes" de su portal web [72], apunta lo siguiente:

> ***¿Diferencia entre acreditación y certificación?***
> *La acreditación es el reconocimiento formal y público por un organismo imparcial y de tercera parte, en este caso la EMA, de la competencia técnica y confiabilidad, de esta forma el Organismo de la Evaluación de la Conformidad recibe un reconocimiento del trabajo realizado correctamente y de acuerdo a una norma apropiada y reconocida internacionalmente. A diferencia la certificación es la confirmación de que una organización ha establecido un sistema de gestión de la calidad conforme con ciertos requisitos.*

Considerando el régimen voluntario de los esquemas de autorregulación, se recomienda analizar la posibilidad de que la acreditación y certificación a que se refiere el citado artículo 83 del Reglamento de la LFPDPPP, se describa en los parámetros en un entorno más flexible que el previsto en la Ley Federal sobre Metrología y Normalización.

[72] Véase al respecto: http://www.ema.org.mx/ema/ema/index.php?option=com_content&task=blogcategory&id=85&Itemid=109

V.- MODELOS NORMATIVOS

De lo investigado hasta el momento se observa que existen -al menos- tres modelos normativos que los diferentes países han adoptado en relación con el tratamiento de datos personales y los mecanismos o esquemas de autorregulación. Se trata de los sistemas de heterorregulación, autorregulación pura y autorregulación mixta.

Cabe aclarar que la práctica no es homogénea, y cada uno de los modelos aquí comentados puede tener a su vez matices o gradualidades. La idea es exponer una visión general sobre las tendencias actuales en materia de autorregulación a fin de abordar los mecanismos en concreto.

5.1 Modelos existentes en México

Primeramente se destaca en este apartado el hecho de que el 22 de Febrero del presente año 2012, la Misión Permanente de México ante la Organización de los Estados Americanos (OEA) envió a la Secretaría de la Comisión de Asuntos Jurídicos y Políticos del Consejo Permanente y al Departamento de Derecho Internacional de la OEA las respuestas a un cuestionario sobre legislación y prácticas de privacidad y protección de datos "para recabar insumos que contribuyan al cumplimiento de los mandatos contemplados en la Resolución AG/RES. 2661 (XLI-O11) del 6 de Octubre de 2011" con el propósito de: (1) que el Departamento de Derecho Internacional elabore un estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, inclusive las leyes, reglamentos y autorregulación nacionales, con miras a explorar la posibilidad de un marco regional en esta área y (2) que el Comité Jurídico Interamericano presente, antes del

cuadragésimo segundo período ordinario de sesiones de la Asamblea General, un documento de principios de privacidad y protección de datos personales en las Américas[73].

En materia de autorregulación, México contestó lo siguiente:

D. ¿Existen en su país códigos de conducta de autocontrol u otros sistemas semejantes de responsabilidad por la privacidad y la protección de datos? En caso afirmativo describa brevemente estos sistemas y adjunte copia de las disposiciones y documentos pertinentes que describan su operación.

El artículo 44 de la LFPDPPP prevé que las personas físicas o morales puedan convenir entre ellas o con organizaciones civiles o gubernamentales esquemas de autorregulación vinculante en la materia, los cuales

6

deben notificarse al IFAI a efecto de que lleve el registro correspondiente, de acuerdo con el artículo 86 del Reglamento de la LFPDPPP.

Aún no se encuentra inscrito ningún mecanismo de autorregulación en el registro que administrará el IFAI, debido a que el mismo será instrumentado próximamente. Sin embargo, se tiene conocimiento de que existen empresas privadas que cuentan actualmente con esquemas de autorregulación que incorporan disposiciones en materia de protección de datos personales y privacidad. A continuación se mencionan algunos ejemplos, no sin antes aclarar que en la elaboración y revisión de los mismos el IFAI no ha participado en modo alguno ni ha emitido ningún tipo de validación al respecto.

- **Asociación Mexicana de Internet (AMIPCI)**

La AMIPCI, institución privada que integra a empresas de la industria de internet en México, otorga un sello electrónico de confianza que reconoce a los negocios o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidos.

La empresa que lo obtenga se compromete a acatar lo dispuesto por la normativa de privacidad y de protección de datos personales aplicable, así como lo previsto en el Código de Ética de la AMIPCI y el contrato que los poseedores del sello de confianza firmaron con esa asociación.[10]

Por otra parte, el Código de Ética de AMPICI establece, en su artículo 1, normas mínimas de conducta que deben seguir los asociados. Su capítulo VI versa sobre las obligaciones de los asociados para la protección de la privacidad de la información. En particular, el artículo 22 establece que los asociados tienen que cumplir con las normas orientadas hacia la privacidad de los usuarios en línea, por lo cual deben adoptar políticas que se adapten a los estándares de la AMIPCI, en las que se prevean los siguientes aspectos: puesta en práctica de una política de privacidad, avisos y divulgación, opciones y consentimiento, calidad de los datos, y limitaciones de uso y seguridad. Este Código de Ética también establece, en su Título III, la imposición de sanciones para cualquier asociado que incumpla con esta norma.[11]

[73] CUESTIONARIO DE LEGISLACIÓN Y PRÁCTICAS SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS**1/** [AG/RES. 2661 (XLI-O/11)](Documento presentado conforme a lo acordado en la reunión de la Comisión de Asuntos Jurídicos y Políticos del 6 de octubre de 2011).

- **Grupo Financiero Banco Bilbao Vizcaya Argentaria, S.A. Bancomer (BBVA Bancomer)**

Esta institución tiene un Código de Ética[12] que, en materia de protección de datos personales y privacidad, contiene un conjunto de normas y procedimientos específicos que han sido adoptados por las entidades del grupo, con la finalidad de proteger y asegurar el tratamiento apropiado de la información de carácter personal que, como consecuencia del desarrollo de sus actividades empresariales, obtienen de sus clientes, accionistas, empleados y administradores, o de cualquier otra persona física con la que se relacionan. El Código establece, entre otras, las siguientes responsabilidades para la institución y sus empleados:

- ✓ Conocer y observar las normas y procedimientos internos que resulten de aplicación en materia de seguridad de la información y de protección de datos de carácter personal.
- ✓ Aplicar medidas adecuadas para evitar el acceso indebido a tal información.
- ✓ Los empleados que, por razón de su cargo o de su actividad, dispongan de datos o tengan acceso a datos personales son responsables últimos de su custodia y apropiado uso.

[10] En particular, el sello de confianza de AMIPCI promueve el cumplimiento de los siguientes documentos: LFPDPPP y su Reglamento, Ley Federal de Protección al Consumidor, Código de Ética de AMIPCI y Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC).
[11] La información sobre la AMIPCI fue obtenida de su propia página electrónica, en las siguientes direcciones:
http://www.amipci.org.mx/somos
http://www.sellosdeconfianza.org.mx/
http://www.sellosdeconfianza.org.mx/etica.php
[12] Disponible en: http://www.segurosbancomer.com.mx/seguros/pdf/CodigoDeConducta_ManualDePol%C3%ACticas.pdf

7

- **Código de Conducta del Grupo Novartis[13]**

El Grupo Novartis está conformado por empresas que desarrollan productos farmacéuticos.[14] Este grupo cuenta con un Código de Ética que en uno de sus puntos señala que sus empresas: respetan el derecho a la privacidad de sus empleados, pacientes, médicos y otros grupos de interés; están obligadas a informar a las personas de la recogida y el tratamiento de sus datos personales; y recogen y procesan datos personales con fines comerciales legítimos y concretos, además de que protegen dichos datos de accesos no autorizados.

Si bien es escasa la experiencia mexicana en materia de autorregulación en el ámbito de la protección de datos y que el Gobierno Mexicano solo reconoce los enunciados en el informe entregado en Washington, D.C. el 8 de febrero del 2012, consideramos que es importante mencionar otros casos de autorregulación vinculante (reglada o mixta) que ya operan en México, específicamente para el ámbito financiero o bancario.

Tal es el caso del modelo previsto en la Ley de Instituciones de Crédito, cuyo artículo 3 establece que el Sistema Bancario Mexicano estará integrado por el Banco de México, las instituciones de banca múltiple, las instituciones de banca de desarrollo y los fideicomisos públicos constituidos por el Gobierno Federal para el fomento económico que realicen actividades financieras, así como los "organismos auto regulatorios bancarios".

Conforme a la misma Ley, dichos organismos tienen como objeto preestablecido e implementar estándares de conducta de sus agremiados:

> **Artículo 7 Bis.-** Los organismos autorregulatorios bancarios tendrán por objeto implementar estándares de conducta y operación entre sus agremiados, a fin de contribuir al sano desarrollo de las instituciones de crédito. Dichos organismos podrán ser de diverso tipo acorde con las actividades que realicen.
>
> Tendrán el carácter de organismos autorregulatorios bancarios las asociaciones o sociedades gremiales de instituciones de crédito que, a solicitud de aquellas, sean reconocidas con tal carácter por la Comisión Nacional Bancaria y de Valores, previo acuerdo de su Junta de Gobierno[74].

Estos organismos pueden además realizar una serie de funciones que pueden ser tomadas como referencia en el ámbito de la protección de datos personales:

> **Artículo 7 Bis 1**.- Los organismos autorregulatorios bancarios podrán, en términos de sus estatutos y sujetándose a lo previsto en el artículo 7 Bis 2 de esta Ley, emitir normas relativas a:
>
> I. Los requisitos de ingreso, exclusión y separación de sus agremiados;
> II. Las políticas y lineamientos que deban seguir sus agremiados en la contratación con la clientela a la cual presten sus servicios;

[74] Artículo adicionado DOF 01-02-2008

III. La revelación al público de información distinta o adicional a la que derive de esta Ley;
IV. Las políticas y lineamientos de conducta tendientes a que sus agremiados y otras personas vinculadas a éstos con motivo de un empleo, cargo o comisión en ellos, conozcan y se apeguen a la normativa aplicable, así como a los sanos usos y prácticas bancarias;
V. Los requisitos de calidad técnica, honorabilidad e historial crediticio satisfactorio aplicables al personal de sus agremiados;
VI. La procuración de la eficiencia y transparencia en las actividades bancarias;
VII. El proceso para la adopción de normas y la verificación de su cumplimiento;
VIII. Las medidas disciplinarias y correctivas que se aplicarán a sus agremiados en caso de incumplimiento, así como el procedimiento para hacerlas efectivas; y
IX. Los usos y prácticas bancarias.

Además, las asociaciones o sociedades gremiales de instituciones de crédito que obtengan el reconocimiento de organismo autorregulatorio bancario por parte de la Comisión Nacional Bancaria y de Valores podrán llevar a cabo certificaciones de capacidad técnica de empleados, funcionarios y directivos de las instituciones de crédito, así como de sus apoderados, cuando así lo prevean las normas a que se refiere este artículo.

Los organismos autorregulatorios bancarios deberán llevar a cabo evaluaciones periódicas a sus agremiados, sobre el cumplimiento de las normas que expidan dichos organismos para el otorgamiento de las certificaciones a que se refiere el párrafo anterior. Cuando de los resultados de dichas evaluaciones puedan derivar infracciones administrativas o delitos, a juicio del organismo de que se trate, éste deberá informar de ello a la Comisión Nacional Bancaria y de Valores, sin perjuicio de las facultades de supervisión que corresponda ejercer a la propia Comisión. Asimismo, dichos organismos deberán llevar un registro de las medidas correctivas y disciplinarias que apliquen a las personas certificadas por ellos, el cual estará a disposición de la propia Comisión.

Las normas autorregulatorias que se expidan en términos de lo previsto en este artículo no podrán contravenir o exceptuar lo establecido en la presente Ley y demás disposiciones aplicables.

> **Artículo 7 Bis 2.-** La Comisión Nacional Bancaria y de Valores expedirá disposiciones de carácter general en las que establezca los requisitos que deberán cumplir las asociaciones o sociedades gremiales de instituciones de crédito para obtener, acorde con su tipo, el reconocimiento de organismo autorregulatorio a que se refiere el artículo 7 Bis de esta Ley, así como para regular su funcionamiento.
>
> Las referidas disposiciones de carácter general preverán requisitos relacionados con la organización y funcionamiento interno de las asociaciones y sociedades gremiales que quieran ser reconocidos como organismos de autorregulación, a fin de propiciar que sus órganos sociales se integren en forma equitativa, por personas con honorabilidad y capacidad técnica, se conduzcan con independencia y cuenten con la representativa del gremio para el ejercicio de sus actividades, así como cualquier otro que contribuya a su sano desarrollo.

Por otro lado, el artículo 230 de la Ley del Mercado de Valores establece que la Comisión Nacional Bancaria y de Valores (CNBV) podrá expedir *disposiciones* de carácter general en las que establezca los requisitos que deberán cumplir los organismos autorregulatorios para obtener el reconocimiento a que se refiere el artículo 228 de dicha Ley, así como para regular su funcionamiento.

En ejercicio de esa facultad la CNBV emitió en 2006 las "Disposiciones generales aplicables a los organismos autorregulatorios del mercado de valores reconocidos por la Comisión Nacional Bancaria y de Valores"[75], que entre otras cuestiones disponen:

> **Articulo 5.-** Las Asociaciones que obtengan el reconocimiento para actuar como organismo autorregulatorio del mercado de valores, cuando así lo soliciten a la Comisión Nacional Bancaria y de Valores, podrán certificar la capacidad técnica de las personas físicas que pretendan actuar como operadores de bolsa o apoderados de intermediarios del mercado de valores y Asesores de Inversión para la

75 Publicada en el Diario Oficial de la Federación el 27 de junio de 2002, actualizada con las modificaciones publicadas en el propio Diario el 16 de junio de 2006.

celebración de operaciones con el público, mediante la aplicación de exámenes, o bien, tratándose de personas que cuenten con al menos veinticinco años de experiencia en el sistema financiero, mediante cualquier otro procedimiento de acreditación que al efecto determinen las Asociaciones, siempre que sea adecuado para demostrar la capacidad técnica.

Asimismo, las Asociaciones citadas que reciban autorización para realizar la actividad a que se refiere el párrafo anterior, deberán verificar el historial crediticio y honorabilidad de los aspirantes que pretendan actuar con el carácter de operadores de bolsa o apoderados de intermediarios del mercado de valores y Asesores de Inversión para la celebración de operaciones con el público.

La Ley de Ahorro y Crédito Popular establece asimismo que los organismos autorregulatorios de las Sociedades Financieras Populares tendrán por objeto implementar estándares de conducta y operación entre sus agremiados, a fin de contribuir al sano desarrollo de las Sociedades Financieras Populares. Dichos organismos podrán ser de diverso tipo acorde con las actividades que realicen (art. 113).

Señala dicho ordenamiento que tendrán el carácter de organismos autorregulatorios de las Sociedades Financieras Populares las asociaciones o sociedades gremiales de Sociedades Financieras Populares que, a solicitud de aquellas, sean reconocidas con tal carácter por la Comisión, previo acuerdo de su Junta de Gobierno.

Artículo 114. Los organismos autorregulatorios de las Sociedades Financieras Populares podrán, en términos de sus estatutos y sujetándose a lo previsto en el Artículo 115 de esta Ley, emitir normas relativas a:

I. Los requisitos de ingreso, exclusión y separación de sus agremiados;
II. Las políticas y lineamientos que deban seguir sus agremiados en la contratación con los Clientes a los cuales presten sus servicios;

III. La revelación al público de información distinta o adicional a la que derive de esta Ley;
IV. Las políticas y lineamientos de conducta tendientes a que sus agremiados y otras personas vinculadas a éstos con motivo de un empleo, cargo o comisión en ellos, conozcan y se apeguen a la normativa aplicable, así como a los sanos usos y prácticas imperantes entre las Sociedades Financieras Populares;
V. Los requisitos de calidad técnica, honorabilidad e historial crediticio satisfactorio aplicables al personal de sus agremiados;
VI. La procuración de la eficiencia y transparencia en las actividades de las Sociedades Financieras Populares;
VII. El proceso para la adopción de normas y la verificación de su cumplimiento;
VIII. Las medidas disciplinarias y correctivas que se aplicarán a sus agremiados en caso de incumplimiento, así como el procedimiento para hacerlas efectivas; y
IX. Los usos y prácticas mercantiles imperantes entre las Sociedades Financieras Populares.
X. Además, las asociaciones o sociedades gremiales de Sociedades Financieras Populares que obtengan el reconocimiento de organismo autorregulatorio por parte de la Comisión podrán llevar a cabo certificaciones de capacidad técnica de empleados, funcionarios y directivos de las Sociedades Financieras Populares, así como de sus apoderados, cuando así lo prevean las normas a que se refiere este Artículo.

Los organismos autorregulatorios de las Sociedades Financieras Populares deberán llevar a cabo evaluaciones periódicas a sus agremiados, sobre el cumplimiento de las normas que expidan dichos organismos para el otorgamiento de las certificaciones a que se refiere el párrafo anterior. Cuando de los resultados de dichas evaluaciones puedan derivar infracciones administrativas o delitos, a juicio del organismo de que se trate, éste deberá informar de ello a la Comisión, sin perjuicio de las facultades de supervisión que corresponda ejercer a la propia Comisión. Asimismo, dichos organismos deberán llevar un registro de las medidas correctivas y disciplinarias que apliquen a las personas certificadas por ellos, el cual estará a disposición de la propia Comisión.

Las normas autorregulatorias que se expidan en términos de lo previsto en este Artículo no podrán contravenir o exceptuar lo establecido en la presente Ley y demás disposiciones aplicables.

La Ley señalada establece que la Comisión expedirá disposiciones de carácter general en las que establezca los requisitos que deberán cumplir las asociaciones o sociedades gremiales de Sociedades Financieras Populares para obtener, acorde con su tipo, el reconocimiento de organismo autorregulatorio, así como para regular su funcionamiento.

Y se agrega que las referidas disposiciones de carácter general preverán requisitos relacionados con la organización y funcionamiento interno de las asociaciones y sociedades gremiales que quieran ser reconocidos como organismos de autorregulación, a fin de propiciar que sus órganos sociales se integren en forma equitativa, por personas con honorabilidad y capacidad técnica, se conduzcan con independencia y cuenten con la representativa del gremio para el ejercicio de sus actividades, así como cualquier otro que contribuya a su sano desarrollo.

5.2 Códigos Privados

No se debe soslayar la existencia de varios códigos de conducta y esquemas de autorregulación en el ámbito de la publicidad y el comercio que han adoptado varios sectores, algunos como BCRs, pero dada su naturaleza privada no encuadran en un sistema vinculante como el que se ha escogido para la privacidad en nuestro país. Sin embargo, la estructura y contenido de esos códigos pueden ser útiles para la industria referencia modo de referencia, como es el caso del Código PABI (Código de Autorregulación de Publicidad de Alimentos y Bebidas no Alcohólicas dirigida al público infantil impulsado por el Consejo de Autorregulación y Ética Publicitaria (*CONAR*), el cual reporta que tiene un cumplimiento del 90%[76]; y otros códigos de privacidad impulsados por empresas multinacionales.

[76] Véase: http://www.e-consulta.com/blogs/educacion/imgs_10/codigo_pabi.pdf

VI.- HETERORREGULACIÓN

Como primer grupo de estudio, se observa que existen los países que cuentan con una legislación sobre protección de datos personales, pero que no incluyen modelos de autorregulación (*modelo de heterorregulación*).

Este modelo se centra en reglamentar la actividad de las autoridades públicas y los particulares respecto del tratamiento de los datos de carácter personal. Generalmente contemplan entidades de naturaleza administrativa encargadas de velar por el cumplimiento de la normativa, con facultades de fiscalización y sanción[77]. Ejemplos de este tipo de modelo son Nueva Zelanda e Italia.

Aunque hay países, como Estados Unidos, donde opera la autorregulación pura (no vinculante), es decir, sin intervención de la autoridad, existe heterorregulación de protección de datos personales en posesión de particulares en materia de telecomunicaciones e información genética en el ámbito laboral. Además por su carácter federal existen diversas leyes locales que eventualmente abordan la temática.

Como dato histórico, cabe mencionar que en Suecia se adoptó la primera Ley de Datos por la cual se impuso un sistema de registro abierto para publicar bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar por la autoridad pública. Además, previó una autoridad de control, la Inspección de Datos, velaba por el respeto a la ley, con facultades

[77] Cerda Silva, Alberto, *"Hacia un modelo integrado de regulación y control en la protección de datos personales"*, Revista Derecho y Humanidades, No. 13, Universidad de Chile, 2008, p. 122.

inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones[78].

Ahora bien, un caso de autorregulación que se puede considerar prácticamente heterorregulatorio es el modelo canadiense, que no podría ubicarse en los casos integrados o mixtos por lo que se explica a continuación.

6.1 Canadá

De acuerdo con su Constitución Política, Canadá (oficialmente *Constitution Act*) es desde 1867 un Estado Federal integrado en la Commonwealth británica bajo la forma de Monarquía Parlamentaria[79]. La cabeza de Estado es la Reina Isabel II de Inglaterra, representada desde octubre de 2010 por el Gobernador General, David Johnston.

Canadá está formada por diez colonias: Quebec, Nueva Brunswick, Nueva Escocia, Manitoba, Columbia Británica, Isla del Príncipe Eduardo, Alberta, Saskatchewan, Terranova y Ontario. En esta última se encuentra Ottawa, la capital del país.

6.1.1 Privacy Act 1985

Con la finalidad de regular de forma más específica la protección de datos personales, en el año de 1985 el Parlamento de Canadá aprobó la Privacy Act.[80]

[78] *Ibídem*.
79 Véase Constitution Act de 1867.
80 Véase preámbulo de la Privacy Act de 1985.

Esta Ley tiene por objeto regular la protección de la información personal en posesión del sector público, así como garantizar el acceso a dicha información. Para ello creó la figura del Comisionado de Privacidad y estableció principios para la protección de los datos personales basados en los lineamientos de la OCDE.[81]

6.1.2 Personal Information and Electronic Documents Act (PIPEDA), 2000

El 13 de abril del año 2000 el Parlamento de Canadá aprobó la Personal Information and Electronic Documents Act[82], regulación de gran importancia que tiene como propósito normar de forma más específica las obligaciones del sector privado con relación a la protección de datos personales, siendo así que establece obligaciones a las *organizaciones*[83] con la finalidad de impulsar el desarrollo del comercio electrónico con el pleno respeto a la privacidad. La Privacy Commissioner es la autoridad encargada de implementar la PIPEDA, así como de la Privacy Act.

En esta ley se establecen las obligaciones que los particulares deben cumplir en la obtención, uso, tratamiento y revelación, y los términos en los que se realizará el acceso a los datos personales de particulares, con la particularidad referente a las personas con una discapacidad, imponiendo a

81 Véase Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OCDE

82 Véase preámbulo de la Personal Information and Electronic Documents Act

83 De acuerdo con la propia Ley, una *organización* incluye una asociación, sociedad, persona o sindicato. Véase el apartado de definiciones de la Personal Information and Electronic Documents Act. De acuerdo a la información vertida por la Oficina del Comisionado de Privacidad en Canadá, la ley fue aplicada en una primera etapa a obras federales (federal work) empresas o negocios (bancos, compañías de telecomunicaciones, líneas aéreas), así como información relativa a los registros de empleados de las empresas o negocios; en una segunda etapa se aplico a los datos personales relacionados con la salud y, en una tercera etapa a la recolección, uso y divulgación de información personal en actividades comerciales. Véase An Overview Personal Information and Electronic Documents Act, Office of the Privacy Commissioner of Canada

la organización la obligación de contar con formatos alternativos para dichas personas.

Conforme a la ley se otorga a los particulares el derecho a consentir la recolección de sus datos, la finalidad con la que son recabados, el uso que se haga de estos y saber qué datos personales posee una organización acerca de ellos, así como a corregir dicha información en caso de ser incorrecta.

Es importante destacar que la Ley recoge los principios que fueron establecidos en el Código Modelo para la Protección de Datos Personales (Model Privacy Code for the Protection of Personal Information), de la Asociación Canadiense de Estándares (Canadian Standards Association's), en el que intervinieron diversos actores interesados en la protección de los datos personales.

Es oportuno señalar que PIPEDA no se aplica en las provincias de Quebec[84], Columbia Británica[85] y Alberta[86], en razón de que dichas provincias cuentan con regulación que ha sido declarada "sustancialmente parecida"[87]. Ontario[88] cuenta con una legislación específica para la protección de datos personales relacionados con la salud, que se encuentre en posesión de empresas, profesionales, proveedores y en general servicios de salud. Las normas de estas provincias debe cumplir con los 10 principios que se establecen tanto en la PIPEDA como en el código modelo de protección de datos personales.

84 Véase *An Act Respesting the Protection of Personal Information in the Private Sector*
85 Véase *Personal Information Protection Act*
86 *Ídem*
87 Véase *Process for the Determination for "Substantially Similar" Provincial Legislation by the Governor in Council*, publicado en el Diario Oficial de Canadá el 03 de agosto de 2002.
88 Véase *Personal Health Infomation Protection Act, 2004*

6.1.3 Código Modelo de Privacidad

La Personal Information and Electronic Documents Act, señala que el Comisionado deberá alentar a las organizaciones o empresas a desarrollar políticas y prácticas así como códigos de protección de datos personales, es por ellos que en su Anexo 1 incluye un Código Modelo para la Protección de Datos Personales conforme a los principios establecidos por los estándares nacionales. Es así que la ley permite a las organizaciones crear y operar sus propios Códigos de Protección de Datos Personales (*Code for the Protection of Personal Information*), con los mínimos señalados en el código modelo.

La Ley establece que el Código debe contener los siguientes principios: a) Responsabilidad *(Accountability), b)* Finalidad *(Identifying Purposes), c)* Consentimiento *(Consent), d)* Proporcionalidad *(Limiting Collection), e)* Uso, divulgación y retención *(Limiting Use, Disclosure and Retention), f)* Exactitud Precisión *(Accuracy), g)* Medidas de Seguridad *(Safeguards), h)* Información *(Opnness), i)* Acceso *(Individual Access) y j)* Atención de quejas *(*Challenging)[89]. Señalando cuales obligaciones podrán adecuarse a las excepciones que se establecen a lo largo de la ley.

6.1.4 Lineamientos relativos a PIPEDA

El Privacy Commissioner of Canada conforme a los establecido por la *Personal Information Protection and Electronic Documents Act,* está facultado para emitir y establecer programas de información que permitan a los particulares que recopilan y tratan datos personales cumplir con las obligaciones establecidas en la Ley.

[89] Estos principios corresponden a las obligaciones de: 1) responsabilidad 2) finalidad 3) consentimiento 4) proporcionalidad 5) uso, divulgación y retención 6) precisión 7) seguridad 8) información 9) acceso 10) challenging. *Cfr. Anexo 1,* Model Privacy Code for the Protecction of Personal Information de PIPEDA.

Con base en lo anterior, el Comisionado de Privacidad publicó las siguientes directrices o *guidelines:*

Privacy and Online Behavioural Advertising, Diciembre, 2011. Los lineamientos fueron emitidos con el objetivo de asegurar que las prácticas de empresas dedicadas a la publicidad dirigida en línea para que sean equitativas, transparentes y conforme a lo establecido por PIPEDA. Entre los aspectos que pretende aclarar es en torno a la obtención del consentimiento en línea. Por lo que en caso de datos personales menos sensibles el consentimiento tácito (opt-out) se considerará siempre y cuando:

- Las empresas empleen mecanismos para tener informados a los individuos (por ejemplo banners).
- La información sea puesta a disposición del individuo antes de la recolección.
- El usuario tenga una forma fácil de decidir sobre el tratamiento de sus datos.
- Cuando el individuo no otorgue su consentimiento éste surte efectos inmediatamente.
- En la medida de lo posible se debe evitar la recolección de datos personales sensibles o confidenciales (ejemplo: información médica).
- La destrucción inmediata de la información personal o su disociación.

Las organizaciones no deben emplear tecnología en línea que no permita al individuo decidir sobre su información personal. Indica como

buena práctica evitar el seguimiento de comportamiento de niños, en sitios Web dirigidos a este sector.

Finalmente indica que la organización debe contar con una política de privacidad que permita establecer y mantener la confianza del usuario o consumidor en el ámbito digital.

Guidance on Covert Video Surveillance in the Private Sector*,* Mayo, 2009. (Relacionada con *Guidelines for Overt Video Surveillance in the Private Sector,* Marzo, 2008) Tiene como objetivo servir de guía para el cumplimiento de PIPEDA por las organizaciones del sector privado que utilizan el sistema de video vigilancia "encubierta", que a Criterio de la Oficina del Comisionado de Privacidad es una tecnología invasiva de la privacidad. Las consideraciones que deben tener en cuenta las organizaciones en este rubro son:

- ¿Cuál es la razón para recolectar información personal a través de video vigilancia "encubierta"?
- ¿Por qué, cuándo y dónde se recogen datos personales?
- Justificar y demostrar la necesidad de utilizar este medio de recolección de datos.
- La información recopilada debe estar relacionada con un propósito comercial legítimo y objetivo.
- La pérdida de privacidad de un individuo debe ser proporcional al beneficio obtenido por la organización.
- Consideración de otros medios para la recolección de datos personales o analizar si es el medio idóneo el de video vigilancia "encubierta".

- Consentimiento.
- Proporcionalidad.
- Documentación de la política y guía de procesos, que en términos generales debe contener:
  - Criterios específicos a cumplirse antes de llevar a cabo la video vigilancia “encubierta”.
  - Documentar las razones y propósitos.
  - Proporcionalidad.
  - Almacenamiento de la información de forma segura.
  - Restricción de accesos.
  - Procedimientos para la transferencia a terceros.
  - Periodo de retención.
  - Procedimiento de eliminación de información personal.

Guidelines for Processing Personal Data Across Borders, Enero, 2009. Lineamiento elaborado para el tratamiento de datos personales transferidos a un tercero, incluyendo los que se encuentren fuera de Canadá. Señala que las organizaciones deben cumplir con los siguientes puntos:

- La transferencia de datos a un tercero debe constar en un contrato.
- La organización debe tomar medidas razonables para proteger

la información de usos no autorizados o revelaciones, cuando esté siendo procesada por un tercero.

- Asegurarse que el tercero cuenta con políticas, procesos de privacidad, personal capacitado y medidas de seguridad eficaces que garanticen la protección de datos personales.

- Posibilidad de evaluar o auditar el manejo que hace un tercero de los datos personales que le son transferidos.

Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation – A Guide for Retailers, December, 2008 (*Your Customers' Driver's Licence Card – Do you need it? A Guide for Retailers,* Abril, 2009). Establece algunas consideraciones sobre la recolección de información personal contendida en licencias de conducir por pequeñas empresas, indicando que la regla de oro es recopilar la menor información posible para la satisfacción de una finalidad comercial legítima.

Guidelines for Recording Customer Telephone Calls, Revisado en Junio del 2008. Señala consideraciones que las organizaciones que emplean la grabación de llamadas telefónicas tanto las iniciadas por el cliente como las que realiza la organización, señalando lo siguiente:

- Únicamente realizar grabaciones con fines específicos.

- Informar al cliente que la llamada puede ser grabada.

- Registro sólo con el consentimiento.

- La información solo se debe utilizar para los fines especificados.

- Cumplimiento de los requerimientos establecidos por la Ley,

como seguridad, acceso, retención o eliminación de la información.

Guidelines for Organizations Responding to Privacy Breaches, Agosto, 2007

- ***Key Steps for Organizations in Responding to Privacy Breaches***. El propósito es orientar a las organizaciones del sector privado, para afrontar violaciones a la privacidad (acceso, recopilación, uso o divulgación de información personal no autorizado). Los pasos clave que establece para enfrentar una violación son:

  - Detener inmediatamente la práctica no autorizada: A tal efecto debe designarse una persona para iniciar la investigación e indagar sobre las causas, ya sean internas o externas de la amenaza. Si de ello se desprende que fue causado por una conducta criminal debe notificarse a la policía.

  - Evaluación de riesgos: Saber qué tipo de información fue violentada, e identificar si fue información sensible, ya que son los que más ataques reciben. La causa del ataque, así como determinar si los datos fueron perdidos o robados. También debe considerarse el uso que pueda darse a la información robada para identificar los potenciales culpables.

  - Aviso al titular de los datos personales.

  - Plan de prevención.

- ***Privacy Breach Checklist.*** Señala un listado de preguntas para la atención de incidentes de violación de datos personales.

Guidelines for Identification and Authentication*,* Octubre, 2006. Lineamientos destinadas a ayudar a las organizaciones a desarrollar procesos de identificación y autenticación, entre las que señala:

- Sólo debe autenticar cuando sea necesario.
- Nivel de identificación acorde al riesgo de información protegida.
- Evaluación periódica de riesgos y amenazas.
- Monitoreo de ataques, averías y pérdidas.
- Capacitación de personal.
- Responsabilidad de los individuos.
- Opción de modificación de identificadores y autenticadores.
- Opción para los individuos en la elección de identificadores y autenticadores.

Además de las directrices señalas anteriormente la Oficina del Comisionado de Privacidad de Canadá cuenta con una serie de manuales dirigidos a las organizaciones, con la finalidad e apoyarlas al cumplimiento de las obligaciones que les impone la ley PIPEDA.

Es así que encontramos las siguientes guías y manuales:

Herramienta en línea

- ***Build a Privacy Plan for Your Bussiness***[90]**,** herramienta que funciona a través de la aplicación de un cuestionario, que permitirá a la organización desarrollar procedimientos para la protección de datos personales, capacitación de personal para la solución de preguntas, así como la atención de quejas. Al concluir el cuestionario se indica que la organización contará con una auditoría de la información que recopila, las disposiciones que deberá cumplir, un plan de seguridad, un folleto muestra de privacidad para clientes y evaluación de necesidades. Además se le proporcionará políticas de privacidad muestra.[91]

Guías

- ***A Guide for Businesses and Organizations Your Privacy Responsabilities.*** Documento elaborado por la Oficina del Comisionado de Privacidad, cuyo objetivo es brindar a las organizaciones la oportunidad de revisar y mejorar sus políticas y prácticas de gestión de información personal.

- ***Privacy Guide for Small Businesses: The Basics.*** Documento elaborado para orientar a las pequeñas empresas a mejorar sus prácticas de privacidad y evitar investigaciones.

- **Código Modelo para la Protección de Datos Personales de la Asociación Canadiense de Estándares.**

90 Disponible en: http://www.priv.gc.ca/resource/tool-outil/english/index.asp?a=logout
91 Véase My Privacy Plan

El Código Modelo fue elaborado por el Comité Técnico sobre Privacidad del la Asociación Canadiense de Estándares[92], mismo que fue reconocido por el Consejo Canadiense de Normas[93].

La Asociación señala en la introducción del código modelo que se deberá adecuar a las necesidades del particular o usuario, que deberá adecuarlo a los propósitos específicos, el modelo es sujeto a revisiones periódicas y sugerencias para el mejoramiento y adecuación.[94]

A continuación se expone de forma sintetizada el contenido del Código Modelo:

Alcance

De acuerdo con este documento, cualquier organización (asociaciones, empresas, organizaciones de beneficencia, clubes, instituciones, sindicatos, etcétera) puede adoptar el código modelo, orientándola a considerar los requisitos mínimos para la protección de datos personales, pudiendo adaptarla a las necesidades y circunstancias específicas, por ejemplo al tipo de datos personales que se tratan.

Definiciones

El documento contempla un apartado de definiciones para homologar las consideraciones respecto a puntos como conceptualizar los alcances de la recolección de datos personales, los tipos de consentimiento, la información personal no disponible, los sujetos que son considerados como “organización”, cuál es la información personal, los alcances del tratamiento de datos personales.

92 http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/technical-committee-on-privacy

93 Es el órgano federal que tiene como facultad promover la estandarización y eficiencia de las normas canadienses. Véase *Standards Council of Canada Act.*

94 Véase Introducción del Código Modelo para la Protección de Datos Personales de la Asociación Canadiense de Estándares.

Disposiciones Generales

Dispone que los diez principios que son desarrollados en el código modelo deberán ser cumplidos en su totalidad por las empresas, ya que se encuentran correlacionados; pudiendo adecuarlo a los requerimientos particulares. Señala que el documento es de adopción voluntaria; sin embargo, cuando el modelo sea adoptado por una organización, lo establecido se convertirá en una obligación. Aclara que el término "debe" tiene el alcance de una recomendación.

Principios

Nota: Todos y cada uno de los principios están correlacionados.

- **Co-Responsabilidad – *Accountability***. La organización es responsable de proteger los datos personales que ha recabado y los transferidos a terceros; asimismo está obligada a designar a la o las personas responsables que vigilen del cumplimiento de los principios. Señala la obligación de establecer "cláusulas contractuales" en la prestación de servicios de terceros que realizan tratamiento de información personal recabada por la organización, para que protejan los datos personales conforme a los estándares nacionales. Establece como requerimiento para cumplir con los principios señalados el de: a) procedimientos para proteger la información personal, b) procedimientos para la recepción y atención de quejas y consultas; c) capacitación del personal sobre las políticas y prácticas respecto al tratamiento de datos personales, y d) Formulación e mecanismos de información para explicar las políticas y procedimiento de la organización en materia de protección de datos personales.

- **Finalidad** – ***Identifying Purposes***. La organización deberá señalar los fines para los que hace la recolección de datos personales bien antes o en el mismo momento en el que obtiene la información, teniendo la oportunidad de identificar la información necesaria para el cumplimiento del propósito establecido; siendo necesario documentar el cumplimiento de esta obligación. Señala los medios por lo que puede informarse a los particulares sobre los propósitos de la recolección de datos, ejemplificando que un formulario como herramienta de información y solicitud de información personal. Impone la obligación de informar al particular sobre nuevos propósitos de tratamiento, por lo que deberá obtener el consentimiento sobre la nueva condición.

- **Consentimiento – *Concert.*** Un principio fundamental para el tratamiento de información personal es la obtención del consentimiento del particular, señalando que existirán excepciones a este principio (causas legales, imposibilidad material, causas medicas o de seguridad nacional), así como la postura de los terceros en la obtención del consentimiento o bien cuando los propósitos han cambiado o surgido nuevos. Se correlaciona al principio de información, obligando a la empresa a realizar "esfuerzos razonables" para garantizar que el particular esté enterado del uso y finalidades con las que se han recabado sus datos, así como el cambio de propósitos de ser el caso. Prohíbe a las organizaciones condicionar la prestación de servicios a la obtención del conocimiento y el tratamiento de datos. Indica que para la obtención del consentimiento y la forma o medios en que se debe hacer, la organización debe tener claridad en el tipo de datos (sensibles) que se están solicitando, señalando que "dependiendo del contexto cualquier información pudiera ser sensible". Señala que el consentimiento no debe ser obtenido por medio de engaños. En lo concerniente al tipo de consentimiento, es señalado que la regla general para el caso de datos sensibles será el expreso, cuando sea información "menos sensible" será el tácito; sin limitar que pueda ser otorgado por un representante legal con poderes especiales para ellos. Las personas tienen derecho a revocar su consentimiento en cualquier momento (previa revisión de restricciones legales o contractuales), y la organización debe informarle de las consecuencias.

- **Proporcionalidad – *Limiting collection*.** Es obligación de las organizaciones recabar únicamente los datos personales que son necesarios para el cumplimiento de sus fines, utilizando medios idóneos y legales, que impidan la obtención de información por error o con engaños, incorporando a las políticas de tratamiento de datos personales la especificación de la información que es recopilada.

- **Limitación de uso, divulgación y retención – *Limiting Use, Disclosure and Retention*.** El código modelo señala que la información personal será utilizada o en su caso revelada únicamente para los fines por los cuales fue obtenida, o bien, previo consentimiento del individuo; conservando la información solo el tiempo necesario para el cumplimiento de sus fines, desarrollando lineamientos e implementar procedimientos correspondientes a la retención, señalando periodos mínimos y máximos, quedando sujetos a los requisitos establecidos por la legislación. Para el caso de información que ya no resulta necesaria, esta deberá ser destruida, borrada o disociarse, para lo cual la organización deberá

establecer los lineamientos o procedimientos para regular la destrucción de datos personales.

- **Calidad – *Accuracy.*** La organización deberá cuidar que la información personal que recolecta o somete a tratamiento necesaria para la realización de sus propósitos es exacta, completa y actualizada, lo anterior para que poder reducir al mínimo la posibilidad de toma de decisiones de un individuo con base en información inadecuada, el mismo principio debe respetarse para los datos personales que son tratados por terceros.

- **Seguridad – *Safeguards***. La información personal en posesión de particulares estará protegida por medidas de seguridad adecuadas y necesarias al tipo de datos que se esté tratando. Dichas medidas serán contra el robo o pérdida, el acceso no autorizado, revelación, copiado, uso o modificación de la información personal; lo anterior será aplicado sin importar el formato en que se lleva a cabo. Precisa que tratándose de datos personales sensibles el nivel en las medidas de seguridad será mayor o más alto. Las medidas serán: a) físicas, b) administrativas y c) tecnológicas. Correlacionado con lo anterior, la organización deberá concientizar a los empleados sobre la importancia de mantener la confidencialidad de los datos personales.

- **Información – *Openness*.** Deberá la organización poner a disposición de los particulares información precisas, clara y accesible sobre sus políticas y prácticas relacionadas con el tratamiento de datos personales, entre la información que se señalada deberá estar disponible está: a) nombre, cargo y dirección del responsable de la protección de datos personales, así como de la atención de quejas o envío de consultas, b) procedimientos para acceder a la información que se encuentra en posesión de la organización, c) Información sobre el tipo de información que está en pode de la organización así como el uso que se hace de esta, d) Documentos en los que se explique las políticas, normas o códigos respecto a protección de datos personas -el formato dependerá de cada organización-, y e) Información sobre qué datos personales son transmitidos a organizaciones afines (filiales por ejemplo).

- **Acceso** – ***Individual Access.*** Los particulares previa solicitud deberán obtener información sobre la existencia, uso y divulgación de su información personal, así como la rectificación o modificación de los datos que no sean exactos; indicando que la excepción al cumplimiento de este principio (costos elevados, información relacionada con otras personas, por causas de seguridad, en

relaciones cliente-abogado, etcétera). Se sugiere en el documento a las organizaciones, revelen la fuente por la que se obtuvo la información personal. Señala como excepción para los datos de salud la obtención de información relacionada con la salud del particular a través de un médico. Señala como obligación del particular, el proporcionar información precisa y suficiente a la organización, para que está a su vez esté en condiciones de atender una solicitud de existencia, uso y divulgación de información personal, y dicha información será utilizada únicamente para este fin. Asimismo al proporcionar atender una solicitud de información, la organización deberá ser específico al proporcionar información sobre terceros a los que se les ha revelado información. La atención de solicitudes debe realizarse en un plazo razonable y con un costo mínimo o gratuito para el individuo, en un formato sencillo y comprensible. Cundo los individuos que comprueben la existencia de información personal inexacta, la organización realizará la acción correspondiente y necesaria –ya sea de corrección, eliminación o adición-, haciéndola del conocimiento de terceros que intervengan en el tratamiento.

- **Atención de Quejas - *Challenging Compliance***. La organización deberá contar con procedimientos para la atención de quejas o recepción de preguntas sobre sus políticas y prácticas relativas a la protección de datos personales, que deberán ser accesibles. Con lo anterior el individuo podrá solicitar el cumplimiento de los principios descritos en el código modelo. Asimismo deberán hacer del conocimiento de los individuos que realicen consultas o solicitudes, la existencia de procedimientos de atención a quejas, (existen organismos reguladores de empresas específicas que tramitan quejas). El obligación de la organización la investigación de todas las denuncias, así como tomar las medidas necesarias inclusive realizar modificaciones a sus políticas o prácticas de privacidad.

Anexo A.

Se adjunta la Directriz de la OCDE sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales, indicando que la directriz fue la base para la elaboración del Código Modelo elaborado por la Asociación Canadiense de Estándares.

6.2 Diagnóstico del modelo canadiense

Es pertinente señalar que la autorregulación en Canadá no cuenta con un basamento normativo robusto que permita el impulso, desarrollo e implementación de esquemas de autorregulación en el que la participación de la autoridad sea visiblemente importante, ya que cuenta únicamente con un código tipo.

Es importante destacar el papel que desempeña la Oficina del Alto Comisionado de Privacidad de Canadá en los términos y facultades que le impone PIPEDA, siendo principalmente investigar quejas, formular conclusiones y emitir recomendaciones no vinculantes, así como alentar a las organizaciones a desarrollar políticas y prácticas; o bien, códigos de protección de datos personales.

Una característica de PIPEDA es la de establecer que tanto el titular de la información personal como el Comisionado de Privacidad podrán acudir ante la Corte Federal para exigir el cumplimiento de la ley.

6.2.1 Problemáticas

Las interpretaciones que las autoridades han realizado de PIPEDA tienen como finalidad orientar y clarificar los alcances de la ley, apoyando a las organizaciones para adoptar o implementar nuevas tecnologías que les permitan seguir siendo competitivas en una economía global, logrando establecer prácticas responsables sobre la protección de datos personales que están en posesión de particulares buscando equilibrar la privacidad con el desarrollo de negocios legítimos.

Derivado de los diversos casos que han sido dirimidos tanto por el Comisionado, como por los Tribunales Canadienses; se han interpretado o aclarado disposiciones establecidas en PIPEDA.

La primer problemática que enfrentaron las autoridades en la implementación de PIPEDA fue la de limitar el ámbito de aplicación de la ley, surgiendo la interrogante sobre cuáles serían los datos personales que estarían en el ámbito de protección de la ley, diferenciando la información personal de la actividad comercial. A tal efecto se ha expandido la protección a las fotografías, la dirección de correo electrónico para negocios, el número de identificación ligado a un empleado, y la dirección IP (computer Internet Protocol).

Respecto a las fotografías95 se ha determinado que son un dato personal, esto derivado del estudio que se hizo de un caso sometido al Comisionado de Privacidad en Canadá. Se consideró que las fotografías de inmuebles tomadas por los corredores de bienes raíces o aseguradoras constituían un dato personal ya que a través de estas podría identificarse a un individuo o bien revelarse información personal, por lo tanto es necesario recabar el consentimiento del titular en forma previa a la toma de fotografías, así como informarle de las finalidades. Puntualizando que, aunque se trate de una práctica comercial, para los alcances de PIPEDA se trata de un dato personal que requerirá de protección e información al titular de las políticas y prácticas relacionadas con la gestión de información personal.

En cuanto al **criterio de información identificable**, una Corte Federal elaboró el siguiente criterio:

95 Véase PIPEDA Case Summary #2006-349 [Disponible en línea: http://www.priv.gc.ca/cf-dc/2006/349_20060824_e.cfm]

> [Se considera] información identificable sobre un individuo aquella donde hay una seria posibilidad que pueda ser identificado de acuerdo al uso de esa información, sólo o en combinación con otra información disponible. ("Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.")

De igual manera la Corte canadiense constató que cierto tipo de información puede ser relacionada con otros campos a los que pueden tenerse acceso, por ejemplo, una base de datos con información médica (fuente privada), ligada a los obituarios (información pública); por lo que incrementan las posibilidades de identificar a un sujeto.

Es así que, se han hecho pronunciamientos tanto por la Oficina del Alto Comisionado de Privacidad como de la Corte Federal en relación a interpretaciones sobre los siguientes temas:

6.2.2 Actividades transfronterizas

La principal preocupación al respecto ha sido el intercambio de información con Estados Unidos, y que en virtud de la *Patriot Act* el gobierno estadounidense pueda irrumpir en los datos personales de canadienses. Para poder intercambiar datos en otras jurisdicciones las empresas deben utilizar algún medio adecuado, como un contrato, que otorgue la protección mínima ofrecida por PIPEDA, avisar al cliente cómo será utilizada su información, y que los gobiernos extranjeros donde se transfiera la información pueden obtener sus datos en virtud de sus leyes.

Este fenómeno es muy frecuente en Canadá, ya que existe una gran cantidad de empresas extranjeras con filiales a lo largo del país, por lo que ha ocurrido que las empresas asentadas en Canadá den la opción a sus clientes de que sus datos sean tratados en otros países o en Canadá, con las desventajas de que en Canadá el tratamiento tiene menor protección que si son enviados a otro territorio.

Vigilancia apropiada o inapropiada. Bajo este tópico la autoridad se ha enfrentado principalmente a dos dificultades: las cámaras de seguridad y la vigilancia a empleados. Para determinar la legitimidad de la vigilancia la ley determina analizar si es el medio necesario, si es efectivo, la proporcionalidad de la medida con el beneficio y si es el medio menos invasivo. En cuanto a las cámaras de seguridad la autoridad ha encontrado satisfactoria la medida, no obstante ha realizado recomendaciones a las empresas para su implementación96.

Por otro lado la vigilancia a los empleados para propósitos disciplinarios se ha considerado como una invasión arbitraria a la intimidad, por lo tanto la práctica se encuentra prohibida bajo la PIPEDA.

Nuevas tecnologías. En cuando a las nuevas tecnologías ha prestado atención los datos biométricos, como los sistemas de reconocimiento de voz, y los dispositivos con tecnología GPS, mismos que se encuentran bajo el amparo de la ley.

Violación a medidas de seguridad. Ante diversos casos el Comisionado advirtió la falta de una disposición expresa que obligara a las empresas a dar aviso a sus usuarios de que hubo acceso indebido a sus datos personales,

96 Véase "Guidelines for Overt Video Surveillance in the Private Sector", marzo de 2008, [Disponible en línea: http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.pdf]

por lo que en 2007 emitió los lineamientos respectivos97.

Capacitación de empleados. En 2006 fueron emitidos lineamientos relativos a la identificación y autentificación de clientes98, ya que los empleados de diversas compañías telefónicas no se cercioraban de la identidad del usuario del servicio.

Información personal y el respeto al principio de proporcionalidad. Bajo este rubro la autoridad ha prestado mayor atención a los servicios financieros, ya que a los usuarios de tarjetas de crédito se les solicitan muchos datos personales con la finalidad de prevenir el robo de identidad y el fraude. Específicamente se ha solicitado una foto del usuario para tal fin, a lo que el comisionado ha visto como buena práctica que no sea cualquier empleado quien lo maneje o recabe, sino una oficina especializada en ese tratamiento.

Respecto a la información sobre la salud las empresas han tenido prácticas negativas al recabar este tipo de datos de sus empleados, por lo que ha resultado violatorio al principio de proporcionalidad.

Acceso de los particulares a la información personal (procedimientos y tarifas de acceso)

Uso indebido y divulgación de la información personal con fines comerciales secundarios. En razón de que, las facultades del Alto Comisionado sólo se limitan a promover la adopción de códigos de protección de datos personales, la autoridad no presenta información relativa

97 Véase "Key Steps for Organizations in Responding to Privacy Breaches" [Disponible en línea: http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf]

98 Véase Guidelines for Identification and Authentication [Disponible en línea: http://www.priv.gc.ca/information/guide/auth_061013_e.asp]

al grado de adopción y cumplimiento por las organizaciones del código modelo.

En su reporte al Congreso de 201099 el Comisionado siguió de cerca diversos casos significativos de privacidad, de los que destacan Facebook, eHarmony y Google. Respecto a Facebook investigó las aplicaciones de terceros, por lo que se le solicito ser más explícito respecto a las características y condiciones que se prestaría el servicio.

Ahora bien, eHarmony es un sitio de citas por Internet, en el que la autoridad comenzó una investigación luego de que una persona solicitara borrar su perfil en el cual aparecían muchos datos personales, incluso algunos muy sensibles. Ante su solicitud eHarmony bloqueó el perfil del usuario, sin embargo lo que realmente pedía era borrar toda su información. La autoridad recomendó a la compañía a hacer una distinción entre la opción de desactivar (temporal) y eliminar (permanente); para ello se implementó un sistema de guardar dos años los datos de sus usuarios para que pudieran recuperarlos en ese periodo.

En cuanto a Google hubo un incidente respecto a la obtención de información de redes inalámbricas (wi-fi) no protegidas por medio de los autos que tomaban imágenes para Google Street View, por lo que violentaba la ley canadiense al no existir consentimiento para la obtención de datos; ante ello expertos informáticos se trasladaron a las oficinas de Google en Estados Unidos y verificaron el manejo de dichos datos. Por este mismo incidente la autoridad española y francesa habían multado a Google.

99 Véase Annual Report to Parliament 2010, Report on the Personal Information Protection and Electronic Documents Act [Disponible en línea en http://www.priv.gc.ca/information/ar/201011/2010_pipeda_e.pdf]

En 2010 la oficina del Comisionado inició una consulta pública relacionada a la aplicación de la ley. Con beneplácito la autoridad encontró que en opinión de la industria era favorable a la PIPEDA, ya que ha podido adaptarse al uso de nuevas tecnologías. Una de las dificultades más frecuentes por parte de la industria era identificar cuándo se encontraban frente a datos personales. Por otra parte los usuarios mostraron mayor preocupación respecto a la protección de datos personales de menores y la retención de información personal en particulares, no obstante, a criterio de la autoridad, son problemáticas que pueden ser atendidas bajo el marco jurídico existente.

6.3 NYMITY

Para los efectos de esta investigación, es importante señalar el caso de la empresa denominada **"Nymity"**[100], misma que fue fundada en Canadá en el año 2002, que de acuerdo con la información vertida en su página de Internet es "*una organización mundial de investigación y apoyo en materia de privacidad".* Sus servicios están encaminados a la creación de políticas y procedimientos para las empresas que realizan tratamiento de datos personales, así como la implementación de un programa de gestión privacidad para auditar y evaluar el cumplimiento de los mismos.

Como se ha indicado anteriormente, uno de los principios que son establecidos en PIPEDA y desarrollado en el Código Modelo de Protección de Datos Personales, es el relativo a la Responsabilidad o rendición de cuentas *(Accountability),* recordando que dicho principio fue establecido por la Asociación Canadiense de Estándares (Canadian Standards Association's) en 1995, y posteriormente plasmado en el código modelo. Es así que, para Nymity la rendición de cuentas es un componente central de su metodología

[100] 100 Véase página de Internet de la empresa Nymity Disponible en línea: http://www.nymity.com/

de investigación e implementación de políticas y procedimientos de privacidad.

Señala que cuenta con más de 1000 suscriptores101 de todo el mundo, representando diversos sectores e industrias (pequeñas empresas, grandes corporaciones multinacionales, proveedores de servicios médicos, reguladores y gobierno).

Nymity indica que cuenta con relaciones estratégicas con organizaciones que pueden ayudar a sus clientes; o bien, a diversos profesionales con el cumplimiento de protección de datos personales y gestión de riesgos. Entre las que se encuentran:

- Asociación Internacional de Profesionales de la Privacidad (IAPP).
- LexisNexis.
- TRUSTe.
- RSA Archer
- Privacy by Design
- Ponemon Institute
- United States Council for International Business (USCIB)

De la información que proporciona Nymity, se encuentra un cuadro102 en el que se describen los componentes de un **programa básico de privacidad**, entre los que se mencionan los siguientes:

- Aprobación de cláusulas modelo
- Creación de la Oficina de Privacidad

101 Véase lista de clientes [Disponible en línea: http://www.nymity.com/About_Nymity/Customers.aspx]
102 Véase Implement and Maintain an Effective Privacy Program

- Aviso de Privacidad en línea
- Procedimientos de Protección de Datos
- Política interna de Privacidad
- Medidas de Seguridad
- Privacy by Design
- Informes de incumplimiento de protocolo
- Capacitación de empleados
- Evaluaciones
- Programa de Concientización de Empleados
- Contratos con proveedores
- Seguimiento de quejas

Asimismo entre los componentes que indica para un **programa "maduro"** están:

- Proveedor de servicios de autoevaluación
- Grupo de Trabajo de Privacidad
- Programa de Privacidad del Empleado
- Manuales o Políticas Operativas de Privacidad
- Convenios entre empresas
- Código de Conducta del Empleado
- Programa de Educación al Consumidor
- Auditoría Interna
- Informes de Rendición de Cuentas
- Programa de Gobernabilidad de Datos
- Auditoría Interna de los Proveedores de Servicios
- Programa de Monitoreo de Cumplimiento.

6.4 Privacidad por Diseño (Applying Privacy by Design, Best Practices to SDG&E's, Smart Pricing Program)

La compañía San Diego Gas & Electric (SDG & E) y la Oficina del Comisionado de Información y Privacidad de Ontario, Canadá, elaboraron de forma conjunta un documento en el que se adopta el "**Privacy by Design**" en la red de distribución inteligente o Smart Grid que proporciona SDG&E; es así que, en el documento se plasma el compromiso de la compañía en diseñar, construir e implementar un sistema de redes inteligentes confiable que protegerá la privacidad de los clientes.

Se indica que, los principios en lo que se deberá basar el diseño o implementación de mejores prácticas en privacidad en una red de distribución inteligente son:

- Incorporar en los diseños de redes inteligentes, así como en la planeación general de los proyectos el tema de protección de datos personales de los clientes.

- Se debe garantizar la privacidad en todos los programas

- La protección de datos personales será un requisito *sine qua non* en el diseño de sistemas de redes inteligentes.

- Protección de los datos personales en todo el ciclo vital de cualquier información de carácter personal.

VII.- AUTORREGULACIÓN PURA

En segundo lugar se observa que existen países que no tienen propiamente una legislación sobre protección de datos personales comprehensiva y que, en su mayoría, dejan este tema en manos de los particulares (*modelo de autorregulación pura*).

7.1 Estados Unidos

Estados Unidos se caracteriza por tener un marco jurídico muy flexible en materia de protección de datos personales en el cual se le deja a las empresas actuar conforme a sus necesidades. Dicho marco se compone de las mejores prácticas de las empresas, la actuación de la Federal Trade Commission (FTC) y un grupo de autoridades y profesionales que desarrollan diversas prácticas para promover la cultura de la privacidad.

Sólo con cierto tipo de datos personales existe una regulación más profunda para proteger a los usuarios, como los datos bancarios, médicos o de menores. Esta tendencia de la autorregulación pura, es decir, sin participación de la autoridad, salvo dichas excepciones parece que cambia de rumbo hacia una mayor injerencia del Estado en beneficio de los ciudadanos.

Dicha tendencia se deriva de la importancia de las tecnologías de la información en la vida cotidiana. Por ejemplo, en Estados Unidos las ventas al menudeo por Internet alcanzan los 145 mil millones de dólares anualmente[103]. Otro dato de relevancia es que 5% de las quejas por robo de

103 Véase White House "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy", febrero 2012, pag. 6. Disponible en http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

identidad son de servicios por Internet[104], razón por la cual ha sido necesario regular más este medio.

También existe heterorregulación en materia de telecomunicaciones e información genética en el ámbito laboral. Además por su carácter federal existen diversas leyes locales que eventualmente abordan la temática.

Primero, en las áreas donde no existe regulación, la Federal Trade Commission (FTC) actúa como autoridad para vigilar que las prácticas comerciales no sean contrarias a la ley[105], por lo que ha realizado estudios y lineamientos para apoyar a la industria a elaborar sus esquemas de autorregulación.

7.1.1 Autorregulación de la industria en línea

Respecto a industria en línea en febrero de 2009 la FTC elaboró principios para el uso de **software de comportamiento de usuarios**.106 Para este fin fueron realizadas diversas consultas en las que se solicitó los comentarios de las empresas. Los principios consolidados son los siguientes:

- Transparencia y control del consumidor: Debe advertirse en un lenguaje claro, conciso, amigable y de forma destacada los propósitos de recabar su información, y la opción de negarse.
- Seguridad razonable y límite de retención de datos para los datos de los usuarios: Deben cumplirse con las leyes en materia de seguridad y las acciones emprendidas por la FTC en la materia. El tipo de seguridad debe

104Véase Federal Trade Commission, Consumer Sentinel Network Data Book for january – december, pág. 3. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf
105 Véase sección 5 de la Federal Trade Commission Act.
106 http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf

basarse en la sensibilidad de la información, la naturaleza de las operaciones comerciales, el tipo de riesgos a los que se enfrenta la compañía y la protección razonable con la que cuente la compañía. Así como limitar la obtención de información en tanto sea necesario para el negocio o lo requiera la ley.

- Consentimiento expreso afirmativo para cambios de material para la promesa de privacidad existente.
- La afirmativa del consentimiento expreso para usar información sensible.

7.1.2 Modelos de autorregulación exitosos

A manera de ejemplo son representativos los siguientes modelos de empresas de autorregulación.

a. TRUSTe[107]

TRUSTe es una compañía con sede en San Francisco, que se encarga de ofrecer servicios de soluciones de privacidad en línea y proporciona un amplio conjunto de servicios de privacidad para ayudar a las empresas a crear confianza y aumentar la participación a través de todos sus canales en línea, incluyendo sitios web, aplicaciones móviles, publicidad, servicios de nube, análisis de negocio y marketing por correo electrónico.

Más de 4.000 sitios web, incluidos los de las principales compañías como Apple, AT&T, Disney, eBay, HP, Microsoft y Yelp dependen de TRUSTe para garantizar el cumplimiento dee sus obligaciones y los complejos requisitos de privacidad. La misión de TRUSTe, basado en una "verdad en la privacidad", se construye sobre una sólida base de la transparencia, la elección y la

[107] www.truste.com

rendición de cuentas respecto a la recopilación y el uso de información personal.

En su aviso de privacidad detalla que recabará nombre, correo electrónico y localización en caso de utilizar su servicio de quejas (Watchdog Dispute Resolution process) por un mal uso de datos personales por parte de las empresas certificadas o de TRUSTe. Luego de resuelto el problema se dará la opción al usuario de responder una encuesta de satisfacción del servicio. TRUSTe no compartirá la información del cliente a la empresa certificada sin su autorización.

Quienes apliquen para la certificación se recabarán sus datos de contacto necesarios para brindar soporte técnico, explicar las opciones que ofrece TRUSTe y acelerar el proceso de certificación. Estos datos no se compartirán con terceros con propósitos comerciales sin el consentimiento.

TRUSTe podrá utilizar la información de sus clientes para realizar encuestas o estadísticas sin que se identifique a cada uno de ellos. Ocasionalmente TRUSTe realiza encuestas a los consumidores respecto a la satisfacción del servicio, esta información la utilizará para mejorar sus servicios.

Además TRUSTe utiliza cookies con opción de eliminarse (opt-out) para auxiliar en la navegación de su sitio. Automáticamente se recabarán la dirección IP, tipo de navegador, páginas de ingreso o salida (referring/exit pages) y sistema operativo, que sólo será utilizada para entender el tipo de visitantes que entran al sitio.

Respecto a compartir la información personal con terceros, sólo es respecto quienes ayudan a TRUSTe en proveer sus servicios, tales como análisis o servicios al cliente. También compartirá los datos personales si es requerido

por la ley, cuando se crea que puede ayudar a proteger los derechos o seguridad de sus clientes como investigación de fraude o requerimiento del gobierno. Además notificará de cualquier cambio que afecte las condiciones de privacidad. En cualquier otro caso se necesitará el consentimiento para compartir información con un tercero.

Se podrá accesar y modificar la información personal. En materia de seguridad se comprometen a utilizar medios adecuados, y finalmente si se sale del sitio de TRUSTe deberán atenerse a otros avisos de privacidad.

Se recomienda conocer el estudio comparado108 que Trust-e hace de otras marcas.

b. Better Business Bureau

BBB Better Business Bureau es un conjunto nacional de organizaciones sin fines lucrativos que trabaja principalmente en Estados Unidos y Canadá, apoyado financieramente por la clase empresarial de cada área de servicios. BBB trabaja para mejorar las relaciones entre consumidores y compañías, pero sobretodo se enfoca en la protección de los consumidores.

Dentro de las funciones que realizan está la de promover normas éticas entre la comunidad empresarial, ayudar a la resolución de problemas que tiene con

108 http://www.truste.com/consumer-privacy/comparing-web-privacy-seals Se comparan:

- Verisign Trust Seal. The Verisign Trust Seal verifies the identity of a website's owner and operator and confirms that the site is subject to daily malware scans and uses verified data encryption (SSL).
- McAfee Secure Trustmark.The McAfee Secure Trustmark confirms that a website is subject to daily malware and vulnerability scans.
- Comodo HackerProof SealThe Comodo HackerProof Seal confirms that a website is subject to daily malware and site vulnerability scans as well as quarterly PCI compliance scans. .
- GeoTrust SSL Certificates.The GeoTrust SSL Certificate indicates that a website uses verified data encryption (SSL).

compañías, trabajando como mediadores entre los dos; vigilar anuncios para verificar si son honestos, justos, y si califican a las regulaciones del gobierno, vigilan organizaciones de caridad y sin fines lucrativos para verificar qué hacen con las donaciones y cómo funcionan, así como avisar sobre estafas y problemas con compañías y ofertas discutibles.

Para ser acreditado y formar parte de la BBB es necesario apegarse a su código de buenas prácticas de comercio que consta de ocho principios:

- Construir confianza: La empresa debe haber operado en los últimos doce meses, contar con todos los permisos que requiera la ley, no haber sido multado/sentenciado (goverment action) por conductas contrarias al Código, y haber obtenido al menos la calificación “B” de la valoración BBB.
- Publicidad Honesta: Adherirse a todos los modelos de BBB, así como evitar la publicidad que cause en los clientes una falsa impresión de sus productos o servicios.
- Decir la verdad: Comprometerse a mostrar las verdaderas características de los productos o servicios que la empresa en cualquier tipo de representación, si fuere por escrito de forma clara y comprensible, además de no omitir información relevante.
- Ser transparente: Mostrar la información relevante para que el consumidor pueda elegir el adquirir sus bienes o servicios. También es necesario mostrar la información de la empresa a los clientes y a BBB con el propósito de acreditarlo. En caso de que la empresa lleve a cabo ventas por internet debe ser claro respecto a las características del producto, mostrar las condiciones de la compra, tener la oportunidad de revisar y confirmar la compra antes de hacer la transacción, y proveer un resumen de la operación después de la

compra.

- Promesas de Honor: Mantener la promesa que se realice al cliente y tener encargados que remedien los errores rápidamente.
- Ser responsable: Responder las quejas de los clientes con rapidez, responsabilidad y de buena fe.
- Salvaguardar la privacidad: Proteger los datos personales del fraude y mal manejo. Obtener los datos personales sólo si son necesario y respetar las preferencias de los clientes respecto al uso de su información. Quienes realicen comercio por internet se comprometen a mostrar qué información recolectan, con quién, cómo ser corregida, cómo es cuidada, cómo se comunicará los cambios de la política de privacidad y cómo proceder ante el mal uso de sus datos personales. Quieres recaben información sensible (tarjeta de crédito, números de cuentas bancarias, número de seguridad social, salario u otra información financiera, historial médico, etc.) deberán cumplir con las mejores prácticas/estándares de protección de la industria.
- Honestidad: Ser honesto con los clientes y comportarse de tal manera que no repercuta de forma negativa en la imagen de BBB.

c. Square Trade

SquareTrade es una empresa proveedora de garantías para los productos electrónicos y electrodomésticos con sede en San Francisco y que trabaja solo en Estados Unidos. Las garantías que provee a los consumidores están disponibles para cualquier aparato electrónico o electrodoméstico comprado en linea o en cualquier otra tienda. Además es la aseguradora de eBay. El contrato entre Square Trade y el vendedor que utiliza la plataforma de eBay estipula que:

Permitirá la incorporación del banner de garantía de Square Trade (SquareTrade Warranty Banner) en las listas de ofrecimiento del producto. Contactar por correo electrónico a sus clientes para darles información del servicio, a menos que ellos o el vendedor se nieguen (opt-out). No hacer representaciones falsas de sus productos. Debe pagarse a Square Trade una cuota por cada venta realizada, que será calculada con base en muchos factores como cancelaciones, costos de seguros, costos de pago y servicios de administración.

Además el vendedor se compromete a indemnizar a Square Trade en caso de incurrir en alguna responsabilidad por mal manejo del contrato.

d. VeriSign109

Con sede en Mountain View, California, Estados Unidos, VeriSign es una empresa de seguridad informática que se dedica a la emisión de certificados digitales RSA para su uso en las transmisiones seguras por SSL, principalmente para la protección de sitios en Internet en su acceso por http.

Provee asimismo el sello de confianza mundial **VeriSign Trust™ Seal** cuyo costo anual es de $299.00 dólares aproximadamente.

109 www.verisign.com

e. Web Assured110

Webassured, establecida en Amarillo, Texas, fue fundada como un servicio de protección a los consumidores, pero actualmente se dedica a desarrollar nuevas tecnologías para incrementar la credibilidad y confianza de las páginas web, mediante un sistema de resolución extrajudicial de conflictos.

Esta empresa creó también Shop Assured, un buscador que transmite al usuario información sobre empresas en las cuales se considera que se puede comprar con confianza.

Para la obtención de la marca Webassured se deben seguir los siguientes pasos: 1. Identificación de la razón social y URL; 2. Aceptación de las Normas Universales de ética; 3. Firma del contrato con Webassured; y 4. Determinación del periodo de vigencia del sello

Para la obtención de la marca se requiere cumplir con los siguientes requisitos:

1. Ética
2. Quejas
3. Publicidad
4. Revelación de datos
5. Observación de las leyes
6. Privacidad

110 www.webassured.com

Conforme al Libro Blanco de i+Confianza, el precio establecido para la marca se determina en función de dos parámetros: por una parte los ingresos anuales de la empresa solicitante y por otra la duración solicitada de la vigencia de la marca, siendo el mínimo anual $180.00 dólares.

7.2 Insuficiencias de los modelos

En diciembre de 2010 el Departamento de Comercio de Estados Unidos emitió un informe titulado "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"[111] en el que propone dar mayor protagonismo de la autoridad en la protección de datos personales. En su opinión la adopción de códigos de conducta ayudan a incrementar la certeza, especificidad y dinamismo que requiere la industria, por lo que el gobierno debe promover su creación a través de incentivos. Para tal propósito en materia de autorregulación propone lo siguiente:

- Persuadir a los empresarios y consumidores de las ventajas que conlleva un código de conducta.

- Reforzar las facultades de la FTC para aplicar la ley.

- Otorgar un "safe harbor" [sello de confianza] a las empresas que adopten y cumplan un código de conducta de acuerdo con sus características.

Para lograr estos objetivos el Departamento de Comercio estima necesario **que la FTC apruebe los códigos** previa consulta pública.

111Disponible en http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf

Por otra parte, en marzo de 2012 la FTC envió un informe al Congreso titulado "Protecting consumers privacy in an era of rapid change. Recommendations for Businesses and policymakers"[112]; la cual es la versión final del estudio preliminar de diciembre de 2010[113].

Ante el rápido desarrollo de las tecnologías se ha planteado la necesidad de abordar el modelo adoptado por la FTC para la protección de información personal, sobre este punto existe una perspectiva de protección basada en el daño, es decir, se enfoca en atender las conductas que causen un daño físico o económico, o una intromisión a la vida diaria de los usuarios. Bajo esta visión se puede proteger a los consumidores ante las nuevas tecnologías en numerosos contextos como protección de datos, robo de identidad, privacidad de los niños, spam, "spyware" y telemarketing no deseado.

No obstante este modelo tiene limitantes, ya que algunos usuarios consideran daño no sólo al físico o económico, sino también a su reputación, en el que es incluido el miedo a ser espiado o simplemente a tener datos personales "por ahí". También los consumidores se sienten dañados cuando su información personal, especialmente sus datos médicos o financieros, son obtenidos, usados o compartidos sin su consentimiento o de una manera contraria a sus expectativas[114].

Derivado de este modelo, de 2001 a 2010 fueron ventilados 29 casos contra diversas empresas por violentar la seguridad de datos personales, de ellos cinco se debieron a incumplir su propio código de privacidad, los demás fueron por no tomar los cuidados necesarios para prevenir los ataques más

112 disponible en http://www.ftc.gov/os/2012/03/120326privacyreport.pdf
113 Véase el informe preliminar Federal Trade Commission, "Protecting consumer privacy in a era of rapid change", disponible en http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
114 *Ídem*, pág. 20.

comunes, disponer de manera inadecuada los datos personales de sus clientes y por compartir sus bases de datos con terceros no autorizados[115].

En estos casos la autoridad estadounidense ha ordenado implementar programas de seguridad, así como obtener **auditorías por parte de terceros** imparciales para hacer efectivos dichos programas. Además ha obtenido indemnizaciones a su favor y compensaciones a usuarios.

Otro enfoque es el "**notice-and-choice**", es decir, las políticas de privacidad, pero a criterio de la autoridad éstas se han vuelto más largas, complejas e incomprensibles para los consumidores. Se dice que limitan la responsabilidad frente al cliente con sólo informarlos acerca de cómo será usada su información. Esto hace que los usuarios no tengan control de esas prácticas, por lo que pierden interés y dejan de ejercer sus derechos[116].

Es por las dificultades descritas que la FTC propuso un nuevo marco normativo basado en su experiencia. *Grosso modo* ha sido sistematizado de la siguiente forma:

> **Alcance:** Dirigido a todas las entidades comerciales que obtengan o usen información personal que pueda ser razonablemente identificable con un consumidor específico, computadora u otro servicio, a menos que la entidad recolecte sólo información no sensible de menos de 5,000 consumidores por año y no lo comparta con terceros.

En el informe final al Congreso, la FTC recibió distintos comentarios de la industria, por lo que concluyó que este marco normativo no sería aplicable a aquellas entidades que sólo recolecten información no sensible de menos de

115 *Ídem*,págs. 10 y 11.
116 *Ídem*, pág. 19.

5,000 consumidores por año y no lo comparta con terceros, ya que disminuyen considerablemente el riesgo de daño bajo estas condiciones.

Adicionalmente sobre este rubro la autoridad ha advertido conflictos con el concepto de información de identificación personal [personally identifiable information ("PII")], ya que puede prestarse a arbitrariedad por parte de las empresas, al contrario de la noción "razonablemente identificable", la cual se ajusta a los cambios de las nuevas tecnologías por ser más abierta, puesto que consiste en cualquier dato que pueda ser relacionado con una persona.

Este marco es compatible con otras leyes en materia de protección de datos personales, como la Health Information Technology for Economic and Clinical Health Act ("HITECH") o la Gramm-Leach-Bliley Act ("GLBA"); además de que está dirigida a las compañías que trabajan en línea, como a las que no lo hacen[117].

Por lo que respecta a los principios sustantivos, los de Estados Unidos son acordes con las directrices de la OCDE. Al respecto las prácticas sugeridas son asignar a una persona para proteger los datos personales, capacitar personal en materia de privacidad y cuidar sus transferencias de datos con terceros. El nuevo marco norteamericano también llama a la industria a incrementar sus esfuerzos para educar a los consumidores en materia de privacidad y las herramientas disponibles para ejercer sus derechos.

117 En este sentido se busca hablar de Privacidad a la Medida, según la cual las compañías deben promover la privacidad de sus clientes entre sus organizaciones en todos los niveles de desarrollo de sus productos y servicios:

- Las empresas deben incorporar principios sustantivos para proteger los datos personales de sus clientes, tales como seguridad, límites razonables de recolección, prácticas de eliminación de datos y exactitud en los datos.
- Además deben mantener procedimientos exhaustivos de manejo de datos que incluya todo el ciclo de vida de sus productos y servicios.

Estos principios sustantivos incluyen el "**derecho a ser olvidado" (derecho al olvido),** que incluye la obligación de las empresas de eliminar aquellos datos que ya no le son necesarios, así como el derecho del usuario de acceder a sus datos, y en ciertos casos poder eliminarlos.

En este aspecto Vint Cerf, creador del protocolo TCP/IP y Vicepresidente Mundial de Google en la actualidad, ha manifestado su preocupación sobre la ley del "derecho al olvido" propuesta por la Unión Europea, considerando que puede ser una amenaza para la web**.** Según Cerf, "el derecho al olvido es imposible de lograr, debido a que copiar información que está en Internet a los computadores y volver a subirla es demasiado fácil. Además –agrega-, nuestro mundo ya tiene clara la idea de que una vez que algo se hace público (en un libro, revista o diario por ejemplo), no puede ser retractado fácilmente. Esto también debería aplicarse al mundo digital…".

> *"No puedes ir y eliminar contenido del computador de todo el mundo sólo porque quieres que el mundo se olvide de algo. No creo que sea una propuesta práctica"*. El equivalente a esta idea en el mundo físico, *"es aterrador; si alguien dijera 'quiero que todos se olviden de este libro que publiqué porque es vergonzoso', ¿cómo implementas eso? Tendrías que entrar a las casas de las personas y sacar el libro de los estantes. Hay algunos problemas legales con eso, y me parece a mí que no debería ser más fácil en el mundo online".*

El "derecho al olvido" apunta a permitir a los ciudadanos eliminar información específica sobre ellos de los buscadores, o de toda la red. Sin embargo, la regulación no ha sido bien definida debido a la enorme dificultad técnica de implementar algo como eso, además de las consecuencias legales que tendría[118].

118 Vint Cerf attacks European Internet policy *(The Telegraph). Disponible en: www.fayerwayer.com/2012/03/vint-cerf-critica-el-derecho-al-olvido-en-Internet*

La **opción simplificada** es otra propuesta que permea en Estados Unidos, a fin de que las compañías simplifiquen las opciones del consumidor, conforme a los siguientes conceptos:

- No es necesario otorgar una opción antes de recabar y usar datos personales para prácticas consistentes en una transacción o en la relación entre la compañía y el consumidor, o las requeridas o autorizadas por la ley.
- Para prácticas que requieren una opción por parte del consumidor, las compañías deben ofrecer la elección al momento y en el contexto en el cual el consumidor realiza la decisión acerca de sus datos. Las compañías deben obtener el consentimiento expreso de los consumidores antes de usar sus datos de manera diferente a los propósitos con que fueron obtenidos; o para obtener información sensible para ciertos propósitos.

Igualmente se está exigiendo mayor **transparencia**, y al efecto se pide a las empresas que:

- Los avisos de privacidad sean más claros, cortos y estandarizados para una mejor comprensión y comparación de sus prácticas de privacidad.
- Las compañías provean a los consumidores acceso razonable a sus propia información, dicho acceso debe depender de la sensibilidad de los datos o la naturaleza del uso.
- Todos los interesados incrementen sus esfuerzos para educar a los consumidores sobre las prácticas comerciales en materia de privacidad.

La FTC también ha hecho un llamado al Congreso norteamericano para considerar estos principios como base de una legislación en materia de privacidad y está exhortando a la industria a acelerar el paso en materia de autorregulación. Y para implementar este marco normativo dicho organismo se centrará en cinco áreas:

1) Estimular una política dirigida a las empresas consistente en "No realizar seguimiento" (Do not track).
2) Mejorar las políticas de privacidad en dispositivos móviles, debido a que en los últimos años ha aumentado su uso y capacidades.
3) Llamar a los consultores (Data Brokers) a cumplir con estándares de privacidad para incrementar la transparencia de sus servicios.
4) Extender su trabajo a los grandes proveedores de plataformas, tales como proveedores de servicios de Internet, desarrolladores de sistemas operativos, buscadores y redes sociales, con el objetivo de incrementar sus niveles de privacidad a favor de los consumidores.
5) Promover la autorregulación con la creación de códigos vinculantes (enforceable).

Acerca de este último punto, el Departamento de Comercio con el apoyo de los principales actores de cada industria han comenzado un proyecto para facilitar el desarrollo de **códigos de conducta para sectores específicos**. La Comisión ha visto este esfuerzo de manera favorable y llama a las compañías, asociaciones y empresas de autorregulación a adoptar los principios contenidos en el marco normativo.

Ahora bien, ante la complejidad planteada, la Casa Blanca emitió recientemente un estudio llamado "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the

global digital economy"[119], el cual incluye los Consumer Privacy Bill of Rights, que son principios para proteger los datos personales y tienen por objetivo pasar al Congreso para ser ley, o bien servir de base para la elaboración de códigos de conducta. Con el objetivo de reforzar su normativa fueron propuestos cuatro ejes:

1.- Implementar los Consumer Privacy Bill of Rights. Éstos consisten en:

- Control individual: Los consumidores tienen derecho sobre qué información otorgar y cómo debe usarse.
- Transparencia: Los usuarios tienen derecho a saber de forma sencilla y comprensible cómo serán utilizados sus datos personales, así como sus prácticas de seguridad.
- Respeto al contexto: Las compañías deben utilizar los datos personales de sus clientes de acuerdo al contexto en el que les fueron otorgados.
- Seguridad.
- Acceso y precisión: Los usuarios deben tener acceso a sus datos y poder modificarlos.
- Centrar la recolección: Los consumidores tienen derecho a que se recabe y almacene sólo la información razonablemente necesaria.
- Rendición de cuentas: Es el derecho de los consumidores de saber que sus datos son manejados conforme a los Consumer Privacy Bill of Rights.

119Disponible en http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

2.- Crear códigos de conducta consolidados por medio de consultas públicas acorde con los Consumer Privacy Bill of Rights. Esto implica que la Administración debe alentar a las compañías, grupos de industrias, defensores privados, grupos de consumidores, víctimas, académicos, empresas internacionales, autoridades locales, y en general cualquier otro grupo relevante interesado en el proceso de desarrollar códigos de conducta que implementen los principios generales. Estos tipos de consultas son flexibles, rápidas y lo suficientemente especializadas para dar soluciones creativas a diversos problemas.

También es de recalcar que son los mismos actores no estatales quienes tienen el control y poder de decisión en estos foros, ya que la autoridad sólo interviene como otro interesado para lograr la transparencia y apertura que merece el proceso, de tal forma que el resultado sólo es vinculante en tanto la empresa se obligue por sí misma a cumplir con el código de conducta discutido.

El procedimiento descrito tiene dos propósitos: primero generar confianza entre todos los involucrados, especialmente sus consumidores; y en segundo lugar si la FTC comienza una investigación por violentar la privacidad de los usuarios tomará favorablemente que se hayan adherido a un código con el procedimiento de consulta pública.

3.- Reforzar a la FTC como autoridad encargada de prohibir las conductas que estén en contra de los derechos de los consumidores. La FTC tiene diversas facultades para proteger los datos personales de los usuarios, por lo que a criterio de la Administración debe ser quien fomente la creación y desarrollo de los

modelos de autorregulación basados en los Consumer Privacy Bill of Rights a través de las consultas públicas propuestas.

4.- Incrementar la interoperatibilidad global entre Estados Unidos y otros sistemas jurídicos a través del desarrollo de modelos de privacidad con un proceso de consulta, y reforzando la cooperación para eliminar las barreras para el intercambio de datos. Las empresas que realizan flujo transfronterizo de datos deben enfrentarse al cumplimiento de múltiples jurisdicciones, ya que existe poca armonía entre las leyes extranjeras.

Sin embargo es necesario el reconocimiento mutuo entre países, es decir, tomar en consideración los sistemas jurídicos con los que se convive. Esto se materializa con acciones y mecanismos que demuestren el grado de cumplimiento de los mecanismos de autorregulación.

Los esfuerzos en este ramo han sido con la Asia-Pacific Economic Cooperation's (APEC), ya que las empresas que tienen códigos de conducta apegados a sus parámetros suelen ser quienes tienen presencia en muchos países de la región; de igual manera con la Unión Europea a través del programa de Safe Harbor para el flujo transfronterizo de datos.

Ahora bien, las propuestas de la Casa Blanca en relación con las facultades de la FTC es que sea la encargada de revisar los códigos de conducta para determinar si están de acuerdo a la legislación, que los someta a consulta y garantizar un mecanismo de revisión de los códigos con el propósito de ajustarse a las nuevas tecnologías. Además, la Casa Blanca sugiere que

aquellas empresas adheridas a un código aprobado por la FTC se les otorgue la garantía de lugar o puerto seguro o “safe harbor”.

7.3 Transferencia de datos EU – UE

Ahora bien, en cuanto a la transferencia de datos entre Estados Unidos y la Unión Europea, la Directiva 95/46/CE de la Unión Europea (UE) prohíbe la transferencia de datos personales con países que no cuenten con un marco legal adecuado que garantice una protección similar a la de la Unión; por ello, el Departamento de Comercio de Estados Unidos adoptó los “Safe Harbor Privacy Principles” con ayuda de la UE para garantizar que las empresas estadounidenses cumplan con los requisitos europeos120.

Estos principios son: notificación, elección, “onward transfer”, seguridad, integridad de información, acceso y “enforcement”. Una vez que una empresa adopte un modelo de autorregulación de conformidad con los Safe Harbor Privacy Principles puede pedir su certificación al Departamento de Comercio.

Para obtener este sello de confianza la empresa debe asegurarse que esté en la jurisdicción de la FTC o del Department of Transportation y revisar que su política de privacidad esté conforme los Safe Harbor Privacy Principles. Además debe establecerse un programa de solución de controversias independiente, para ello puede optarse por una empresa certificadora (por ejemplo: TRUSTe, BBB OnLine) o bien por una autoridad europea (European Union Data Protection Authorities).

120 http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf

Finalmente es necesario designar un encargado (contact point) que sea el vínculo con el programa de Safe Harbor. El sello tiene una vigencia de un año. En la actualidad más de 2,700 empresas son parte del programa de flujo transfronterizo de datos con la Unión Europea[121]. Existe un procedimiento similar respecto a la transferencia de datos entre Estados Unidos y Suiza.

En opinión del Departamento de Comercio el sello de confianza otorgado para el flujo transfronterizo de datos entre Estados Unidos y la Unión Europea ha sido un éxito, ya que las personas que cuentan con esta certificación suelen cumplirlo, lo que no impide a la autoridad de iniciar un proceso en contra por violentar el modelo[122].

Pero una problemática a la que se ha enfrentado la autoridad es el engaño de las empresas, ya que sólo dura un año la vigencia del sello por lo que siguen utilizándolo luego de que expira. Como sanción a estas empresas se les prohíbe la participación a cualquier programa de seguridad o privacidad[123].

121 Véase White House, nota 1 *supra*, pág. 33.

122 Véase Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" pág. 44
http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf

123 Véase nota 4 supra, pág. 18.

7.4 Childen's Online Privacy Protection Act

Respecto a la protección de datos de menores, la Childen's Online Privacy Protection Act (COPPA) protege los datos personales de los menores de 13 años. Por lo que limita su uso y requiere el consentimiento de los padres para que sus datos sean obtenidos. Además faculta a la FTC para aprobar los lineamientos de los esquemas de autorregulación. Estos lineamientos deben estar acorde con la Ley. La FTC tiene 180 días para emitir su resolución[124].

Conforme a la COPPA, la FTC es quien emite la legislación secundaria para su regulación e implementación[125] por lo que emitió la Children's Online Privacy Protection Rule. De acuerdo con el Children's Online Privacy Protection Rule[126] los criterios que debe tomar en cuenta la FTC para la aprobación de lineamientos son:

- Otorgar un nivel de protección mínimo conforme a la Ley.
- Garantizar un mecanismo independiente para la revisión de los lineamientos.
- Incentivos para el cumplimiento del esquema de autorregulación, como: reportes públicos de quienes incumplan, un recurso de los consumidores, contribuciones voluntarias al Departamento del Tesoro de Estados Unidos en conexión con un programa de la industria por violar las directrices, remisión a la FTC de quien viole los lineamientos.

124 Véase sección 1304 de la Childen's Online Privacy Protection Act.
125 Véase sección 1303, (a) de la Childen's Online Privacy Protection Act.
126 Véase sección 1312.10 http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=f7fecb0438482fc957bf76f12d726c6f&rgn=div5&view=text&node=16:1.0.1.3.36&idno=16

A esta fecha, la FTC ha aprobado 5 lineamientos: Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus, Inc., ESRB Privacy Online, A Division of the Entertainment Software Rating Board (ESRB), TRUSTe, Privo, Inc y Aristotle International Inc.[127]

Bajo este esquema de autorregulación la FTC aprueba los lineamientos de una empresa certificadora. Para esto es necesario presentar una solicitud a la FTC, quien hará una consulta pública y tomará nota de los comentarios en su decisión.

Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus

El primer lineamiento que aprobó la FTC fue el de la Children's Advertising Review Unit (CARU) of the Council of Better Business Bureaus[128]. Esta organización tiene por objeto regular la publicidad dirigida a menores por medio de monitoreo y revisión de la publicidad directa a menores.

Los lineamientos son dirigidos a los contenidos de todos los medios. De acuerdo a sus lineamientos, sus principios son129:

- Tomar en cuenta la capacidad, "sofisticación" y madurez del menor.
- No utilizar de forma "prejuiciosa" la imaginación de los niños y niñas.
- Comunicar información veraz y con lenguaje acorde con la edad de los menores.

127 Véase https://business.ftc.gov/content/safe-harbor-program (visto en junio de 2012).
128 Véase "Letter to Children's Advertising Review Unit (BBB) Approving CARU Program" en http://www.ftc.gov/os/2001/02/caruletter.pdf
129 Disponible en http://www.ftc.gov/privacy/safeharbor/caruselfreg.pdf

- Promover valores positivos como el bienestar social, amistad, bondad, honestidad, justicia y generosidad respecto a otros.
- Tomar acciones, incorporar a minorías y otros grupos en "situación de vulnerabilidad" para incorporar positivamente a cada persona en su rol social; así como eliminar los estereotipos y prejuicios.
- Reforzar la figura de los padres como guías de los niños y niñas.

La publicidad no debe ser engañosa, y debe ser presentada con claridad respecto al uso, características, seguridad, precio y edad recomendada. Las ofertas deben evitar las palabras que denoten urgencia como "sólo" (only) o "ahora" (now).

Ahora bien, respecto a la protección de los niños y niñas en línea, las páginas de quien adopte los lineamientos CARU debe evitar incluir links a otras páginas que no estén conforme a estos lineamientos.

Los anunciantes que se comuniquen con los niños a través de correo electrónico deben asegurarse que los padres puedan monitorear la actividad que realizan. Respecto a la los datos personales de los padres, los anunciantes sólo pueden conservarla para obtener el consentimiento en los casos previstos por la Ley y el Reglamento.

En cuanto las ventas por internet se debe contar con la autorización de los padres, ya que en caso de no obtenerse dicha autorización debe reembolsarse la cantidad sin ningún cargo; además muchas legislaciones locales no obligan a los padres a pagar por negocios jurídicos realizados con sus hijos.

En caso de realizar una transacción comercial debe comunicarse claramente, contar con un "botón" que diga "click here to order" o similar y tener un mecanismo para cancelar la orden.

Para la obtención de datos personales estos son los lineamientos:

- Mostrar claramente los usos y política de protección de datos personales, con una liga que pueda ayudar a los padres a obtener mayor información al respecto.
- En caso de que la información del menor sea publicada (publicly posted), por ejemplo, para interactuar con otros niños, debe obtenerse el permiso "autentificado/verificable" (prior verifiable parental consent) de los padres.
- Contar con el permiso "autentificado/verificable" (prior verifiable parental consent) de los padres en caso de compartir información personal del menor a terceros; no se considera tercero a aquellos agentes o afiliados que presten servicio y soporte a la empresa de manera interna.
- Si los datos personales no serán mostrados el permiso de los padres podrá realizarse por medio de correo electrónico en adición con algún medio adicional para asegurarse de la identidad del padre.
- Cuando la información de contacto es requerida y almacenada para hacer contacto en más de una ocasión es necesario contactar con los padres para obtener que elimine o modifique los datos.

Además:

- Debe existir un anuncio previo a obtener datos personales para obtener el consentimiento de los padres. Ejemplo: "You must ask your

Mom or Dad if you can answer these questions".

- Debe advertirse al menor en un lenguaje claro y comprensible el uso que se le dará a su información. Ejemplo: "We'll use your name and email to enter you in this contest and also add it to our mailing list".
- Mostrar tanto a los niños y niñas como a los padres si los datos personales serán obtenidos de forma pasiva (navigational tracking tools, browser files, etc.).
- Especificar cuál será el nombre mostrado a otros (alias, nombre, e-mail, etc.).
- Anunciar claramente y de forma comprensible si los datos solicitados son opcionales; y asegurarse de recolectar sólo los necesarios para llevar a cabo la actividad de la empresa.
- Tener la oportunidad de elegir si recibir comunicación o no por correo electrónico, tanto de los padres como del menor.

ESRB Privacy Online

Los lineamientos de la ESRB Privacy Online[130] se componen de principios relativos al uso de datos personales que deben acatar sus afiliados, y son: notificación del uso dado a los datos, elección del usuario respecto al uso de sus datos, límites a la obtención y retención de datos (en tanto sea necesario para el proveedor y obtenidos por medios legales), seguridad, acceso, mecanismos de ejecución, y políticas conforme a la Ley.

130 http://www.ftc.gov/privacy/safeharbor/esrbpopg_rev.htm

Las empresas afiliadas obtienen el certificado ESRB Privacy Online Children's Certification Seal; éste sello de confianza debe estar disponible en todos los sitios que recaben información personal de niños menores de 13 años, así como en la página de inicio. Dicho sello debe ser un link que lleve a otro sitio donde se encuentre la siguiente información: datos de contacto, tipo de información que se colecta, uso de los datos personales, uso de terceros y aprobación de los padres, límites de obtención de datos y acceso de los padres.

Respecto al permiso de los padres las empresas afiliadas deben informar el uso que se dará a los datos personales, y tener mecanismos para verificar la autenticidad del permiso. Estos mecanismos pueden consistir en: recibir la firma por correo o fax, uso de tarjeta de crédito, llamada telefónica con la compañía, firma digital, o correo electrónico acompañado de una contraseña previamente otorgada por alguno de los medios anteriores. Las excepciones a este permiso son: obtener el consentimiento de los padres, si sólo se hará contacto una vez, requerimiento constante, proteger la seguridad del menor, y proteger a otros.

La ESRB Privacy Online ofrece como parte de sus servicios asesoría para crear o adaptar las políticas de privacidad de sus afiliados.

El proceso de auditoría se compone de una “auto evaluación” y una auditoría de la ESRB, la ESRB Privacy Online Onsite Audit, que verificará anualmente las prácticas de la empresa afiliada.

Este modelo de autorregulación además ofrece un programa de refuerzo para garantizar la aplicación de sus lineamientos, el Sentinel Program. En primer lugar el Sentinel Monitoring and Verification es una revisión trimestral del sitio web; este monitoreo no es anunciado a la empresa, y es llevado a

cabo por especialistas (specially trained online monitors) que metódicamente realizan una revisión página por página. En caso de detectar alguna irregularidad, el "monitor" lo incluye en su reporte, y un Compliance Manager evaluará la situación y requerirá información al afiliado. Si la ESRB Privacy Online advierte violaciones a los lineamientos se notificará por escrito a la empresa acerca de las sanciones, que pueden ser imposición de multas, retiro de la ESRB Privacy Online Children's Certification Seal o remisión a la Federal Trade Commission.

El segundo mecanismo de refuerzo es el Sentinel Spot Checks, consistente en la revisión aleatoria de un sitio, en la cual un Monitor crea una personalidad ficticia y evalúa las prácticas del sitio. Por último, el tercer mecanismo de refuerzo es el Sentinel Consumer Online-Hotline, en el cual la ESRB Privacy Online ofrece a los usuarios un servicio de quejas atendidas vía telefónica o en línea a quienes aleguen la violación a su privacidad.

Finalmente los lineamientos de la ESRB Privacy Online incluyen la obligación de implementar un mecanismo de solución de controversias interno, mismo que si el cliente no estuviere satisfecho del resultado pueda ser remitido al ESRB Privacy Online's Alternative Dispute Resolution.

TRUSTe Children´s Privacy.

TRUSTe Children's Privacy Program es el tercer Save Harbor autorizado por la FTC bajo la COPPA[131].

[131] Disponible en http://www.ftc.gov/privacy/safeharbor/truselicenseagreement.pdf

Por lo que respecta a TRUSTe, sus lineamientos se muestran a manera de un contrato, razón por la cual especifica los términos en que debe ser usado su logo o marca para no incurrir en violaciones a sus derechos de autor. Contiene reglas muy amplias sobre la contratación, costos, terminación o renovación de la licencia. La empresa tiene 30 días para decidir si desea estar en la lista de contactos.

Este contrato está acorde con la legislación de California y la jurisdicción respecto a un conflicto será una Corte local o federal donde TRUSTe tenga sus oficinas principales. En dado caso que esto último no suceda se procurará buscar una jurisdicción en la que no se incurran en gastos excesivos para el litigio.

El Site Coordinator es designado por la empresa, es el encargado de implementar el TRUSTe Children's Privacy Program y ser el enlace entre la empresa y TRUSTe. El Account Manager es designado por TRUSTe y es quien mantiene la comunicación con el Site Coordinator. El Coordinators' Site es el sitio en el cual se mantienen los datos de la empresa. En la Self-Assessment Sheet una persona de confianza de la empresa deberá testificar y firmar sobre las prácticas de privacidad; la Self-Assessment Sheet servirá de base en el monitoreo/auditoría.

Aviso de Privacidad: El aviso de privacidad debe ser aprobado por TRUSTe y ser reflejo de las prácticas de privacidad, sin ser confuso o contradictorio. Debe contener:

- El tipo de información que recolecte.
- La forma de recolectar la información, ya sea por medios pasivos o activos.

- Qué información será utilizada.
- No limitar el uso del sitio a recabar más datos personales a menos que sea necesario.
- La forma en que debe darse el consentimiento de los padres, así como los casos en que transmiten los datos a terceros y la forma de hacerse efectivo ese derecho.
- La manera de que los padres revisen, modifiquen o eliminen la información personal del niño.
- Los datos de la empresa y el contacto en caso de inconformidad de los padres.
- Condiciones de uso y seguridad de los casos en que los datos personales se transferirán a un tercero.
- La indicación de que se utiliza una licencia de TRUSTe, cómo se accede a una certificación y el uso de la marca TRUSTe.
- La información de contacto de TRUSTe.
- Los procedimientos de seguridad en caso de acceso, modificación o uso sin autorización.
- El hecho de que el manejo de los datos personales recabados son regulados, y puede contraer sanciones a la empresa.
- El procedimiento para modificar la política de privacidad, los avisos para ello y la obtención del permiso de los padres.
- En caso de co-propiedad (co-branded) indicar quién es el encargado de recabar los datos.

El link al aviso de privacidad debe ser claro y estar en la página de inicio, o en cualquier sitio en la que se recaben datos personales. En caso de tener un sitio para niños el link debe estar ahí. El aviso debe estar en el servidor de la empresa y notificar la URL a TRUSTe, y avisar con dos días de anticipación en caso de cambio.

Respecto al aviso de privacidad debe ser un hipervículo o “botón” que diga “Privacy Statement” y dirija a otro sitio. Este link debe ser mínimo de tamaño 10 en concordancia con el sitio. La marca de verificación estará en la parte superior del aviso de privacidad, que consiste en un hipervínculo a un sitio en el servidor de TRUSTe que garantiza la autenticidad del sello de confianza.

Las prácticas a las que deben adherirse son acordes con la COPPA, es decir, es necesario el permiso de los padres para la obtención de datos personales de menores de 13 años, y tener un mecanismo de verificación [igual al descrito arriba]. Además de poseer mecanismos de seguridad, acceso de los padres, limitación en uso, muestra y recolección de datos. Los cambios de personal encargado, o contacto de la empresa deben ser notificados con anterioridad.

En cuanto a las auditorías se realiza una revisión cuando inicia la licencia, se revisa la política de privacidad, la práctica y la Self-Assessment Sheet. Luego de esto se sugiere qué cambios podrían realizarse para estar conforme a los lineamientos de TRUSTe y la COPPA. Este mismo procedimiento es el que se instrumenta anualmente. Luego de recibir la licencia se realizan monitoreos espontáneos que revisan las prácticas de la empresa (Ongoing Periodic Monitoring). La licencia incluye el seguimiento de las quejas recibidas (Online Community Monitoring), y la posibilidad de iniciar una investigación exhaustiva si existe suficiente evidencia que se ha trasgredido el esquema de autorregulación (Escalated Investigations).

Para las autorías es necesario que la empresa permita a TRUSTe o tercero independiente acceso ilimitado al sitio y razonablemente a sus bases de datos. Cualquier solicitud debe proporcionarse en un plazo de diez días. Además la empresa se compromete a reintegrar los costos que cause una

queja de algún cliente en tanto se compruebe que es resultado de una práctica contraria a los lineamientos.

Las sugerencias realizadas por TRUSTe a la empresa en relación con una queja del usuario deberá acatarla, y de no hacerlo podrá revocar el contrato. También podrá informar a la FTC o hacer público la naturaleza del incumplimiento.

Privo

Privacy Vaults Online, Inc., d/b/a Privo es una empresa que se encarga de promover relaciones responsables entre el cliente y las empresas a través de la plataforma PrivoLock™ system, destinada a comprobar la identidad de los usuarios[132]. El Privacy Assurance Program de Privo se enfoca en auxiliar al manejo de datos personales de menores acorde con los parámetros de la OCDE, la COPPA y la Rule.

Las compañías que decidan adherirse al Privacy Assurance Program y cumplan con los requisitos se les otorgará un sello de confianza, el Privo's Seal of Approval; así los visitantes podrán corroborar la autenticidad al dirigirse a un sitio de verificación en el servidor de Privo (click to verify). Como parte del programa, Privo otorga asistencia para la elaboración y modificación de avisos de privacidad.

132 http://www.privo.com/about_us.htm

La auditoría se compone de las siguientes etapas: Primero la empresa realiza una auto-evaluación respecto a las prácticas sobre la obtención, uso y muestra de datos personales en un formulario. Un representante del programa revisa el formulario de auto-evaluación para asegurarse de que esté acorde con el programa y la COPPA, en caso de que sus prácticas no sean adecuadas se realizan las observaciones correspondientes. Este mismo procedimiento se repite anualmente.

Trimestralmente se realiza un monitoreo sistemático sobre el sitio web que revisa el sello de confianza, el aviso de privacidad, y en general todos los requerimientos del programa. Otro método del programa es la "siembra" (seed) periódica de información falsa para corroborar que el uso dado a los datos personales del menor sean acorde con los lineamientos y la ley. Todos los datos de las auditorías son guardados por un periodo de tres años.

Finalmente el sistema de quejas o preguntas de usuarios es atendido por Privo, que les da seguimiento. Puede consistir en el enlace con el personal de la empresa o en el programa de solución alternativa de conflictos.

Los principios son:

Notificación: Los sitios deben tener un aviso de privacidad, con un link en la prágina de inicio y en todos los sitios donde se colecten datos personales. Debe ser claro y comprensible, sin ser confuso o contradictorio. Debe contener información de contacto, tipo de información recabada, uso y muestra de datos personales, información del responsable de información, restricción de colecta, acceso y forma de realizar quejas.

Consentimiento de los padres y autenticidad del permiso conforme a la Ley. Modificación de información. Seguridad. Los miembros deben tener un responsable de implementar el Programa de privacidad.

Uno de los grandes atractivos del programa es el software PrivoLock™ system, que consiste en un método para verificar la autenticidad del permiso de los padres. Tiene cinco métodos de verificación, tres en línea y dos off-line. Los mecanismos en línea son: los últimos cuatro dígitos del número de seguridad social, verificar la licencia de manejo y utilizar una tarjeta de crédito en conexión con una transacción. Los métodos off-line son: imprimir un formulario, firmarlo y mandarlo por fax o correo; y realizar una llamada para otorgar el consentimiento.

La página abre un "puerto" (gate) en el que se solicita la fecha de nacimiento, y de comprobarse que el menor tiene menos de 13 años se solicita el permiso de los padres por alguno de los métodos descritos.

7.5 Diagnóstico del modelo de protección a datos personales de menores

A siete años de poner en marcha la legislación de protección de datos de menores obtenidos por internet la FTC realizó en 2007 un informe al Congreso para evaluar su función. En esa ocasión sugería no realizar modificaciones a la *Act* ni a la *Rule*[133]. En el informe citado la FTC asegura que los dos objetivos de su programa "safe harbor" son promovidos, el primero fomentar la autorregulación, que en opinión de la Comisión responde de forma más rápida y flexible que la regulación tradicional en concordancia con las necesidades de la industria y de los consumidores en la dinámica del

133 Federal Trade Commission, Implementing the Childen's Online Privacy Protection Act, a Report to Congress. Disponible en http://www.ftc.gov/oia/ftccoppareport.pdf Pág. 1

mercado. El segundo objetivo consistente en el monitoreo constante de las empresas certificadoras también fue satisfecho[134].

Se ha considerado que los esquemas de autorregulación auxilian a la FTC a implementar la ley al realizar acciones tales como monitorear el Internet, educar a los operadores y consumidores, así como mostrar los sitios que no cumplen con los esquemas[135].

La FTC notó un incremento sustancial en el uso del Internet por parte de los niños. Para 2004 el 74% de los niños entre 8 y 18 años tenían acceso al Internet desde sus casas y los niños entre 8 y 10 años pasaban 25 minutos en línea.

En cuanto a las sanciones la FTC ha ganado 3.2 millones de dólares en demandas civiles[136]. La razón principal ha sido utilizar los datos de los menores sin el permiso de sus padres.

Respecto a las nuevas tecnologías destacan las redes sociales, ya que los datos expuestos en esas páginas pueden ser vistos por otras personas. Por esa razón la FTC ha emitido recomendaciones para los usuarios en los que sugieren ser precavidos con sus datos que muestren en redes sociales[137]. De igual manera el uso de teléfonos celulares con Internet ha presentado un mayor uso por parte de menores.

134 *Ídem.* Pág. 22
135 *Ídem.* Pág. 23
136 Véase el informe de la Federal Trade Commission "An examination of children's privacy: new technology and the children's online privacy protection act", 29 abril 2010, pag. 5 http://www.ftc.gov/os/testimony/100429coppastatement.pdf
137 Véase www.ftc.gov/opa/2006/05/socialnetworking.htm y http://onguardonline.gov/articles/0012-kids-and-socializing-online

En el informe del 2010 ya mencionado, la FTC sugirió al Congreso otorgar protección a los adolescentes entre 13 y 18 años, ya fuera con la ampliación del rango de protección de la COPPA, o con una legislación especial. Ampliar la cobertura de la ley sería complejo, ya que existe una gran diferencia de comportamiento en línea y uso del Internet, incluso limitar el uso a este sector de la población podría ser contrario a la constitución por restringir su libertad de expresión y el derecho a recibir información.

Es por ello que propone crear una ley para proteger los datos personales de los adolescentes[138].

En cuanto a la protección que brinda la COPPA ha preocupado expandir su ámbito, ya que hay más medios digitales por los que pueden extraerse datos personales. Es por ello que una noción más amplia del significado de Internet ha podido abarcar a dispositivos móviles, televisión interactiva, o juegos interactivos.

Otro medio al que la FTC ha prestado atención son las aplicaciones (apps) para teléfonos inteligentes y tablets por su alto desarrollo en las últimas décadas. En 2008 sólo existían 600 de estas aplicaciones, mientras que en la actualidad hay más de 500,000 en la Apple store, y otras 380,000 en el Android Market, las cuales son descargadas más de 28 mil millones de veces. De éstas hay 8,000 en la Apple Store y 3,600 en la Android Market que se relacionan con la palabra “kids”[139].

138 Véase el informe de la Federal Trade Commission, “Protecting youths in an online world”, 15 julio 2010, http://www.ftc.gov/os/testimony/100715toopatestimony.pdfg

139 Véase el informe de la Federal Trade Commission, “Mobile Apps for Kids: current privacy disclosures are disappointing” pág.1 http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Al respecto la Comisión recomienda a las tiendas en línea agregar un apartado que muestre si la aplicación por descargar está bajo la reglamentación de la COPPA, es decir, estandarizar un ícono que sea mostrado dentro de las características de la aplicación. Aunado a ello los desarrolladores de aplicaciones deben explicar en un lenguaje más claro que sea comprendido por los niños cómo serán utilizados sus datos personales.

7.6 Servicios financieros

Las autoridades en la materia son el Consumer Financial Protection Bureau (CFPB) y la FTC. La Fair Credit Reporting Act (FCRA) es la ley que regula las prácticas de las "consumer reporting agencies", estas agencias se encargan de recabar información que afecten a los consumidores, primordialmente para registrar si una persona es apta para recibir un crédito o un empleo. Respecto a tecnologías de la información esta Ley prevé la obtención de datos personales por medios digitales[140]. Algunos de estos datos personales son nombre, dirección, antecedentes penales o información médica[141].

Además la Right to Financial Privacy Act protege a los usuarios de servicios financieros de las injerencias arbitrarias del gobierno para obtener sus datos personales de los bancos.

Aunado a estos ordenamientos la Gramm-Leach-Bliley Act es la ley que protege los datos personales de los usuarios de servicios financieros. Las obligaciones de los clientes es dar su aprobación de la política de privacidad, y debe darse la oportunidad a los clientes de dar su negativa en ciertos

[140] Véase Sección 604 (b, 2, B).
[141] Véase Federal Trade Commission. FTC Issues Report: "Forty Years of Experience with the Fair Credit Reporting Act", pág. 1. Disponible en http://ftc.gov/os/2011/07/110720fcrareport.pdf

casos como: compartir información no pública con terceros no afiliados, para esto es necesario notificar con 30 días de anticipación; y ante cambios en la política de privacidad.

A la institución se le obliga a dar al cliente un aviso de privacidad cuando se establece su relación, mismo que tendrá vigencia de un año y está obligado a renovar. Además debe darse opción al ciente de no compartir información no pública con terceros afiliados, tiene 30 días para pedir la decisión del cliente y está obligado a respetar esa decisión. Si cambia la política de privacidad debe notificarlo y revisar la conformidad de sus clientes en caso que requiera optar por una opción de privacidad.

La información no pública es la información obtenida con motivo de proveer un producto o servicio. La ley señala como ejemplos de información no pública el hecho de que una persona es usuaria de un servicio financiero, nombre, domicilio, número de seguridad social, número de cuenta, cualquier información otorgada en un formulario, o información derivada de una "cookie".

Las notificaciones deben ser claras, comprensibles, y diseñadas para llamar la atención. En todas las notificaciones debe señalarse los datos no públicos a recabarse. El principal derecho consagrado en esta Ley es que el cliente tenga la oportunidad de negar la divulgación de sus datos personales (opt-out). Recientemente diversas compañías fueron advertidas por la FTC de que sus aplicaciones (apps) violaban la Fair Credit Reporting Act, ya que recolectaban información personal de los usuarios como sus antecedentes penales sin que lo supieran[142].

[142] http://www.ftc.gov/opa/2012/02/mobileapps.shtm

7.7 Otros Modelos de Autorregulación

En materia de de protección de datos personales está Health Insurance Portability And Accountability Act de1996.

La Cable Communications Policy Act of 1984 obliga a los provedores de servicios de televisión por cable a tener un aviso de privacidad que detalle el uso de información personal “localizable” (identifiable) (sec. 631).

También la Video Privacy Protection Act of 1988 protege los datos personales que identifiquen a los clientes (Personally identifiable information) de los vendedores de materiales audiovisuales precargados (video tape service provider), y sólo podrán hacer uso de ella bajo la autorización expresa del cliente.

Finalmente la “Genetic Information Nondiscrimination Act of 2008” prohibe la discriminación a los empleadores en caso de contar con información genética de sus empleados.

7.8 Problemáticas no contempladas por los modelos

Una de las problemáticas relacionadas con las TI es la aparición de nuevas formas de recabar información, razón por la cual es muy complicado regular esos campos. Por ejemplo, los negocios que dependen de capturar información personal, como son los software de seguimiento de comportamiento de usuarios, servicios de redes sociales o servicios móviles de localización.

Ejemplo de ello es el tipo de software que recaba información de manera pasiva, es decir, sin que el usuario tenga conocimiento. Para ello algunas empresas engañan a sus clientes para que descarguen un software que luego manda información personal como páginas visitadas, compras realizadas, movimientos bancarios, prescripciones médicas, listas de videos rentados o búsquedas de libros.

Para ello la FTC tuvo que construir un nuevo concepto de aplicaciones de rastreo como el software diseñado para instalarse en una computadora del consumidor y puede transmitir la información sobre actividades de la computadora donde es instalada y transmitirla a otra[143]. Por ello, en 2009 la FTC ordenó a la empresa Sears Holdings Management Corporation indemnizar con 10 dólares a todos sus clientes por engañarlos, ya que consideró que su aviso de privacidad no era el adecuado.

Esta misma dificultad ha sido observada en los software *peer-to-peer* (P2P) que comparten archivos entre usuarios, ya que recolecta el comportamiento del usuario sin que exista seguridad o conocimiento al respecto. Para ello la Comisión ha realizado labores de educación de usuarios sobre los riesgos de instalar este tipo de programas[144].

143"Tracking Application" shall mean any software program or application disseminated by or on behalf of respondent, its subsidiaries or affiliated companies, that is capable of being installed on consumers' computers and used by or on behalf of respondent to monitor, record, or transmit information about activities occurring on computers on which it is installed, or about data that is stored on, created on, transmitted from, or transmitted to the computers on which it is installed.
http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf

144 Véase nota 4 supra, pág. 50.

7.9 Cuadro, diagnóstico de la autorregulación en Estados Unidos

Esquema	Ventajas	Desventajas
Modelo laxo (autorregulación pura)	Se ajusta a las necesidades de cada industria.	Poca protección al usuario.
Códigos de conducta (sin intervención directa de la autoridad)	Incrementa la certeza, especificidad y dinamismo de las empresas.	No son conocidos por los usuarios.
Sancionar a las empresas ante el "daño"	➢ Abarca múltiples actividades como spam, "spyware" y telemarketing no deseado. ➢ Las sanciones no sólo son pecuniarias, sino obligan a las empresas a cambiar su forma de manipular los datos personales ➢	En ocasiones es complicado determinar cuándo se genera un daño.
Políticas de privacidad		➢ Son largas, complejas e incomprensibles para los consumidores. ➢ Las empresas limitan su responsabilidad frente su cliente con sólo informarlos acerca de cómo será usada su información. ➢ Los usuarios no tienen control de esas prácticas, por lo que pierden interés y dejan de ejercer sus derechos.
Sello de confianza otorgado por el Departamento de Comercio	➢ Más de 2,700 empresas están certificadas. ➢ Genera mucha confianza no sólo con los clientes, sino con los gobiernos.	Sólo dura un año, muchas empresas no lo renuevan y siguen trabajando con el sello caduco.
Sello de confianza de protección a niños	➢ Modelo muy completo, con protección al usuario y certificación con auditorías. El certificador debe estar validado por la autoridad. ➢ Sólo protege a los niños menores de 13 años.	La autoridad sólo ha validado a 5 empresas certificadoras.

VIII. MODELO INTEGRADO O MIXTO DE PROTECCIÓN DE DATOS Y AUTORREGULACIÓN

8.1 Generalidades

Dentro de un tercer grupo de esquemas de autorregulación, se observa una clara tendencia de los países hacia un modelo que, comprende, por un lado, una legislación más o menos comprehensiva sobre protección de datos personales, que a su vez incluye y reconoce modelos de autorregulación (*modelo mixto o integrado*).

De este modo, los países cuentan con una legislación sobre protección de los datos personales que reconoce y fomenta la adopción de mecanismos de autorregulación en el texto legal. Esto a su vez puede significar el otorgamiento de efectos jurídicos variados[145] a los mecanismos de autorregulación.

Como se especificará más adelante, México se encuentra dentro de esta categoría (ver artículo 43 y 44 de la LFPDPPP). Un enfoque similar se encuentra en Alemania[146], Argentina[147], Australia[148], Chipre[149], España[150], Grecia[151] Irlanda[152], Italia[153] Japón[154], Luxemburgo[155], Perú[156], Uruguay[157] y la UE[158].

[145] Los efectos jurídicos varían según la legislación de que se trate. Estos pueden ir desde la inscripción del mecanismo de autorregulación en un registro público, hasta la substitución de la ley.
[146] Sección 38 (a) de la Ley Federal de Protección de Datos.
[147] Artículo 30 de la Ley de Protección de Datos Personales
[148] Apartado III AA, Sección 18BB de la Privacy Act.
[149] Artículo 23 b) de la Ley de Procesamiento de Datos Personales de 2001.
[150] Artículo 32 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal
[151] Sección 2)19(1)(b) de la Ley 2472/1997 sobre la Protección de Individuos en relación con el Tratamiento de Datos Personales.
[152] Sección 13 de la Ley de Protección de Datos (reformada en 2003).
[153] Artículo 12 del Código en Materia de Protección de Datos Personales.
[154] Artículo 37 de la Ley de Protección de la Información Personal

De estos sistemas, en este apartado se comentan las características de esquemas generalmente adoptados, tales como códigos deontológicos, certificación y sellos de certificación.

8.2 Códigos de privacidad

En México, de acuerdo con el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, los esquemas de autorregulación *"podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos*". Y en el derecho comparado, se observa que los códigos de privacidad son el mecanismo de autorregulación más usual previsto hasta ahora en las legislaciones.

Estos reciben diferentes denominaciones (códigos de buenas prácticas, códigos de conducta, códigos deontológicos, códigos tipo, etc.); sin embargo, todos hacen referencia a normas de comportamiento adoptadas por los propios destinatarios de sus previsiones, ya sea sectores empresariales, asociaciones gremiales o profesionales.

Estos códigos -por lo general- se encuentran señalados en la Ley y son elaborados por las propias empresas, las asociaciones representativas o la industria. En muchos casos no son claros los efectos jurídicos que las legislaciones otorgan a estos códigos, o cuáles son los incentivos para

[155] Artículo 2 y 32 de la Ley sobre la Protección de las Personas en relación con el Procesamiento de Datos Personales de Agosto de 2002.
[156] Artículo 31 de la Ley de Protección de Datos Personales.
[157] Artículo 36 de la Ley de Protección de Datos Personales y Acción de "Hábeas Data"
[158] Directiva 95/46/CE de Protección de Datos Personales, artículo 27.

adoptarlos, ya que la mayoría de las legislaciones se limitan a señalar que estos serán “inscritos” o “registrados” ante la autoridad correspondiente.

En México no obstante, el artículo 81 del Reglamento de la LFPDPPP establece **incentivos para la autorregulación:**

> **Artículo 81.**Cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la Ley y el presente Reglamento, por parte del Instituto. Asimismo, el Instituto podrá determinar otros incentivos para la adopción de esquemas de autorregulación, así como mecanismos que faciliten procesos administrativos ante el mismo.

Hablando en general sobre la autorregulación, se argumenta que la autorregulación podría funcionar si existe interés por parte de los proveedores por crear una **reputación de buena calidad (incentivo reputacional)**, de tal manera que los consumidores confíen y compren el bien en el mercado, aminorando de esta manera el problema informacional[159].

En el rubro de la normalización y con el carácter de estímulo reputacional, el Reglamento de la Ley Federal de Metrología y Normalización, publicado en el Diario Oficial de la Federación el 14 de enero de 1999, prevé en su Título Sexto el estímulo consistente en el Premio Nacional de la Calidad:

> **ARTÍCULO 105.** El Premio Nacional de Calidad será un instrumento para promover, desarrollar y difundir la calidad de los procesos industriales, comerciales, de servicios y sus productos, con el fin de apoyar la modernización y competitividad de las empresas establecidas en el país.

[159] **Nuñez E., Javier y Lima, José Luis**, *Incentivos Reputacionales para la Autorregulación: Un Análisis Experimental*. Disponible en: www.econ.uchile.cl/uploads/publicacion/61f57e85-5657-4551-b53b-59a24c79baed.pdf

Por otro lado, en la materia ambiental, se fomentan programas de autorregulación y auditoría, otorgándose incentivos fiscales, a quienes participen en dichos programas[160]:

> **Artículo 62.-** La Secretaría fomentará **programas de autorregulación** y auditoría ambiental y promoverá la aplicación de incentivos fiscales, a quienes participen en dichos programas.
>
> El desarrollo de la auditoría ambiental es de carácter voluntario y no limita las facultades que esta Ley confiere a la autoridad en materia de inspección y vigilancia.

Hablando de los efectos jurídicos que pueden tener los códigos, se retoma el caso mencionado en entregas previas sobre las consecuencias "corregulatorias" que estos tienen en Australia. Conforme a los diez Principios Nacionales de Privacidad (NPPs por sus siglas en inglés)[161], la *Privacy Act* permite a las organizaciones crear y operar sus propios Códigos de Privacidad (*Privacy Codes*) los cuales, al ser aprobados por el Comisionado de Privacidad[162], sustituyen la aplicación de dichos principios.

Como se ha dicho, este modelo, que otorga cierta flexibilidad a las organizaciones en el cumplimiento de sus obligaciones, fue ideado como un mecanismo para favorecer la seguridad y la confianza de los consumidores y usuarios ya que permite a la industria y a sus clientes elaborar un marco de protección que se ajuste a sus necesidades. Este enfoque, en el que participan tanto los particulares como el Estado, ha sido denominado por la doctrina y las autoridades australianas como *corregulación*[163].

[160] Ley Ambiental del Distrito Federal. Publicada en la Gaceta Oficial del Distrito Federal el 13 de enero del 2000.
[161] Estos principios corresponden a las obligaciones de: 1) obtención 2) uso y revelación 3) calidad de la información 4) seguridad de la información 5) transparencia 6) acceso y corrección 7) identificador 8) anonimidad 9) Flujo transfronterizo 10) Información sensible. *Cfr.* Anexo 3 de la Privacy Act de 1988.
[162] Véase Apartado III AA de la Privacy Act.
[163] Véase *Revised Version of the Code Development Guideliness de Septiembre de 2001*.

De acuerdo con la Ley, el Comisionado de Privacidad sólo podrá aprobar un código de privacidad cuando éste: a) incorpore todos los Principios Nacionales de Privacidad, o bien, establezca obligaciones que sean al menos equivalentes; b) especifique aquellos sujetos obligados, o bien, señale la forma de determinarlos; c) sea voluntario; d) establezca el procedimiento por el cual una organización dejará de estar obligada por el código, y la fecha en que la cesación tomará efecto. Igualmente, el Comisionado deberá cerciorarse que el público haya tenido la oportunidad de comentar el proyecto de código de privacidad propuesto[164].

En el supuesto de que el código establezca procedimientos para el planteamiento y tratamiento de quejas, la autoridad deberá además corroborar que dichos procedimientos cumplan con los estándares y lineamientos que en su caso emita la Oficina del Comisionado de Privacidad. En todo caso, el código deberá establecer un procedimiento para la designación de un árbitro independiente (quien deberá tener atribuciones similares a las señaladas en la Ley para el Comisionado en el tratamiento de quejas) y obligar a los miembros del código a cooperar en las funciones del árbitro.

El Comisionado de Privacidad lleva un registro de todos los códigos de privacidad aprobados[165], quien además se reserva la facultad de revisar la operación de los mismos con la posibilidad de revocarlos en caso de encontrar alguna irregularidad.

Cabe señalar que en todos los casos el Comisionado de Privacidad posee la facultad de revisar o conocer sobre aquellas determinaciones emitidas por los árbitros en los que las partes no hayan quedado conformes. Asimismo,

[164] Véase Apartado III AA, Sección 18BB de la *Privacy Act.*
[165] Este registro puede ser consultado en http://www.privacy.gov.au/business/codes/register.

los Tribunales Federales pueden ejecutar las determinaciones de los árbitros o del Comisionado, o en su caso conocer y revisar las determinaciones del Comisionado de Privacidad, pero sólo para revisar que el procedimiento se haya llevado correctamente y no sobre la decisión de fondo.

8.3 Características de los Códigos Deontológicos

Del estudio realizado, se ha observado que los códigos de conducta (Deontológicos) presentan ciertas características fundamentales relacionadas con su operatividad que vale la pena destacar.

8.3.1 Representatividad

Una primera característica es la relativa a la representatividad**.** En Argentina, Alemania, Irlanda, Luxemburgo, Perú, Uruguay y la Unión Europea se establece claramente que los códigos deberán ser elaborados por Asociaciones o Entidades *representativas.*

De acuerdo con la Comisión Europea[166], este elemento puede resultar fundamental para la certeza y operatividad de los códigos, toda vez que ayuda a reducir el grado de confusión en que puede caer un consumidor o usuario frente a un sector o industria fragmentada. Aunado a ello, en el caso de algunos tipos de industrias, como el Marketing Directo, en donde la información es transmitida constantemente entre organizaciones del mismo sector, puede pasar que una empresa que revele información personal no esté sujeta al mismo código de la empresa que lo recibe.

[166] Comisión Europea, *Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero?*, adoptado por el Grupo de Trabajo sobre Protección de Datos de carácter personal el 14 de enero de 1998, DG XV D/5057/97 final.

En el caso de Australia por ejemplo, el Comisionado de Privacidad antes de aprobar cualquier código debe cerciorarse de que la organización solicitante haya llevado a cabo un proceso de consulta pública durante un tiempo adecuado (generalmente seis semanas) en donde se asegure que todos los sectores o interesados más relevantes hayan tenido la oportunidad efectiva de participar y hacer comentarios al código[167].

Por otro lado, en España, si bien es parte de la Unión Europea y regula la elaboración de códigos tipo, su enfoque se aparta de este principio ya que permite la adopción de códigos individuales[168].

No obstante, a la fecha, la mayoría de los códigos inscritos corresponden a asociaciones sectoriales.

En México, por otro lado, no parece haber una indicación que exija el cumplimiento de cierta representatividad como se advierte del artículo 79 del Reglamento:

> *"**Artículo 79.** De conformidad con lo establecido en el artículo 44 de la Ley, las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos personales, que complementen lo dispuesto por la Ley, el presente Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones. Asimismo, a través de dichos esquemas el responsable podrá demostrar ante el Instituto el cumplimiento de las obligaciones previstas en dicha normativa."*

[167] Véase *Revised Version of the Code Development Guideliness de Septiembre de 2001.*
[168] Artículo 72 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

8.3.2 Complementariedad

Otra característica que se presenta en la mayoría de los casos, es el carácter complementario de los códigos. En la mayoría de las legislaciones se observa que los códigos de conducta están destinados a facilitar o mejorar la aplicación de la Ley, así como el ejercicio de los derechos de los particulares (en México conocidos como derechos ARCO). Así lo prevén, por ejemplo Argentina, Alemania, Grecia, Luxemburgo, Perú y Uruguay.

La anterior característica está relacionada también con la *legalidad* ya que en la mayoría de los casos analizados, la autoridad puede denegar el registro de un código de conducta si este no se ajusta a las disposiciones legales aplicables; lo que es el caso del modelo adoptado por México[169].

El carácter complementario de los códigos se ve reforzado en muchos casos por la circunstancia de que los particulares pueden acudir a reclamar sus derechos conforme a la legislación vigente ante las autoridades correspondientes.

Ahora bien, en Australia la aprobación por parte del Comisionado de Privacidad de un código de privacidad, implica varios efectos jurídicos importantes:

En primer lugar, a las empresas que se encuentran sujetas por el código ya no les serán aplicables los Principios Nacionales de Privacidad establecidos en ley, sino aquellos que sean referidos en el propio código.

[169] Ver Artículo 86 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En segundo lugar, cualquier reclamación en relación con una violación a los derechos de particulares por parte de alguna de las empresas vinculadas al código tendrá que agotar primero los mecanismos de solicitud ante la propia empresa y los mecanismos de solución de controversias que en su caso prevea el código antes de poder acudir ante la autoridad correspondiente.

No obstante, en México no existe una disposición similar, por lo que podemos deducir que la adopción de un código de conducta por parte de un sector o una empresa, de ningún modo podrá limitar la posibilidad de los particulares de acudir ante el IFAIPD cuando no hayan agotado las vías alternativas que en su caso prevean los códigos.

8.3.3 Publicidad y Registro

Una característica que se presenta también en varias de las legislaciones es la *publicidad* y el *registro*. En un gran número de casos, como es Argentina, Alemania, Australia, España, Italia y Uruguay, las legislaciones prevén mecanismos para hacer públicos los códigos de conducta.

En el caso de Uruguay por ejemplo, existe un Registro Nacional de Protección de Datos Personales el cual entre sus funciones se encuentra la de inscribir "*Los códigos de conducta de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada".*

En Argentina, los Códigos de Conducta Homologados son publicados con su respectivo decreto en la página de la Dirección Nacional de Protección de Datos Personales[170].

[170] Tal es el caso del Código de Ética Homologado de AMDIA, véase http://www.jus.gov.ar/datos-personales/documentos/normativa.aspx

En Australia, de acuerdo con el Apartado III AA, Sección 18BG de la Privacy Act, se prevé que el Comisionado de Privacidad lleve un registro de los códigos aprobados. En la actualidad este registro se lleva mediante la página de Internet del Comisionado en donde se muestran los códigos vigentes, los códigos en trámite, así como los códigos revocados y las variaciones a estos[171].

En cuanto al procedimiento de *inscripción*, resulta muy ilustrativo lo dispuesto por el Reglamento de desarrollo de la Ley Orgánica 15/1999 de España, la cual regula el Procedimiento de inscripción de códigos tipo en el Titulo IX, capítulo VI.

En este sentido, establece que el procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

A dicha solicitud, deberá acompañarse:

a) La acreditación de la representación que concurra en la persona que presente la solicitud.
b) El contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.
c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa, certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

[171] Véase http://www.privacy.gov.au/business/codes/register

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.
e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.
f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

Una vez presentada la solicitud junto con la documentación requerida, el Registro General de Protección de Datos, durante los treinta días siguientes a la notificación, podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo. Transcurrido dicho plazo, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Reglamento.

Además, el Director de la Agencia Española de Protección de Datos puede acordar, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, la apertura de un período de información pública. En su caso, el plazo para la formulación de alegaciones será de diez días contados desde la publicación en el Boletín Oficial del Estado del anuncio correspondiente.

De acuerdo con el artículo 148 del Decreto, "*si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días*

introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos". Si el solicitante no da cumplimiento al requerimiento, se declarará la suspensión del procedimiento.

Ahora bien, en caso de que durante el trámite se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

De acuerdo con el propio Decreto, el plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar *estimada* su solicitud.

Finalmente, una vez aprobados los códigos, la Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

En el caso de México, el Reglamento prevé una disposición que se refiere al "registro de esquemas de autorregulación":

> **Artículo 86**. Los esquemas de autorregulación notificados en términos del último párrafo del artículo 44 de la Ley formarán parte de un registro, que será administrado por el Instituto y en el que se incluirán aquéllos que cumplan con los requisitos que establezcan los parámetros previstos en el artículo 43, fracción V de la Ley.

Sin embargo, la norma no establece un procedimiento con formalidades ni plazos; por lo que el IFAIPD deberá establecer reglas o lineamientos para complementarla.

8.3.4 Revisión

Otra característica que se ha advertido sólo en algunos casos es el establecimiento de procedimientos de *revisión.* En el caso de Australia, se establece que todos los códigos de privacidad aprobados deberán establecer un proceso de revisión de código que tenga lugar al menos *cada tres años*; contener una declaración por la cual se comprometan los recursos necesarios para la revisión del código; y requerir al Administrador del código que emita una contestación al reporte de revisión independiente y presentarla ante el Comisionado dentro de los 30 días siguientes a la finalización del reporte.

En España por su parte, se establece como una obligación posterior a la inscripción del código *"Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento. Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor".*

En el caso de nuestro país, ni la LFPDPPP ni su Reglamento contemplan términos o vigencias. En tal sentido, los parámetros que emitan la SE en coadyuvancia con el IFAIPD, deberán considerar esta cuestión, tomando como referencia el hecho de que un código debe ser de más largo plazo que un sello de confianza.

8.3.5 Revocación

En relación con la revocación de los códigos las legislaciones actuales no son muy explícitas al respecto, pero el caso de Australia es ilustrativo.

Cconforme a la sección 18BE del Privacy Act, el Comisionado tiene la facultad de revocar un código de privacidad previamente aprobado. La revocación puede ocurrir a iniciativa del Comisionado a petición del Administrador del código.

De acuerdo con los *Code Development Guidelines*, un código puede ser revocado por alguna de las siguientes causas:

- Falsedad de la información proporcionada durante el proceso de aprobación.
- Cambio de circunstancias sobre las cuales fue otorgado el código (por ejemplo, la introducción de controles legales, cambios tecnológicos, actitud de la comunidad, etc.)
- El Administrador no cuenta con los requisitos necesarios para ser autorizado.
- Las decisiones adoptadas por los árbitros son sistemáticamente revocadas en apelación por el Comisionado.
- Una vez que el Comisionado ha informado sobre un mal funcionamiento del código y el Administrador del código no ha adoptado medidas necesarias a fin de corregir los errores o estas han resultado infructuosas.

Cuando el Comisionado advierta alguna de estas situaciones, primero consultará con el Administrador del código a fin de solucionar el problema. Si este persiste, iniciará un procedimiento de revisión de contenido y operación del código el cual incluirá las observaciones de la Oficina de Privacidad, Administrador(es) del código y público interesado. El propósito de la revisión será definir claramente mediante consenso cualquier debilidad del código o su operación y proponer mecanismos para corregirlo.

En caso de no llegar a un acuerdo, el Comisionado de Privacidad iniciará el procedimiento de revocación, que consistirá en:

1) Elaboración de un plan de revocación conjuntamente con los interesados. El plan deberá considerar asuntos como el tiempo de la revocación, mecanismos idóneos para informar al público y la solución de cualquier queja que esté pendiente;

2) El Comisionado informará al público general sobre la intención de revocar el código y delimitará los tiempos y circunstancias para hacerlo;

3) Se notificará oficialmente al Administrador del código sobre la revocación.

En cada caso, el Comisionado evaluará la mejor forma de informar al público sobre la intención de revocar un código. Si la revocación tiene lugar a solicitud del Administrador, una forma podría ser el llevar a cabo una campaña pública donde se informe a los consumidores sobre la revocación del código y los efectos que esto podría tener en la protección de su información personal.

A la fecha sólo se tiene conocimiento de la revocación de un código, hecha en el año 2006 respecto del Código de Información General de Seguros que había sido previamente aprobado en 2002. Este código preveía en su cláusula 1.24 la revisión de la operación del código transcurridos tres años desde su adopción.

En Marzo de 2005, el *Insurance Council of Australia* (ICA) encargó la revisión del código, la cual fue completada el 4 de julio de 2005. La revisión independiente encontró que:

1) 24 organizaciones habían suscrito el código.
2) Durante tres años, el Árbitro recibió 5 quejas, y fue requerido a emitir una resolución sólo en tres de ellas.
3) Cada queja tenía un costo de 65,330 dólares australianos.
4) Durante el mismo periodo, la Oficina del Comisionado de Privacidad reportó 82 quejas sobre la industria de seguros.

En consecuencia, como resultado de los altos costos que representaba el código, el número reducido de quejas, y el relativamente poco seguimiento del código por parte de la industria, el *Insurance Ombudsman Service Ltd.* (IOS) respaldó la recomendación hecha por el Revisor, de revocar el código.

De acuerdo con la declaración explicativa[172], el Comisionado de Privacidad no participó directamente en el procedimiento de consulta para la revocación del código. No obstante, de acuerdo con la sección 18 de la Ley de Instrumentos Legislativos, hay ciertos casos en los cuales la autoridad puede determinar que su participación en la consulta es innecesaria o inapropiada.

[172] Véase Office of the Privacy Commissioner, Explanatory Statement: *Revocation of the General Insurance Information Privacy Code*, de 31 de enero de 2006.

La sección 18 (2) (e) provee algunos ejemplos de casos en los cuales puede acreditarse que se ha llevado un proceso de consulta apropiado sin la participación o conducción de la autoridad.

El procedimiento independiente de revisión implicó los siguientes pasos:

1) Se publicaron anuncios en prensa de circulación nacional. Se otorgó un plazo de más de 6 semanas para presentar observaciones durante la revisión.
2) Los miembros de ICA fueron notificados e invitados a comentar al respecto.
3) Los interesados más relevantes fueron contactados por escrito por el Revisor, quien les ofreció la oportunidad de presentar observaciones.
4) Se hicieron entrevistas a miembros de ICA tanto los que formaban parte del código como los que no.
5) Se entrevistó a los miembros del Comité de Cumplimiento de Privacidad.
6) Se entrevistó al personal clave del IOS.
7) Otras asociaciones relacionadas fueron contactadas en relación con sus arreglos industriales para lidiar con las quejas de privacidad. Por ejemplo, la Asociación de Banqueros de Australia, la Asociación de Servicios de Inversión y Financieros, Clubs Queensland y la Asociación Australiana de Casinos.
8) Se realizó una investigación de escritorio.

Finalmente, el Comisionado aprobó la revocación, la cual surtió efectos a partir del 30 de abril de 2006. De acuerdo con el Comisionado, para asegurar una transición (suave) en materia de tratamiento de quejas, las quejas presentadas bajo el código después del 31 de enero de 2006 deberían ser remitidas al Comisionado de Privacidad.

8.3.6 Contenido

En cuanto al *contenido* de los códigos se destaca primeramente que la Red Iberoamericana de Datos también se ha pronunciado en relación con los mecanismos de autorregulación y ha señalado que:

> "(…) resulta imprescindible que los instrumentos de autorregulación dispongan de herramientas que los hagan eficaces. Dentro de estos mecanismos se sugieren los siguientes: (1) Establecer medios ágiles, efectivos y gratuitos en caso de inobservancia del código para que la persona no sólo exija el respeto de sus derechos y libertades sino que se convierta en un "fiscalizador" de la gestión del administrador de sus datos personales (2) Consagrar mecanismos de control interno y externo de verificación del cumplimiento de los códigos, y (3) Prever sanciones por el incumplimiento de los códigos.

Asimismo, la Red Iberoamericana de Datos ha señalado que las medidas de autorregulación deben evaluarse desde dos perspectivas concomitantes: la objetiva y la funcional:

a) La primera busca determinar si el contenido de los mismos consagra un valor añadido y si es acorde con la regulación local o, en caso de inexistencia de la misma, con los principios internacionales sobre protección de datos, de documentos emitidos por, entre otros, la ONU, la Unión Europea y la OCDE; y

b) La segunda, por su parte, busca establecer el nivel de efectividad práctica de dichas normas.

Un análisis de los anteriores factores permitirá determinar el verdadero grado de contribución de los instrumentos de autorregulación relativo a la protección de los datos personales.[173]

Igualmente ha dicho que los instrumentos de autorregulación deben establecer mediante una redacción clara y accesible la política de protección de datos que van a aplicar a los tratamientos de datos personales las entidades que lo suscriben, incluyendo las reglas o estándares que garanticen el cumplimiento del principio de finalidad y calidad de los datos, el derecho de información en la recogida de los datos, la existencia del consentimiento de los afectados, la adopción de medidas de seguridad de los datos, y en su caso, las condiciones aplicables en la comunicación o transferencia internacional de datos a terceros, con el objeto de armonizar los tratamientos de datos efectuados por los adheridos.

Los códigos también deben reunir los procedimientos mediante los que se va a facilitar a los afectados el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los datos.

Además, se pueden prever acciones formativas en materia de protección de datos dirigidas a todos aquellos que realizan los tratamientos de los datos, especialmente en cuanto a su relación con los afectados".

[173] *Autorregulación y Protección de Datos Personales,* Documento elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra, Bolivia, los días 3 a 5 de mayo de 2006. Red Iberoamericana de Datos.

También pueden incorporar un sello de calidad que identifique a sus adheridos. Los responsables de los instrumentos de autorregulación deben dar publicidad de la existencia de los mismos, preferentemente a través de medios informáticos o telemáticos, detallando y publicando la identidad de las entidades adheridas.

En el caso de España, el Reglamento de la Ley Orgánica 15/1999 es específico al establecer el contenido de los códigos tipo:

> **Artículo 73.** Contenido.
> 1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
>
> 2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:
>
> La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
>
> Las previsiones específicas para la aplicación de los principios de protección de datos.
>
> El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
>
> El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
>
> La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
>
> Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
>
> Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en

el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. Compromisos adicionales.

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.

La identificación de las categorías de cesionarios o importadores de los datos.

Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.

El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. Garantías del cumplimiento de los códigos tipo.

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

La independencia e imparcialidad del órgano responsable de la supervisión.

La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

El principio de contradicción.

Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en elartículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. Relación de adheridos.

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. Depósito y publicidad de los códigos tipo.

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en

caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. Obligaciones posteriores a la inscripción del código tipo.

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior. Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar. Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento. Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

> Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

En México el Reglamento establece que los esquemas de autorregulación tendrán objetivos primordiales, y acerca del contenido se pueden extraer líneas para emitir parámetros (para los códigos deontológicos) de lo establecido en los siguientes numerales:

> **Artículo 80.** Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos y tendrán los siguientes objetivos primordiales:
>
> I. Coadyuvar al cumplimiento del principio de responsabilidad al que refiere la Ley y el presente Reglamento;
> II. Establecer procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la Ley;
> III. Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal que esté en su posesión;
> IV. Promover que los responsables de manera voluntaria cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la Ley, y mostrar a los titulares su compromiso con la protección de datos personales;
> V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;
> VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;
> VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;
> VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas, transparencia,

supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación; y
IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.
Estos esquemas serán vinculantes para quienes se adhieran a los mismos; no obstante, la adhesión será de carácter voluntario.

Artículo 82. Los esquemas de autorregulación deberán considerar los parámetros que emita la Secretaría, en coadyuvancia con el Instituto, para el correcto desarrollo de este tipo de mecanismos y medidas de autorregulación, considerando al menos lo siguiente:
I. El tipo de esquema convenido, que podrá constituirse en códigos deontológicos, código de buena práctica profesional, sellos de confianza, u otros que posibilite a los titulares identificar a los responsables comprometidos con la protección de sus datos personales;
II. Ámbito de aplicación de los esquemas de autorregulación;
III. Los procedimientos o mecanismos que se emplearán para hacer eficaz la protección de datos personales por parte de los adheridos, así como para medir la eficacia;
IV. Sistemas de supervisión y vigilancia internos y externos;
V. Programas de capacitación para quienes traten los datos personales;
VI. Los mecanismos para facilitar los derechos de los titulares de los datos personales;
VII. La identificación de las personas físicas o morales adheridas, que posibilite reconocer a los responsables que satisfacen los requisitos exigidos por determinado esquema de autorregulación y que se encuentran comprometidos con la protección de los datos personales que poseen; y
VIII. Las medidas correctivas eficaces en caso de incumplimiento.

Es importante mencionar que en el caso de Argentina, la Ley de Protección de Datos faculta a la autoridad a “homologar” los códigos de conducta que elaboren las asociaciones o entidades representativas de responsables o usuarios (art. 29,4,f). Igualmente ocurre en Chipre conforme al artículo 23 b) de la Ley de Procesamiento de Datos Personales del 2001, y el caso de Grecia es interesante pues el papel de la autoridad es de “asistencia” a las personas físicas o morales en la redacción de estos códigos (sección 2, 19 1

b) de la Ley 2472/1997 sobre la Protección de Individuos en relación con el Tratamiento de Datos Personales.

Sobre el mismo tema del contenido, llama la atención que en Italia, el Código en Materia de Protección de Datos personales establece disposiciones específicas para sujetos o sectores determinados. Así es el caso de la sección 102 (sector relacionado con el procesamiento de datos para propósitos históricos); sección 106 (sector relacionado con el procesamiento de datos para propósitos estadísticos o científicos); sección 111 (sector relacionado con la seguridad social); sección 133 (sector de TI); 140 (práctica profesional del marketing directo); entre otras.

8.3.7 Evaluación

Por otra parte, se considera oportuno que los códigos prevean fórmulas para evaluar periódicamente la eficacia de los instrumentos de autorregulación, midiendo el grado de satisfacción de los afectados y, en caso necesario, actualizando el contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

En el caso de Australia, este es uno de los elementos que es considerado con especial atención por el Comisionado a la hora de revisar un código de privacidad. Se aconseja también que dicho procedimiento permita la inclusión de comentarios por parte de otras dependencias públicas, consumidores e interesados relevantes, así como de la Oficina del propio Comisionado. Si bien este requisito no se encuentra contenido en la Ley, puede ser tomado en consideración por el Comisionado como una causal de revocación.

A fin de que este requisito sea cumplido de forma satisfactoria, los códigos deberán: establecer un proceso de revisión de código que tenga lugar al menos cada tres años; contener una declaración por la cual se comprometan los recursos necesarios para la revisión del código; y requerir al Administrador del código que emita una contestación al reporte de revisión independiente y presentarla ante el Comisionado dentro de los 30 días siguientes a la finalización del reporte.

8.3.8 Temporalidad y Alcance

Siguiendo el caso australiano, y aunado a que los códigos tienen una vigencia preestablecida, podrán existir **Códigos Temporales**, que como se explicó en una fase previa de este estudio, son aquellos que tengan una vida limitada. En este caso, la autoridad requerirá que éstos señalen de forma clara y expresa, cuándo o bajo qué circunstancias dicho código dejará de tener efectos. Asimismo, requerirá que éstos expresen los mecanismos por los cuales se comunique a los consumidores de la terminación del código.

Igualmente podrán existir **Códigos con Alcance Limitado** que, de acuerdo con la ley australiana, se permiten para cubrir únicamente ciertos aspectos u operaciones de las organizaciones.

Por ejemplo: Un tipo específico de información personal; Una actividad específica o clase de actividades; o Un sector de la industria o profesional específico. En ese sentido, se requerirá que el código establezca claramente, de forma que no se generen confusiones a los interesados o consumidores respecto de qué tipo de información, actividades o profesiones habrá de cubrir.

8.3.9 Costos de formulación y adopción

Tomando como base los casos del Reino Unido, al tratarse de códigos de buenas prácticas con origen institucional, los costos de formulación estarán vinculados, en primer lugar al organismo o entidad gubernamental que lo promueva. Se trata de un costo que ningún particular (responsable) debería asumir de forma directa.

Los costos de adopción de cualquiera de las buenas prácticas promovidas por códigos como lo que ha elaborado la ICO inglesa son variables e indeterminables *prima facie*, por muchas razones:

- Sector o actividad del responsable.
- Tamaño de la entidad o entidades.
- Tipo de datos personales tratados.
- Estado de la tecnología de los sistemas que tratan datos personales en la organización correspondiente.
- Estado de implementación de medidas de seguridad existentes para el tratamiento de datos personales.
- Grado de adecuación o adaptación a la legislación de protección de datos por parte de la organización interesada.

De hecho, dada la especificidad de las materias que aborda, es posible pensar en varios tipos de responsables a los que podrían resultar aplicables las recomendaciones de todos los códigos analizados.

Así, es posible pensar en los empleados, los sistemas de CCTV, las páginas web, los avisos de privacidad indispensables para su actividad y las diversas transferencias de datos que deben realizar ciertos responsables como:

- Hospitales,
- Hoteles,
- Escuelas,
- Centros comerciales, etc.

Por lo que se refiere a la fórmula establecida en España (códigos a instancia de parte), el principal costo identificable relativo a la formulación de un código tipo lo constituye la contratación del grupo de expertos legales y técnicos que una organización interesada debería efectuar para su formulación.

Lo anterior es así dado que debemos considerar que la formulación de un código de este tipo, por parte de cualquier entidad (individual o sectorial), debe estar precedida de un análisis profundo y adecuado, relacionado con los siguientes puntos esenciales:

- Actividad de la entidad.
- Estructura y organización.
- Ámbito de validez del código.
- Legislación sectorial que afecte al tratamiento de datos personales.
- Flujo de los datos personales a través de cualquier medio.
- Finalidades de los diversos tratamientos efectuados en la organización.
- Tipo de datos personales tratados, incluyendo datos sensibles.
- Identificación de los sistemas de información que tratan datos personales.
- Inventario de bases de datos y, en su caso, de bases de datos compartidas.
- Cumplimiento de todos los principios relativos al tratamiento de datos personales.

- Identificación de comunicaciones de datos personales (identificadas en España como cesiones y transferencias).
- Identificación de supuestos de excepción para el tratamiento y comunicación de datos personales sin consentimiento de sus titulares.
- Análisis técnico y legal respecto del estado de cumplimiento de las medidas de seguridad exigibles, para todas las bases de datos que tratan datos personales.
- Definición de procedimientos para el cumplimiento de los derechos ARCO.
- Definición e implantación de roles y funciones para el personal con acceso a datos personales.

A la vista de los diversos elementos anteriormente identificados, los costos de adopción de un código tipo serán completamente variables, tomando en consideración la existencia de las siguientes variables:

- Alcance del código (individual o sectorial).
- Tipo de actividad.
- Tamaño de la entidad o entidades.
- Tipo de datos tratados.
- Estado de implementación de medidas de seguridad existentes para el tratamiento de datos personales.

A la vista de la fórmula establecida en España (códigos a instancia de parte), el principal costo identificable relativo a la formulación de un código tipo lo constituye la contratación del grupo de expertos legales y técnicos que una organización interesada debería efectuar para su formulación.

Lo anterior es así dado que debemos considerar que la formulación de un código de este tipo, por parte de cualquier entidad (individual o sectorial), debe estar precedida de un análisis profundo y adecuado, relacionado con los siguientes puntos esenciales:

- Actividad de la entidad.
- Estructura y organización.
- Ámbito de validez del código.
- Legislación sectorial que afecte al tratamiento de datos personales.
- Flujo de los datos personales a través de cualquier medio.
- Finalidades de los diversos tratamientos efectuados en la organización.
- Tipo de datos personales tratados, incluyendo datos sensibles.
- Identificación de los sistemas de información que tratan datos personales.
- Inventario de bases de datos y, en su caso, de bases de datos compartidas.
- Cumplimiento de todos los principios relativos al tratamiento de datos personales.
- Identificación de comunicaciones de datos personales (identificadas en España como cesiones y transferencias).
- Identificación de supuestos de excepción para el tratamiento y comunicación de datos personales sin consentimiento de sus titulares.
- Análisis técnico y legal respecto del estado de cumplimiento de las medidas de seguridad exigibles, para todas las base de datos que tratan datos personales.
- Definición de procedimientos para el cumplimiento de los derechos ARCO.

- Definición e implantación de roles y funciones para el personal con acceso a datos personales.

A la vista de los diversos elementos anteriormente identificados, los costos de adopción de un código tipo serán completamente variables, tomando en consideración la existencia de las siguientes variables:

- Alcance del código (individual o sectorial).
- Tipo de actividad.
- Tamaño de la entidad o entidades.
- Tipo de datos tratados.
- Estado de implementación de medidas de seguridad existentes para el tratamiento de datos personales.

8.4 Los códigos en la Unión Europea

8.4.1 Antecedentes

Frente a la naturaleza *sui generis* del derecho comunitario, resulta necesario recordar que la "Directiva de Protección de Datos Personales"[174] pertenece al orden del derecho derivado; es decir, se trata de una norma aprobada por las instituciones de la Unión Europea (EU) que conforme a su naturaleza obliga a sus miembros al cumplimiento de los objetivos marcados en sus disposiciones.

[174] Directiva 95/46/CE de Protección de Datos Personales 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.

Al día de hoy, esta Directiva constituye la base de la legislación sobre protección de datos personales en cada uno de los estados miembros de la UE,[175] que en mayor o menor medida han implementado sus disposiciones a través de los instrumentos normativos que soberanamente han elegido.

Tal y como será explicado, esta situación puede cambiar próximamente mediante la adopción del Reglamento de Protección de Datos Personales, cuya propuesta ya ha sido presentada por la Comisión Europea.[176] Este cambio es significativo dado que los Reglamentos comunitarios tienen efectos generales para todos los países miembros y no requieren actos de implementación. Se trata de leyes tal y como se conciben en cualquier otro país como México; con efectos generales dentro del territorio de todos los Estados miembros de la UE.

8.4.2 Situación *de facto*

Como ha sido analizado, las disposiciones de la Directiva de Protección de Datos Personales de la UE han dejado espacio para la regulación comunitaria 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*".[177]

Sin embargo, y tal y como también ya ha sido destacado, actualmente sólo puede darse cuenta de **un código de ámbito comunitario** orientado al cumplimiento de las disposiciones emanadas de esta Directiva: el "*Código de Conducta Europeo de la FEDMA (*FEDERATION OF EUROPEAN DIRECT

[175] Ver: Estado de implementación de la Directiva de Protección de Datos Personales en los países de la UE, en: http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm
[176] Ver: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf.
[177] Art. 27.1 de la Directiva de Protección de Datos Personales.

AND INTERACTIVE MARKETING*) sobre la utilización de datos personales en la comercialización directa*".

Frente a esta situación, y por un lado, es de destacar que el ámbito de dicho "Código de Conducta Europeo" es relevante en el marco del sector al que está dirigido, pues se dirige a actividades eminentemente transnacionales propias de la sociedad de la información que promueve la UE.

Por otro lado, la existencia de un solo ejemplo permite detectar las dificultades que plantea la regulación comunitaria de la protección de datos personales, que en la realidad se presenta como un grupo de legislaciones nacionales que conforme a su propia experiencia y antecedentes han ido incorporando la Directiva de Protección de Datos Personales.

8.4.3 Cambios reglamentarios en la UE

En la fecha de realización de este estudio, diversos actores intercambian ideas y opiniones en torno a la propuesta del Reglamento a través del cual se propone elevar a nivel comunitario (europeo) la protección de datos personales.

De hecho, la propia Comisión Europea promueve espacios en los que explica su propuesta: "*Commission proposes a comprehensive reform of the data protection rules*"[178] y "*Why do we need new data protection rules now*?"[179]

Se trata de un proyecto ambicioso a la vez que necesario, sobre el cual es difícil afirmar que exista una aprobación unánime entorno a la propuesta

[178] (http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm)
[179] (http://ec.europa.eu/justice/data-protection/minisite/).

presentada por la Comisión Europea, pues diversas instituciones ya han emitido opiniones corrigiendo o ampliando esta propuesta[180].

Sin embargo, consideramos que la aprobación de un Reglamento que regule la protección de datos personales en la UE es inminente y que su entrada en vigor puede dar lugar a un mayor número de acciones autorregulatorias, con fundamento en los artículos 38 y 39 de la propuesta presentada por la Comisión Europea.

8.5 Los códigos en el Reino Unido

En el Reino Unido coexisten dos tipos de códigos de buenas prácticas sobre protección de datos personales:

1. Aquéllos con origen en la autoridad encargada de aplicar la Ley de Protección de Datos de 1998 (Data Protection Act 1998, la LPD1998), es decir, la Oficina del Comisionado de Información. [181]

2. Aquéllos con origen en asociaciones de comercio, previa presentación al Comisionado[182] para su consideración y opinión[183].

[180] Ver, por ejemplo:"*Opinion of the European Data Protection Supervisor on the data protection reform package*", EDPS, Marzo 2012, en: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf; y además, "*Initial analysis of the European Commission's proposals for a revised data protection legislative framework*" de la ICO, Febrero 2012 en: http://www.ico.gov.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx.

[181] La *Information Commissioner's Office o ICO*: www.ico.gov.uk.

[182] Titular de la ICO.

[183] A pesar de estar previstos, a día de hoy la ICO sólo se da cuenta de la aprobación de un Código de Buenas Prácticas presentado con fundamento en la sección 51(4)(b) de la LPD1998: "*Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998*"

En cuanto a los primeros, hay que tener en cuenta que tras las reformas introducidas a la LPD1998 en el año 2009,[184] en este país se pueden identificar dos sub-tipos:

8.5.1 Códigos de buenas prácticas emitidos con fundamento en la sección 51(3) de la LPD

En esta categoría se encuentran comprendidos aquellos códigos cuya formulación y emisión está a cargo del Comisionado de Información en ejercicio de la competencia general que le faculta para "*promover el seguimiento de buenas prácticas por parte de los responsables del tratamiento"* y de la competencia específica para "*elaborar y difundir, a las personas que considere oportunas, códigos de conducta para la orientación hacia buenas prácticas*" en materia de protección de datos personales.

Para su elaboración, la sección 51(3) de la LPD1998 prevé que el Comisionado deberá realizar consultas previas con las asociaciones de comercio o representantes de los titulares de datos personales que considere apropiadas.

Con fundamento en la sección de referencia, al día de hoy se han difundido los siguientes códigos, explicados más adelante:

- Código de Buenas Prácticas en el Empleo
- Código de Buenas Prácticas para Sistemas de Circuito Cerrado de Televisión
- Código de Buenas Prácticas sobre Datos Personales en Internet
- Código de Buenas Práctica sobre Avisos de Privacidad

[184] Estas reformas se implementaron a través de la *Coroners and Justice Act 2009* (Parte 8). El texto de esta disposición puede ser consultado en el siguiente enlace: http://www.legislation.gov.uk/ukpga/2009/25/contents.

8.5.2 El código a que se refiere el artículo 52A de la LPD1998

El "Código de Buenas Prácticas para el Intercambio de Datos" cuenta con una regulación específica dentro de la LPD1998 y tiene como propósito facilitar prácticas concretas relacionadas con la comunicación de datos personales (cesiones, intercambios o transferencias). Se trata de un código que si bien fue preparado por el Comisionado, fue aprobado por el Secretario de Estado inglés y posteriormente por el Parlamento.

Las normas relativas a su elaboración y sus efectos fueron introducidas en 2009, y le otorgan un estatus especial al establecer en primer lugar que el incumplimiento de cualesquiera de sus disposiciones no genera una responsabilidad legal por sí misma (sección 52E(1)).

Acto seguido, y sin embargo, se dispone que el código es admisible como evidencia en cualquier procedimiento legal (Sección 52E(2)).

A tales efectos, se establece que cualquier disposición de este código deberá ser tomada en cuenta si, en relación con cualquier cuestión surgida en un procedimiento judicial, se considera que dicha disposición tiene relevancia para resolver la cuestión de que se trate (Sección 52E(3)).

El objeto general de todos los códigos enumerados es brindar consejos o sugerencias sobre buenas prácticas para el cumplimiento de las disposiciones de LPD1998.

A partir de dicha premisa la ICO inglesa ha desarrollado los códigos específicos que a continuación se analizan bajo la perspectiva de su objeto y sujetos particulares.

8.5.3 Código de Buenas Prácticas en el Empleo

Este código está dirigido a los empleadores en general y, en consecuencia, puede considerarse uno de los más extensivos de entre aquellos que han sido emitidos por la ICO, en la medida en que un gran número de responsables son a su vez empleadores.

Se trata de un código que establece recomendaciones genéricas sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, dentro de las cuales resalta una de especial relevancia:

> "La protección de datos debe ser vista como una parte integral de las prácticas de empleo. Es importante desarrollar una cultura en la que el respeto a la vida privada, la protección de datos, la seguridad y la confidencialidad de la información personal, sean vistos como la norma."[185]

Además, abarca los siguientes aspectos específicos:

a) Contratación y selección de personal

b) Expedientes de los empleados

c) Monitoreo o vigilancia en el lugar de trabajo

d) Tratamiento de datos de salud de los empleados

8.5.4 Código de Buenas Prácticas para Sistemas de Circuito Cerrado de Televisión (CCTV)

Evidentemente, se trata de un código que únicamente está destinado a aquellos responsables que operen un CCTV u otros dispositivos que

[185] "The Employment Practices Code", ICO, June 2005, p. 10 (la traducción es nuestra).

permiten ver o grabar imágenes de personas, proporcionándoles asesoría sobre buenas prácticas.

Una premisa interesante de este código es su ámbito de aplicación, pues parte de la premisa de que la mayoría de estos sistemas están dirigidos a ver o grabar las actividades de las personas, razón por la cual se considera que la mayoría de sus usos están sujetos a la normativa de protección de datos.

Las materias relevantes del código pueden resumirse en los siguientes puntos:

a) Recomendaciones sobre la correcta administración del sistema

b) Selección y colación de las cámaras

c) Uso del equipo

d) Búsqueda y uso de imágenes guardadas

En un entorno incipiente como el mexicano, la adopción de un código que regule este tratamiento de datos personales tan específico se antoja aún anticipado, si bien eventualmente necesario.

El tratamiento de imágenes de personas identificadas o identificables constituye tan solo un tipo de tratamiento entre los muchos que puede llevar a cabo un responsable que cuente con los recursos para mantener un CCTV.

En la medida de lo posible, sería recomendable alejarnos de una especialización como la que aborda este código, hasta en tanto no exista la conciencia de que un código o guía de este tipo no exime a los responsables del resto de obligaciones en relación con otras bases de datos que pudieran estar bajo su responsabilidad (y que con toda probabilidad lo estarán).

8.5.5 Código de Buenas Prácticas sobre Datos Personales en Internet

Frente al sector de las TI y en consideración del impulso que se pretende brindar a la sociedad de la información en México, este código aporta recomendaciones sobre buenas prácticas en aspectos tan vigentes como:

a) Recopilación de datos personales a través de formularios en línea;

b) Uso de cookies o direcciones IP para dirigir contenidos a personas específicas;

c) Uso de datos personales para comercializar productos o prestar servicios; y

d) Uso de instalaciones de *cloud computing* para tratar datos personales.

En nuestra opinión, es uno de los códigos más completos, concisos e ilustrativos de aquellos que fueron analizados en la región de la UE, tomando en consideración además que incorpora recomendaciones sobre comercio electrónico.

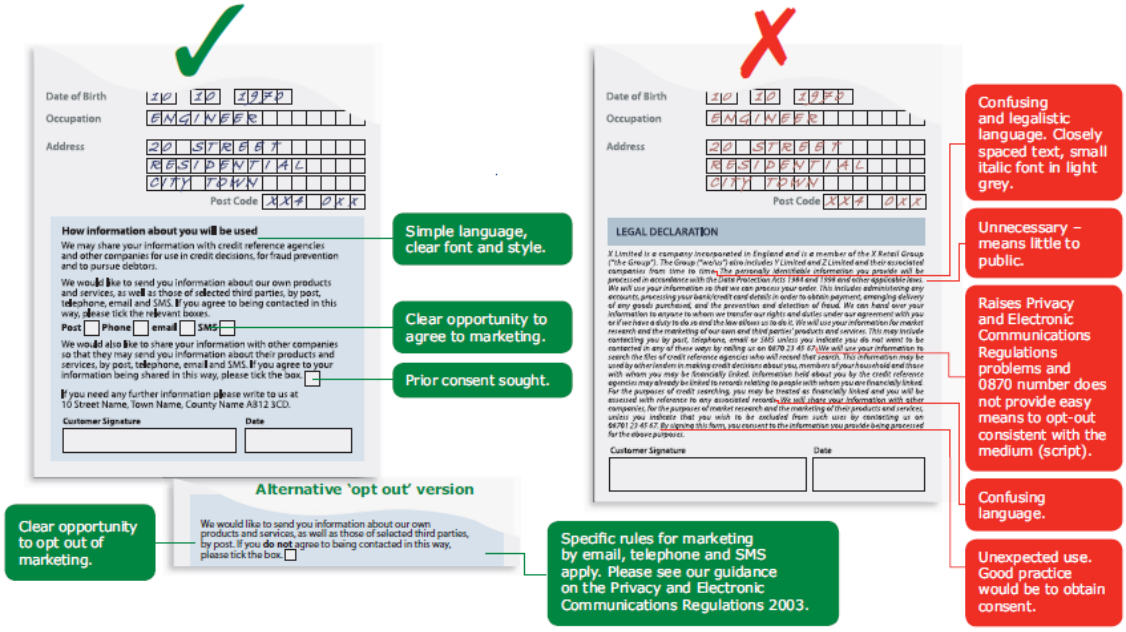
8.5.6 Código de Buenas Prácticas sobre Avisos de Privacidad

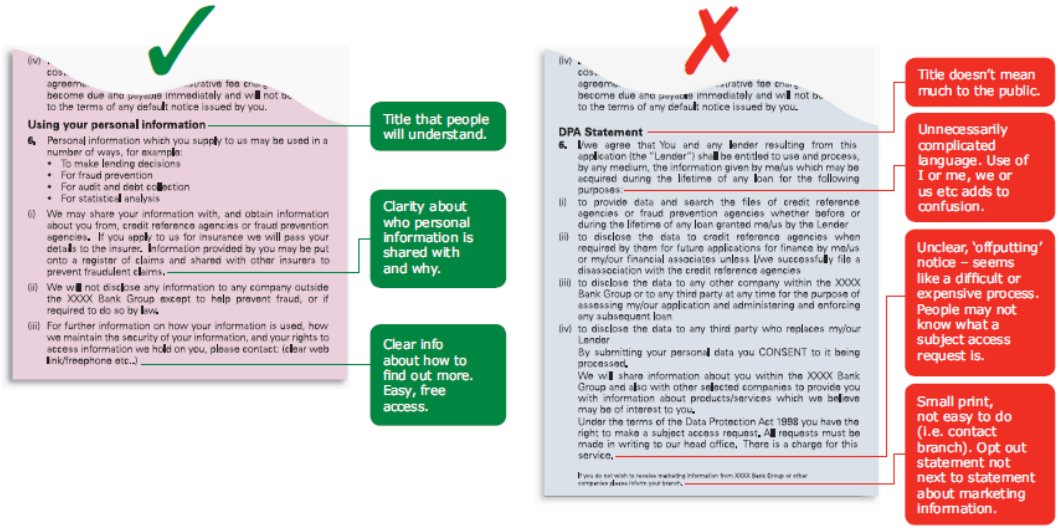
Puede considerarse el equivalente inglés de la “Guía Práctica para Generar el Aviso de Privacidad” del IFAIPD, ya que contiene información relativa a los principios de información, licitud, consentimiento, finalidad y lealtad (transparencia) que deben observarse al momento de redactar un Aviso de Privacidad adecuado y apegado a las disposiciones legales.

Destaca que en sus disposiciones el código identifica los diversos medios a través de los cuales se pueden dar a conocer este tipo de avisos:

- Oralmente
- Por escrito
- Señales
- Medios electrónicos

Adicionalmente, proporciona ejemplos gráficos de buenas y malas prácticas sobre las características y colocación de estos avisos, que muchas veces pueden ser más ilustrativos que diez párrafos explicativos:





8.5.7 Código de Buenas Prácticas para el Intercambio de Datos

Aplicable para cualquier responsable, este código se propone aportar medidas prácticas para cumplir con los requisitos existentes en relación con las transferencias de datos personales.

Dada la multiplicidad de factores que pueden incidir en la procedencia, fundamento y medidas aplicables al intercambio de datos personales, el código se estructura de la siguiente forma:

- Transferencia de datos y legislación aplicable
- La decisión de intercambiar datos personales
- Licitud y transparencia
- Seguridad
- Normativa interna (Governance)
- Derechos de los titulares

- Cosas que deben evitarse
- Facultades de la autoridad y sanciones
- Notificaciones a la ICO sobre intercambios de datos a realizar
- Acceso a la información
- Convenios sobre intercambio de datos

Se trata de un código que por un lado sólo aborda un único aspecto del tratamiento de datos personales, aunque también es cierto que se trata de un aspecto de relevancia importante, pues que la transferencia incontrolada de datos es una de las prácticas que genera mayores riesgos contra la seguridad de los datos personales.

Por sí solo, brinda recomendaciones importantes en cuanto al aspecto que quiere tratar, pero de ninguna forma brinda recomendaciones o buenas prácticas que aseguren el cumplimiento de otras obligaciones y de los principios relativos a la protección de datos personales.

8.5.8 Advertencias

Es importante no dejar de tomar en cuenta que el tipo de códigos adoptados por la ICO abordan cuestiones puntuales relativas al tratamiento de datos personales, por lo que la adopción de todas sus recomendaciones (inclusive) no garantiza el cumplimiento del resto de principios y obligaciones sobre la materia.

En último término, los códigos ingleses funcionan para resolver dudas sobre cuestiones particulares, pero de ninguna forma proporcionan el tipo de información que garantice un cumplimiento integral de la legislación vigente

sobre la materia, que en todo caso debe someterse a un análisis jurídico y técnico.

8.6 Los códigos en España

8.6.1 Antecedentes

El carácter general de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), de obligado cumplimiento tanto para particulares como para los diversos organismos que conforman los tres niveles de la Administración Pública en España, conduce a la posibilidad de que los códigos tipo previstos por su artículo 32 puedan adoptar las siguientes formas:

- Acuerdos sectoriales
- Convenios administrativos
- Decisiones de empresa

Que a su vez podrán ser formulados por "*los responsables de tratamientos de titularidad pública y privada, así como [por] las organizaciones en que se agrupen*".[186]

Por lo demás, no se faculta al Director de la Agencia Española de Protección de Datos (AEPD) para iniciar de oficio algún procedimiento a través del cual dicha entidad proponga o inicie consultas públicas para la elaboración de códigos tipo sobre protección de datos personales, de ningún tipo ni

[186] LOPD, artículo 32.

alcance[187]. Así, este medio de autorregulación surge en España únicamente a iniciativa de parte[188].

Conforme a lo anterior, es posible identificar que en este país europeo los códigos tipo en materia de protección de datos personales pueden adoptar alguna de las siguientes formas:[189]

1. De ámbito privado individual

2. De ámbito privado sectorial

3. De ámbito público individual

4. De ámbito público sectorial

En relación con la primera categoría, actualmente no existe ningún código de ámbito privado individual registrado ante la AEPD. En cuanto al segundo tipo, podemos identificar los códigos de FARMAINDUSTRIA, el de la Asociación Empresarial de Gestión Inmobiliaria, el de la Unión Catalana de Hospitales o el Código Tipo de Confianza Online ©, por citar algunos ejemplos.

Por otro lado, se detecta que únicamente una institución pública ha realizado la inscripción de un código tipo sobre la materia: La Universidad de Castilla-La Mancha; y que únicamente aparece registrado un código de ámbito

[187] El Estatuto de la Agencia Española de Protección de Datos, aprobado mediante Real Decreto 428/1993, de 26 de marzo, únicamente establece, en relación con este tema, la siguiente facultad de su Director: "*Requerir a los responsables de ficheros de titularidad privada a que subsanen deficiencias de los códigos tipo*" (artículo 12.2.b)).

[188] Así lo corrobora el artículo 145.1 del Reglamento de la LOPD: "*El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.*"

[189] Cfr. además el artículo 145.2 del Reglamento de la LOPD.

público sectorial: el código tipo para las entidades locales adheridas a EUDEL (Asociación de Municipios Vascos-Euskadiko Udalen Elkartea).

De todo ello puede concluirse que los códigos privados sectoriales son aquellos mayoritariamente utilizados en España; sin que ello signifique que estemos frente a una práctica altamente difundida, pues a pesar de tratarse de una Ley que entró en vigor en el año 2000, al día de hoy únicamente se han inscrito 13 códigos tipos.

Por otro lado, es preciso identificar que sin negarles carácter vinculante de forma expresa, la LOPD así lo establece al indicar que estos códigos "*tendrán el carácter de códigos deontológicos o de buena práctica profesional*", sin que tampoco se establezcan consecuencias jurídicas específicas derivadas de su incumplimiento, que en todo caso vendrán determinadas a nivel interno en aquellos códigos sectoriales que así lo prevean contra aquellos miembros adheridos que hubiesen vulnerado las disposiciones adoptadas.

Desde un punto de vista formal, el Director de la AEPD no aprueba los Códigos Tipo de aquellos responsables que han decidido formularlos y presentarlos ante esta entidad.

El procedimiento general que estable el artículo 32 de LOPD prevé que dichos códigos deberán ser "*depositados o inscritos en el Registro General de Protección de Datos*" y que dicho Registro podrá denegar la inscripción solicitada "*cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia*". En estos casos, el mismo numeral prevé que el Director de la AEPD deberá requerir a los solicitantes para que efectúen las correcciones oportunas.

Este régimen conduce a que por parte de la entidad encargada de aplicar la LOPD no se otorguen aprobaciones o calificaciones sobre la idoneidad, eficacia o estado de corrección de los Códigos Tipo inscritos en la AEDP; sino que de la misma únicamente se obtiene la aprobación de su registro por ajustarse a las disposiciones legales y reglamentarias sobre protección de datos personales.

En otras palabras, serán registrados aquellos códigos que sean legales, independientemente de su extensión, presentación, organización, configuración o alcance; cuestión que queda claramente establecida en el artículo 150.1 del Reglamento de la LOPD, que expresamente dispone: "*Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos*."

Finalmente, corresponde recordar que el artículo 147.1 del Reglamento de la LOPD establece que corresponde al Director de la AEPD acordar, cuando la naturaleza del procedimiento así lo requiera, la apertura de un periodo de "*información pública*" (10 días hábiles), dentro del cual podrán formularse alegaciones en relación con los códigos presentados para inscripción.

8.6.2 Objeto de los códigos

En todos los casos analizados se aprecia como objeto común de todos los códigos tipo la intención de regular la organización de sus sujetos para facilitar el cumplimiento de los principios y obligaciones establecidos por la LOPD. Este objeto es esencial en este tipo de instrumentos.

En general, las organizaciones que los adoptan parten de una posición más o menos común: la necesaria revisión, adecuación y transformación de su forma de trabajo para cumplir con la normativa sobre protección de datos mediante el diseño de procedimientos que permitan observar las obligaciones formales establecidas y adoptar toda una serie de medidas que garanticen la seguridad de los datos[190].

Esta adecuación y transformación se orienta a asegurar dos tipos generales de cumplimiento, *ad intra*, *ad extra*.

8.6.2.1 Cumplimiento *ad intra*

Con este objetivo nos referimos a la reorganización de cualquier entidad para que sus procedimientos, actividades y forma de trabajo en general tomen en consideración las obligaciones y principios que rigen en materia de protección de datos y que afectan al tratamiento de los datos personales. Se trata de conseguir que a cualquier nivel de la entidad participante se respeten principios como los de calidad, proporcionalidad o finalidad.

El cumplimiento *ad intra* también conlleva la adopción de cuantas medidas administrativas, físicas y técnicas sean necesarias adoptar para garantizar la disponibilidad, integridad y confidencialidad de los datos personales que son objeto de tratamiento por el responsable (medidas de seguridad).

En cuanto al tipo de medidas técnicas que deben adoptarse para garantizar la seguridad de los datos personales, su definición mediante códigos de autorregulación puede ser complicada en virtud de la diversidad de sistemas

[190] En España esta normativa ya sobrepasa a la LOPD, puesto que cada vez existen más leyes y reglamentos sobre diversas materias que incorporan disposiciones específicas en materia de protección de datos personales, si bien es cierto que todas ellas remiten en última instancia a la LOPD, a su reglamento de desarrollo y a los principios generales sobre la materia.

electrónicos, programas y aplicaciones que pueden ser utilizados para tratar datos personales, así como también en razón del estado de la tecnología imperante en el momento en que dicho código sea formulado.

En general, resulta recomendable que las partes adherentes a estos códigos asuman la obligación de adoptar las medidas técnicas exigidas por las disposiciones legales vigentes y, en su caso, en función del tipo de datos personales tratados y de las finalidades del tratamiento.

8.6.2.2 Cumplimiento *ad extra*

La reorganización de una entidad conforme a las buenas prácticas establecidas en un código de autorregulación debe permitirle también cumplir con los principios y obligaciones que pueden ser "percibidos" desde fuera.

Se trata de asignar roles y funciones que aseguren, entre otros aspectos, que no se recabarán datos personales en contravención a las disposiciones legales, que los titulares serán debidamente informados de la finalidad del tratamiento o de que nunca deje de atenderse en tiempo y forma cualquier solicitud de derechos acceso, rectificación, cancelación u oposición.

8.6.3 Sujetos y tipos de datos personales tratados

Por otra parte, el caso español permite determinar que no existe un tipo homogéneo de sujetos inclinados a formular y adoptar un código tipo en materia de datos personales; aunque resulta notable la ausencia de un número mayor de códigos provenientes del sector público.

En cuanto al tipo de datos personales que tratan los sujetos que han formulado algún código tipo, existe una tendencia identificable en relación con aquellos que tratan datos personales considerados sensibles o "especialmente protegidos"[191] o que tratan un "conjunto de datos personales que ofrecen una definición de las características o de la personalidad de los titulares y que permiten evaluar determinados aspectos de la personalidad o del comportamiento de los mismos".[192]

Se trata por un lado de organizaciones que agrupan a responsables que participan en el sector salud (sanidad) que tratan datos personales sensibles (salud) de forma inherente para el desarrollo de sus actividades; y por el otro de responsables que crean bases de datos compartidas cuya finalidad es crear "perfiles" de clientes o usuarios como referencia para evitar fraudes o el inicio de relaciones jurídicas con personas calificadas como morosas.

Finalmente, merece atención el Código Tipo de Confianza Online, diseñado para cubrir tres aspectos esenciales en el ámbito de los prestadores de servicios de la sociedad de la información:

- Protección del consumidor,
- Cumplimiento de las disposiciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y
- Protección de datos personales.

[191] El artículo 7 de la LOPD establece que se consideran datos especialmente protegidos aquellos que "*revelen la ideología, afiliación sindical, religión y creencias*" y aquellos "*que hagan referencia al origen racial, a la salud y a la vida sexual*". También se incluyen en esta categoría a "*los datos de carácter personal relativos a la comisión de infracciones penales o administrativas*", que "*sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.*"

[192] Cfr. artículo 81.2.f) del Reglamento de la LFPD (Real Decreto 1720/2007, de 20 de diciembre).

Este código promueve la adhesión al mismo a través de la creación de un sello distintivo que los prestadores de servicios de la sociedad de la información podrán usar en sus páginas web, como garantía en la seguridad de sus transacciones tanto a nivel de consumidor como en relación con el tratamiento y seguridad de los datos personales que proporcionen a través de medios electrónicos para la adquisición de bienes y servicios.

8.6.4 Procedimiento de depósito/inscripción

Desde un punto de vista formal, el Director de la AEPD no aprueba los códigos tipo de aquellos responsables que han decidido formularlos y presentarlos ante esta entidad.

El procedimiento general que estable el artículo 32 de LOPD prevé que dichos códigos deberán ser "*depositados o inscritos en el Registro General de Protección de Datos*" y que dicho Registro podrá denegar la inscripción solicitada "*cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia*". En estos casos, el mismo numeral prevé que el Director de la AEPD deberá requerir a los solicitantes para que efectúen las correcciones oportunas.

Este régimen conduce a que por parte de la entidad encargada de aplicar la LOPD no se otorguen aprobaciones o calificaciones sobre la idoneidad, eficacia o estado de corrección de los códigos tipo inscritos en la AEDP; sino que de la misma únicamente se obtiene la aprobación de su registro por ajustarse a las disposiciones legales y reglamentarias sobre protección de datos personales.

En otras palabras, serán registrados aquellos códigos que sean legales, independientemente de su extensión, presentación, organización,

configuración o alcance; cuestión que queda claramente establecida en el artículo 150.1 del Reglamento de la LOPD, que expresamente dispone:

> "*Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos*."

Finalmente, corresponde recordar que el artículo 147.1 del Reglamento de la LOPD establece que corresponde al Director de la AEPD acordar, cuando la naturaleza del procedimiento así lo requiera, la apertura de un periodo de "*información pública*" (10 días hábiles), dentro del cual podrán formularse alegaciones en relación con los códigos presentados para inscripción.

8.7 Los códigos en Australia

En este país, a la fecha se encuentran aprobados y en vigor los siguientes códigos de privacidad:

Título del Código	Administrador	Inicio
Market and Social Research Privacy Code	Association of Market + Social Research Organization	1 de septiembre de 2003, con modificaciones el 30 de junio de 2007
Queensland Club Industry Privacy Code	Clubs Queensland	23 de agosto de 2002, con modificaciones el 1 de mayo de 2009
Biometrics Institute Privacy Code	Biometrics Institute	1 de septiembre de 2006

8.7.1 Internet Industry Association Privacy Code 2001

Según información de la propia Oficina del Comisionado de la Información, actualmente se encuentra en trámite de aprobación un código de privacidad que tendrá por objeto regular la industria del Internet. Este código fue sometido a consideración de la Oficina de Privacidad por la Asociación de la Industria del Internet[193] (IIA por sus siglas en inglés) en el año de 2003.

Destaca de la propuesta de código la inclusión de una distinción de aprobación (*Approved Designation*) la cual puede consistir en un símbolo, un conjunto de palabras o cualquier otra identificación que sea aceptada por la mesa directiva de la IIA. El fin primordial de esta distinción será hacer saber al público que el miembro que lo porta se encuentra obligado por el Código de Privacidad de la IIA.

Asimismo, éste código enfatiza la necesidad de que los prestadores de servicios relacionados con el Internet ajusten sus medidas de seguridad y privacidad de modo que también cumplan con la normativa Europea (en particular de acuerdo con *Safe Harbor*), por lo que el código se encuentra diseñado con la mira de estandarizar las prácticas de cumplimiento de acuerdo con ambas legislaciones.

De acuerdo con el propio código entre sus finalidades principales se encuentra facilitar la protección de la información personal, reforzar la protección de la información de o sobre niños, restringir el *marketing directo* a aquellas personas que expresamente lo han consentido, así como permitir a las pequeñas empresas (que de otro modo no estarían obligadas por la

[193] Para mayor información sobre esta organización véase http://www.iia.net.au/

Privacy Act) beneficiarse del empleo de buenas prácticas en relación con la protección de la privacidad.

Además, el proyecto establece reglas en materia de flujo transfronterizo de datos, especificando aquellos casos en los que un miembro podrá transferir datos personales hacia el extranjero (en general cuando haya una ley que exija su protección, contrato o esquema apropiado, o bien, mediante el consentimiento del titular de los datos). También establece la designación de un Administrador, sus funciones, un mecanismo de revisión del código, así como para su modificación.

Algo destacable del código es su apartado de sanciones, el cual establece que en caso de incumplimiento por parte de algún miembro, podrá revocarse la autorización para emplear la distinción de aprobación lo cual conlleva a que el miembro también deja de ser parte del código de privacidad.

La decisión puede ser apelada ante el Órgano Independiente de Revisión del código dentro de los 7 días siguientes a la decisión de revocación. Finalmente, en el supuesto en que un miembro haga uso de la distinción de aprobación u otro reconocimiento derivado del código sin la autorización correspondiente, el código establece que esta se considerará una causa de responsabilidad bajo la Ley de Prácticas Comerciales de 1974 (*Trade Practices Act 1974*).

8.7.2 Guía para la Formulación de Códigos

Como anteriormente se ha explicado, a fin de facilitar a los particulares el proceso de elaboración y aprobación de códigos de privacidad, la *Privacy Act* australiana de 1988 faculta al Comisionado de Privacidad para emitir

lineamientos o directrices *(guidelines)* [194] que además deberán ser cumplidos por las organizaciones a la hora de solicitar la aprobación de un código. Algo muy parecido a los parámetros mexicanos previstos en la LFPDPPP.

Con base en ello, el Comisionado de Privacidad publicó en agosto de 2001 un documento denominado *Code Development Guidelines* el cual tiene como finalidad ayudar a las organizaciones a decidir sobre la conveniencia de adoptar un código de privacidad, así como informar y precisar detalladamente aquellos requisitos que deberán ser satisfechos en la aprobación de un código de privacidad.

A continuación se expone de forma sintetizada el contenido de dichos lineamientos:

Sujetos

De acuerdo con este documento, cualquier organización, grupo de organizaciones o asociación que represente los intereses de sus miembros puede solicitar al Comisionado la aprobación de un Código de Privacidad. Esta categoría incluye también a terceros que con ánimo de lucro (es decir, asociaciones no representativas) busquen atraer a los sujetos obligados a su esquema de solución de controversias.

Consideraciones previas

El documento presenta algunos puntos que deben ser considerados por los particulares antes de embarcarse en la compleja tarea de desarrollar y aplicar un Código de Privacidad. Algunos de estos puntos son: las razones por las cuales conviene adoptar un código; la medición de la necesidad de adoptar el código; el establecimiento o no, de un mecanismo separado de tratamiento de quejas, así como los costos que implica desarrollar y mantener en operación un Código de Privacidad.

[194] Véase Apartado IV, División 2, Seccion 18 BF y 27 (ea) de la Privacy Act de 1988. A partir de noviembre de 2010, con la aprobación de la Australian Information Commissioner Act de 2010 la preparación, publicación, modificación o revocación de estas directrices deberán contar con la aprobación del Comisionado de Información.

Una recomendación del Comisionado de Privacidad es que en el desarrollo de los Códigos, las organizaciones tomen en consideración las disposiciones de la Trade Practices Act de 1974, en particular, aquellas relacionadas con prácticas anticompetitivas. Aunque por sí mismo un Código de Privacidad no represente una práctica anticompetitiva, existe la posibilidad de que en la implementación del Código se actualicen supuestos contrarios a esta ley. Por ejemplo, podría argüirse que un Código de Privacidad adoptado por la asociación relevante de un sector de la industria, que requiera a los miembros invertir en software muy costoso y que no necesariamente sirva para cumplir con los NPPs, podría restringir el acceso y vulnerar la competitividad en perjuicio de la Trade Practices Act. También podría haber infracciones a esta Ley cuando un Código requiera a sus miembros no tratar con otros sujetos que no posean dicho software.

En estos casos, los interesados tienen la posibilidad de acudir ante la Comisión de Competitividad Australiana a solicitar que las cláusulas sean revisadas, y en su caso, autorizadas.

Proceso de consulta

El éxito del modelo de corregulación depende en gran medida de la oportunidad que se brinde al público y a los principales interesados, de comentar y examinar la propuesta de Código de Privacidad, máxime cuando éstos tienen por objeto sustituir la protección que brinda la ley. Para ello, el Comisionado invita a las organizaciones, tomar en cuenta lo siguiente:

- ✓ *Identificar a los principales interesados que puedan verse afectados o tengan interés en el Código propuesto, incluyendo consumidores.*
- ✓ *Identificar la técnica más apropiada para obtener los puntos de vista de los interesados (por ejemplo mediante avisos de prensa, publicidad en los establecimientos, conferencias, discusiones, etc.).*
- ✓ *Definir un periodo de consulta que asegure a los interesados una oportunidad real y adecuada para hacer comentarios al Código.*
- ✓ *Asegurar que la técnica empleada no restrinja el acceso de grupos específicos de interesados (por ejemplo, en el caso de personas con discapacidad o lengua distinta al inglés, puede resultar necesario modificar las fechas de periodo de consulta).*

- ✓ *Asegurar que se tome completa y apropiada consideración de los comentarios vertidos por las personas consultadas.*
- ✓ *Asegurar que los comentarios sean considerados puntualmente y que, en la medida de lo posible, los interesados participen en el ejercicio de modificación del Código que en su caso se realice, como parte del proceso de consulta en curso.*

Definición de "Consulta adecuada"

La Sección 18BB(2) de la Ley señala que el Comisionado sólo podrá aprobar un Código después de cerciorarse que se ha dado adecuada oportunidad al público para hacer comentarios a la propuesta. De acuerdo con los lineamientos, el término "adecuado" es subjetivo y por lo tanto depende de una serie de consideraciones y circunstancias de distinta índole.
Por ejemplo, en el caso de una industria altamente especializada que posea una clientela especifica, no sería necesario consultar con un amplio número de personas, sino que bastaría con que sea consultado el grupo de interesados ya identificado.

En todo caso, el Comisionado requerirá que los proponentes del Código hayan consultado a tantas partes sea posible, de acuerdo con un criterio de racionalidad y tomando en consideración las circunstancias particulares de cada caso.

La Ley da facultades al Comisionado para consultar con cualquier persona que estime conveniente. Esto puede convertirse en un paso medular en el proceso de aprobación, sobre todo cuando los proponentes de un Código no han logrado demostrar fehacientemente que la consulta fue idónea.

Para ayudar a los usuarios a realizar un proceso de consulta exitoso, el Comisionado recomienda revisar las siguientes publicaciones:

- *Getting it Right: Ideas for Consulting Communities, de la División de Asuntos de Consumidores del Departamento del Tesoro, disponible en www.treasury.gov.au/publications*
- *Inclusive Consultation: A practical Guide to Involving People with Disabilities, del Departamento de Servicios Familiares y Comunitarios, disponible en www.facs.gov.au/disability/ood/consgide.htm*

En la mayoría de los casos, se requerirá que los proponentes del Código realicen una consulta pública durante al menos seis semanas (el primer día de la consulta no debe coincidir con un día festivo o ser fin de semana).

Para auxiliar al Comisionado en su decisión sobre la idoneidad de la consulta, los proponentes deberán presentar una declaración junto con la solicitud de aprobación de Código, en el cual expresarán:

i) la fecha de inicio y término de la consulta;
ii) las personas afectadas o interesadas en el Código de Privacidad;
iii) el método empleado en la consulta;
iv) una lista de las personas que hicieron comentarios al Código propuesto;
v) las modificaciones realizadas al Código propuesto en caso de haberlas;
vi) en su caso, un resumen de los asuntos manifestados durante la consulta por los afectados o interesados que no hayan sido resueltos;
vii) las razones por las cuales no fue añadido ningún comentario al documento final; y
viii) un listado de las organizaciones que probablemente adoptarían el Código propuesto.

Equivalencia del Código de Privacidad con los NPPs

Como se mencionó anteriormente, para que un Código pueda ser aprobado debe mantener al menos el mismo nivel de protección que ofrecen los NPPs de la Privacy Act.

Esto significa que los Códigos no tienen que ser, necesariamente, una reproducción de los principios contenidos en la Ley. En lugar de eso, los particulares tienen la oportunidad de modificar estos principios para que se adapten a las necesidades de la organización. De acuerdo con los lineamientos, algunos de los ejemplos de cómo pueden ser modificados los principios son:

1) añadiendo elementos a los principios existentes a fin de elevar el nivel de protección de la privacidad;

2) *incluyendo lenguaje específico de la industria, como una guía de los principios, a efecto de adaptar los principios a las necesidades del sector; y/o*
3) *replanteando las obligaciones contenidas en los NPPs de una forma alternativa.*

Para evaluar este requisito en un Código de Privacidad, el Comisionado revisa los principios contenidos en las cláusulas como un todo, y no como enunciados aislados, con el fin de comprobar si éstas se complementan brindando una protección a la privacidad al menos equivalente a la contenida en la Ley.

El Comisionado recomienda que los Códigos no denominen a los principios contenidos en ellos como "Principios Nacionales de Privacidad" ("National Privacy Principles") o "PNPs" ("NPPs"). Es importante que los consumidores entiendan claramente que cuando una organización está obligada por un Código ya no le son aplicables los principios predeterminados por la Ley. Otras denominaciones pueden ser utilizadas, como "Principios de Privacidad", "Cláusulas", "Disposiciones" o "Estándares".

Producción de material explicativo

El material explicativo puede ayudar a confeccionar un conjunto de principios de privacidad a las necesidades específicas de un grupo o industria. En ocasiones es recomendable que estos materiales incluyan ejemplos prácticos o exposiciones escritas acerca de cómo cumplir con los principios.

En el supuesto de que el Código no establezca mecanismos para solucionar diferencias, o atender quejas, la Ley dispone que será el Comisionado quien resolverá cualquier reclamación derivada del Código.

En este caso, el procedimiento se regirá por lo dispuesto por la Ley. Sin embargo, al evaluar si ha o no existido una violación al Código, el Comisionado puede tomar en consideración, además de los estándares contenidos en el Código, el material explicativo preparado en relación a éste. En caso de no existir ningún material explicativo, cualquier lineamiento emitido por el Comisionado (como los lineamientos sobre los principios de privacidad) podría ser útil para interpretar el Código de Privacidad.

Además, este tipo de materiales puede servir para orientar la función de los árbitros en materia de tratamiento de quejas, cuando son previstos por los Códigos de Privacidad.

Cobertura

La Ley establece que los Códigos deberán especificar a las organizaciones obligadas por el Código, o bien, disponer la forma en que se identificará a las organizaciones que les será vinculante.

En este sentido, el Administrador del Código[195] debe mantener un registro transparente y actualizado de los miembros del Código que además sea accesible.

La Ley establece que el Comisionado deberá llevar un registro de los Códigos aprobados, dejando a su discreción la forma en que éste registro será administrado. En la actualidad, el Comisionado ha optado por llevar el registro en la página web de la Oficina del Comisionado de Privacidad. A su vez, la página del Administrador del Código de Privacidad deberá enlistar a todos los miembros del Código o bien, indicar si el propio Código en su contenido los señala. La página web del Administrador deberá contener un link directo a la página del Comisionado (www.privacy.gov.au).

El Comisionado también solicita a las organizaciones que mantengan un sistema de información disponible para personas que no tengan acceso a internet. Esto puede lograrse a través de una versión impresa del listado / página web, que se ponga a disposición de los individuos mediante solicitud.

Es importante tomar en consideración que la omisión de mantener actualizado el registro de miembros puede constituir prima facie una causal de revocación del Código.

En la mayoría de los casos, el Comisionado puede solicitar que los Códigos dispongan sobre el establecimiento y adecuado financiamiento de un Administrador.

[195] El Administrador es el órgano encargado de vigilar el cumplimiento y operación del Código, y cuando así se establezca, de los procedimientos de tratamiento de quejas.

Los Códigos deberán disponer sobre el establecimiento de un registro que se mantenga actualizado sobre los miembros. El Comisionado también puede solicitar se establezca la forma en que dicha actualización será realizada.

Membresía voluntaria

La pertenencia a un Código debe ser siempre de manera voluntaria.

Cabe destacar que en la mayoría de los casos, el Comisionado puede considerar un Código como voluntario cuando una asociación de industria condiciona la membresía a la asociación al cumplimiento del Código de Privacidad. No obstante, en los casos en que la pertenencia a una asociación es exigida por ley (por ejemplo, tratándose de organismos de acreditación profesional) ningún Código de Privacidad debe considerarse como requisito para obtener la membresía.
Aquellas organizaciones que opten por no pertenecer a un Código de Privacidad, se regirán por los principios de privacidad contenidos en la Ley.

Finalmente, para dar cumplimiento a este requisito, se espera que en la solicitud para la aprobación de un Código de Privacidad se manifieste la forma en que se garantizará que la pertenencia a un éste será de carácter voluntario. Asimismo, se espera que esta manifestación explique también los procedimientos por los cuales una organización estará obligada por un Código, o dejará de estarlo (opt-in, opt-out).

Revisión

Otro de los elementos que son considerados con especial atención por el Comisionado a la hora de revisar un Código de Privacidad, es que el mismo contenga un mecanismo de revisión. Se aconseja también que dicho procedimiento permita la inclusión de comentarios por parte de otras dependencias públicas, consumidores e interesados relevantes, así como de la Oficina del propio Comisionado.

Si bien este requisito no se encuentra contenido en la Ley, puede ser tomado en consideración por el Comisionado como una causal de revocación.

A fin de que este requisito sea cumplido de forma satisfactoria, los Códigos deberán:

1) *establecer un proceso de revisión de Código que tenga lugar al menos cada tres años;*
2) *contener una declaración por la cual se comprometan los recursos necesarios para la revisión del Código; y*
3) *requerir al Administrador del Código que emita una contestación al reporte de revisión independiente y presentarla ante el Comisionado dentro de los 30 días siguientes a la finalización del reporte.*

Códigos temporales

En el caso de aquellos Códigos que tengan una vida limitada, el Comisionado requerirá que éstos señalen de forma clara y expresa, cuándo o bajo que circunstancias dicho Código dejará de tener efectos. Asimismo, requerirá que éstos expresen los mecanismos por los cuales se comunique a los consumidores de la terminación del Código.
La omisión en este sentido tiene como consecuencia la no aprobación del Código.

Códigos con alcance limitado

De acuerdo con la Ley, se permite la aprobación de Códigos que cubran únicamente ciertos aspectos u operaciones de las organizaciones. Por ejemplo:

- *Un tipo específico de información personal.*
- *Una actividad específica o clase de actividades.*
- *Un sector de la industria o profesional específico.*

En ese sentido, el Comisionado requerirá que el Código establezca claramente, de forma que no se generen confusiones a los interesados o consumidores respecto de qué tipo de información, actividades o profesiones habrá de cubrir.

Redacción

De acuerdo con los lineamientos, la redacción de un Código de Privacidad es muy importante en la medida en que puede evitar malas aplicaciones o confusiones.

Para ello, se recomienda utilizar un lenguaje entendible y claro, evitando utilizar léxico demasiado especializado o ambiguo. Asimismo, la enumeración de los párrafos puede facilitar su consulta y aplicación.

Procedimientos para el tratamiento de quejas

Los proponentes de un Código pueden confiar en el Comisionado de Privacidad para resolver las quejas que sean presentadas bajo la aplicación de un Código, quién resolverá conforme a sus atribuciones de investigación dispuestas en la Ley. No obstante, también pueden optar por diseñar su propio sistema de tratamiento de quejas.

En este último caso, el Código debe cumplir con una serie de requisitos que establece la Ley, los estándares emitidos por el Comisionado de Privacidad, así como con los lineamientos que emita el Procurador General.

1) Estándares establecidos en la Ley (Sección 18BB(3)(a)(i):

Accesibilidad: El esquema debe ser accesible para los clientes, promoviendo el conocimiento sobre su existencia y sin establecer barreras de costos.

Independencia: El mecanismo así como su administración serán independientes de los miembros.

Imparcialidad: La decisión debe fundarse en criterios justos y ser debidamente razonada y motivada.

Eficiencia: El esquema operará eficientemente, dando debido seguimiento a las quejas y asegurando que sean tratadas de la forma más apropiada.

Efectividad: El esquema será efectivo, teniendo adecuados y comprensivos términos de referencia y revisiones independientes de forma periódica sobre su operación.

2) Lineamientos del Comisionado de Privacidad

Quejas Colectivas: El Código deberá establecer procedimientos para aceptar, investigar y resolver sobre quejas presentadas a nombre colectivo.

Admisión de la queja: El árbitro, antes de resolver una queja, deberá cerciorarse de que el solicitante haya presentado previamente el asunto ante el demandando[196]. Aquél, sólo dará trámite a la petición una vez que el demandado contestó y el quejoso no se encuentra satisfecho con la decisión adoptada, o bien, cuando en un término de 60 días el demandado no ha contestado.

Remisión de asuntos al Comisionado: La Ley permite que los árbitros remitan los asuntos que le sean presentados directamente al Comisionado para su resolución. No obstante, el Comisionado no se encuentra obligado a admitir los asuntos, y generalmente es de la opinión de que los árbitros deben solucionar todas aquellas quejas que le sean planteadas, salvo ciertas excepciones:

1) *En aquellos casos donde la competencia del Comisionado de Privacidad se encuentra reservada de forma exclusiva (Información Crediticia, Información de Números de Contribuyentes, Información sobre Condenas Extinguidas[197]) los árbitros deben enviar los asuntos para su resolución por parte del Comisionado.*
2) *En los casos en donde el demandado no forma parte del Código y no es posible identificar otro que le sea aplicable.*
3) *Cuando pudiera haber conflicto de intereses entre las partes y el árbitro.*

Es recomendable que el Código exprese estas circunstancias.

Remisión a otro árbitro: Los Códigos pueden establecer que un árbitro podrá remitir un asunto a otro árbitro, sólo cuando el primero ha considerado que la aplicación de otro Código es más apropiada en el caso concreto o provee mayor protección. Sin embargo, el árbitro deberá primero consultar con el nuevo árbitro y obtener el consentimiento del peticionario de la queja.

[196] Este requisito se funda en la premisa de que el demandado debe tener la oportunidad de resolver el asunto personalmente.
[197] Véase Apartados IIIA, III División 4 de la *Privacy Act*.

Reportes: A fin de garantizar el correcto funcionamiento de los Códigos de Privacidad así como la elaboración de informes por la autoridad, el reporte sobre operación del Código deberá:

1) *establecer que el reporte se entregará al Comisionado por medio del formato electrónico que para tal efecto éste emita;*
2) *establecer que el reporte anual se entregará durante los dos meses siguientes de haber concluido el año fiscal correspondiente;*
3) *disponer que el reporte relativo al mecanismo de tratamiento de quejas incluya:*
   a) *El número de quejas recibidas durante cada mes calendario;*
   b) *El lugar de origen de la queja por Estado o Territorio;*
   c) *La naturaleza de la reclamación haciendo referencia a las disposiciones del Código reclamadas;*
   d) *El número de quejas resueltas a satisfacción de las partes sin haberse emitido una determinación;*
   e) *El número de quejas remitidas a otro árbitro o al Comisionado y las razones de la remisión;*
   f) *El número de quejas sin resolver a la fecha de entrega del reporte y la situación que guarda cada una de ellas, organizadas conforme a los estados siguientes:*
      i) Ninguna acción tomada aún;
      ii) En clarificación de hechos/temas;
      iii) En espera de una resolución;
      iv) En espera de contestación del demandado;
      v) En espera de observaciones del peticionario sobre la contestación de demandado; y
      vi) Arreglo por negociación;
   g) *el número de quejas recibidas durante el año fiscal que fueron remitidas al demandado para su solución directamente con el consumidor;*
   h) *el número de quejas que fueron remitidas nuevamente al árbitro por no haber sido resueltas satisfactoriamente entre el demandado y el solicitante;*
   i) *cualquier problema sistemático que se advierta se desprende de las quejas presentadas;*
   j) *ejemplo de casos relevantes;*
   k) *información sobre cómo el Código asegura un acceso igualitario;*
   l) *una lista de los miembros del Código junto con los cambios que hayan ocurrido durante el último año;*

m) los miembros del Código que no han cumplido sus obligaciones; e
n) información sobre nuevos desarrollos o áreas clave en los cuales se requieran políticas o iniciativas educativas;

4) adicionalmente, deberá indicar el tiempo que tardó cada asunto en ser resuelto.

Solicitud

La solicitud deberá realizarse por escrito o correo electrónico y deberá ser acompañada de la documentación que respalda la petición. Si bien no existe un formato oficial para presentar la solicitud, ésta deberá cumplir con lo siguiente:

1) La solicitud hecha por parte de la organización al Comisionado sobre la aprobación del Código;
2) el título del Código propuesto;
3) el nombre de la organización que solicita la aprobación del Código, así como el nombre de la organización que fungirá como Administradora; y
4) el nombre, domicilio, número de teléfono y correo electrónico (en su caso) de un encargado de la organización que esté calificado para auxiliar a la Oficina de Privacidad en el proceso de aprobación;

Tiempos

Una vez recibida la solicitud, el Comisionado enviará un acuse de recibo a los proponentes dentro de los siguientes siete días.
El proceso de evaluación y aprobación podrá variar dependiendo de varios factores, incluyendo:

1) complejidad del Código;
2) la exhaustividad de la consulta pública realizada (si fuese deficiente, el Comisionado procederá a hacer consultas adicionales);
3) presentación completa de la documentación requeridas; y
4) el número de Códigos en trámite ante el Comisionado.

El tiempo aproximado de respuesta es de dos meses.

Notificación

La notificación de la aprobación o no de un Código, se hará por escrito. La notificación incluirá:

a) la fecha en que se tomó la decisión;

b) las razones por las cuales el Código no fue aprobado;
c) los requisitos que debe cumplir el Código antes de ser aprobado; y
d) los medios de apelación que puedan estar disponibles para los proponentes.

Registro

Una vez que el Código es aprobado se incluye en un registro administrado por el Comisionado, donde se especificará el nombre del Código, el nombre del Administrador y detalles del contacto. Este registro se mantiene actualizado en el sitio web del Comisionado.

Variaciones a un Código

Las organizaciones pueden modificar los términos de un Código, sin embargo, deben solicitar autorización del Comisionado por escrito, remitiendo copia del Código que se pretende reformar.

En el proceso de aprobación, dependerá de la importancia de la modificación para determinar si es necesario hacer una nueva consulta pública o no. Si la modificación es menor, podrá dispensar de este requisito.

Revocación de un Código

Conforme a la sección 18BE, el Comisionado tiene la facultad de revocar un Código de Privacidad aprobado. La revocación puede ocurrir a iniciativa del Comisionado a petición del Administrador del Código.

Los siguientes son algunos de los supuestos que pueden ser tomados en cuenta por el Comisionado para revocar un Código:

- ✓ *Falsedad de la información proporcionada durante el proceso de aprobación.*
- ✓ *Cambio de circunstancias sobre las cuales fue otorgado el Código (por ejemplo, la introducción de controles legales, cambios tecnológicos, actitud de la comunidad, etc.)*
- ✓ *El Administrador no cuenta con los requisitos necesarios para ser autorizado.*
- ✓ *Las decisiones adoptadas por los árbitros son sistemáticamente revocadas en apelación por el Comisionado.*

- ✓ *Una vez que el Comisionado ha informado sobre un mal funcionamiento del Código y el Administrador del Código no ha adoptado medidas necesarias a fin de corregir los errores o estas han resultado infructuosas.*

Cuando el Comisionado advierta alguna de estas situaciones, primero consultará con el Administrador del Código a fin de solucionar el problema. Si este persiste, iniciará un procedimiento de revisión de contenido y operación del Código el cual incluirá las observaciones de la Oficina de Privacidad, Administrador(es) del Código y público interesado. El propósito de la revisión será definir claramente mediante consenso cualquier debilidad del Código o su operación y proponer mecanismos para corregirlo.

En caso de no llegar a un acuerdo, el Comisionado de Privacidad iniciará el procedimiento de revocación, que consistirá en:

1. *Elaboración de un plan de revocación conjuntamente con los interesados. El plan deberá considerar asuntos como el tiempo de la revocación, mecanismos idóneos para informar al público y la solución de cualquier queja que esté pendiente.*
2. *El Comisionado informará al público general sobre la intención de revocar el Código y delimitará los tiempos y circunstancias para hacerlo.*
3. *Se notificará oficialmente al Administrador del Código sobre la revocación.*

En cada caso, el Comisionado evaluará la mejor forma de informar al público sobre la intención de revocar un Código. Si la revocación tiene lugar a solicitud del Administrador, una forma podría ser el llevar a cabo una campaña pública donde se informe a los consumidores sobre la revocación del Código y los efectos que esto podría tener en la protección de su información personal.

Revocación de procedimientos de tratamiento de quejas

En el caso de que el Comisionado advierta que el procedimiento de tratamiento de quejas de un Código se encuentra viciado y el Administrador no presenta las modificaciones correspondientes, el Comisionado podrá revocar el Código de Privacidad, pero sólo podrá hacerlo in toto ya que no puede dejar sin efectos una parte del Código, o modificar la parte correspondiente por el mismo.

IX.- CERTIFICACIÓN

9.1 Marco Jurídico Mexicano

En México, además de los códigos de conducta, el artículo 83 del Reglamento de la LFPDPPP prevé un elemento que podrán incorporar los esquemas de autorregulación, al señalar que, "(…) *los esquemas de autorregulación vinculante* ***podrán incluir la certificación*** *de los responsables en materia de protección de datos personales. En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley.*"

Asimismo, el artículo 85 del citado ordenamiento, señala que los parámetros de los esquemas de autorregulación "…*contendrán los mecanismos para* ***acreditar y revocar a las personas físicas certificadoras****, así como sus funciones; los criterios generales para otorgar certificados en materia de protección de datos personales…"*

De la revisión hecha hasta ahora, se observa que actualmente existen pocos mecanismos de certificación que se asemejen al enfoque que se pretende adoptar por México. Si bien existen el sello de confianza de la AMIPCI, y los Códigos de Conducta de BBVA Bancomer y Grupo Novartis, estos han sido, elaborados de acuerdo con estándares propios.

9.1.1 Reglas para el ámbito de la Normalización

Como se comenta en el epígrafe **4.5** de este trabajo, se puede decir que el tema de la certificación actualmente solo tiene como referencia legal lo dispuesto en la Ley Federal sobre Metrología y Normalización, donde se dice que es el procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales.

Dentro de los esquemas de la Evaluación de la Conformidad, la certificación sirve para determinar el grado de cumplimiento con las normas oficiales mexicanas o la conformidad con las normas mexicanas, las normas internacionales u otras especificaciones, prescripciones o características.

Un primer análisis de estas disposiciones indica que la aplicabilidad de las nociones de certificación (y de acreditación inclusive) se enfoca procedimientos y métodos establecidos en las NOM y/o en su defecto a las normas internacionales; por lo que se podría deducir apriorísticamente que no son aplicables al ámbito de los PARAMETROS.

Sin embargo, son útiles para dar sentido a los parámetros que emitan SE-IFAIPD para el tema de la protección de datos personales; sobre todo si el invocado artículo 83 del Reglamento de la LFPDPPP determina que en caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, es decir, a una evaluación de la conformidad de tercera parte.

El Reglamento de la Ley Federal de Metrología y Normalización dispone en su Título Cuarto “De la Acreditación y Determinación del Cumplimiento”, las reglas para obtener la autorización para operar como entidad de acreditación:

> **ARTÍCULO 71.** Para obtener la autorización para operar como entidad de acreditación, se deberá presentar a la Secretaría la documentación que demuestre el cumplimiento de lo dispuesto en el artículo 70-A de la Ley, y además con los requisitos siguientes:
>
> l. Estar constituida como asociación civil, cuyo objeto social único sea desarrollar tareas de acreditación en el marco de la Ley y del presente Reglamento, en concordancia con las normas o lineamientos internacionales;
>
> II. Detallar la estructura organizacional de la entidad, la que deberá contar cuando menos con una asamblea general, un consejo directivo, una comisión de acreditación, los comités de evaluación necesarios y un Director General.
>
> La representación en la asamblea general y en el consejo directivo, a juicio de la Secretaría, deberá garantizar el equilibrio de las partes interesadas en el proceso de acreditación. Se entiende por partes interesadas a las personas acreditadas, usuarios del servicio, asociaciones de profesionales o académicos, cámaras y asociaciones de industriales o comerciantes, instituciones de educación superior, centros de investigación y las dependencias involucradas en las actividades de acreditación de la entidad.
>
> Las partes interesadas que integren una entidad de acreditación, en ningún caso podrán participar directa o indirectamente en otra entidad de acreditación;
>
> III. Organizar su estructura de acuerdo con las normas o lineamientos internacionales sobre acreditación;
>
> IV. Contar permanentemente con técnicos calificados y con experiencia en los respectivos campos, para manejar el tipo, frecuencia y volumen de trabajo o actividad a desempeñar;
>
> V. Presentar las bases conforme a las cuales se establecerá el padrón nacional de evaluadores, y

VI. Contar con un procedimiento transparente basado en costos y condiciones propias de la entidad de acreditación, que determine las tarifas máximas a que esté sujeta la prestación de sus servicios.

9.1.2 Criterios de la Evaluación de la Conformidad

Para ahondar en estas nociones, son importantes los criterios de la Secretaría de Economía[198], así como la NMX-EC-17000-IMNC-2007[199] que precisa lo que se debe entender por estos conceptos:

2.1
Evaluación de la conformidad
Demostración de que se cumplen los requisitos especificados (3.1) relativos a un producto (3.3), proceso, sistema, persona u organismo.

2.4
Actividad de evaluación de conformidad de tercera parte
Actividad de evaluación de la conformidad que lleva a cabo una persona u organismo que es independiente e la persona u organización que provee el objeto[200] y también de los intereses del usuario en dicho objeto.

5.5
Certificación
Atestación[201] de tercera parte relativa a productos, procesos, sistemas o personas

5.6
Acreditación
Atestación de tercera parte relativa a un organismo de evaluación de la conformidad que manifiesta la demostración formal de su

198 http://www.economia.gob.mx/comunidad-negocios/normalizacion/nacional/evaluacion-de-conformidad
199 Evaluación de la conformidad-Vocabulario y principios generales.
200 Objeto: material, producto, instalación, proceso, sistema, persona u organismo particular al que se le aplica la evaluación de la conformidad.
201 Emisión de una declaración, basada en una decisión tomada después de la revisión, de que se ha demostrado que se cumplen los requisitos especificados.

competencia para llevar a cabo tareas específicas de evaluación de la conformidad.

Por su parte, la NMX-EC-17011-IMNC-2005[202] fija los requisitos generales para los organismos de acreditación que realizan la acreditación de organismos de evaluación de la conformidad (OEC) y la NMX-EC-17024-IMNC-2003[203] establece lo que se debe entender por un proceso, esquema, sistema, organismo de certificación.

9.1.3 Costos de acreditación y certificación

A la fecha de este estudio no se ha contado con un presupuesto concreto o fórmula para determinar el costo de los servicios, tanto de acreditación como de certificación. Es importante esta valoración pues se requieren considerar algunas circunstancias.

En el caso de que una organización existente o creada al efecto pretenda ser acreditada como organismo certificador, requeriría previamente de los servicios de un organismo de acreditación. En México existen instituciones como la Entidad Mexicana de Acreditación, A.C. (EMA)[204], y varios organismos de acreditación reconocidos por esta.

Los factores que un organismo acreditador o bien un organismo certificador deberán tener en cuenta, son los relativos a inspección, cuotas de verificación, gastos de acompañamiento, gastos administrativos, instalaciones adecuadas, equipo especializado, diseño de métodos

[202] Evaluación de la conformidad-Requisitos generales para los organismos de acreditación de organismos de evaluación de la conformidad.
[203] Evaluación de la conformidad- Requisitos generales para los organismos que realizan la certificación de personas.
[204] http://www.ema.org.mx

confiables, sistemas de calidad de mejora continua, auditorías periódicas, personal calificado, etc.

El precio de algunos sellos de confianza, como los vistos en este y otros apartados del estudio dan una idea de los costos que tienen los servicios en esta materia. Sin embargo, si al otorgante del sello o marca se le exige un proceso de acreditación para luego certificar procesos relativos al tratamiento de datos personales por parte de responsables o encargados en el entorno digital, se hace necesario un serio planteamiento sobre el costo-beneficio.

Si bien la certificación que se prevé en el Reglamento de la LFPDPPP es opcional, se debe evaluar si un *esquema de acreditación-certificación* requiere considerar si se crean nuevas obligaciones; hace más estrictas las obligaciones existentes; crea o modifica trámites, afecta derechos o prestaciones para los particulares, establece definiciones, clasificaciones, que conjuntamente con otra disposición afecten o puedan afectar los derechos, obligaciones, prestaciones o trámites de los particulares.

> *"Por eso el análisis costo-beneficio [según la COFEMER], incluye[205]:*
> *"►Cómo se identificaron los costos que se generarán y quién los pagará.*
> *"►Cómo se identificaron los beneficios y quién los recibirá".*

En conclusión: el análisis amerita una valoración en términos monetarios de la relación de todos los costos y beneficios derivados directa o indirectamente del modelo de acreditación y certificación que se proponga; tomando en cuenta los estímulos (motivación) que ofrezcan SE-IFAIPD y atendiendo a la población objetivo de responsables que deberá pagar las certificaciones y sellos de confianza derivados (costo de oportunidad).

[205] Véase http://www.cofemer.gob.mx/images/stories/documents/tabasco/03.pdf

Como antes se indicó, tener muchos requisitos para ser una empresa certificadora, por ejemplo, para protección de menores ha llevado a que solo 5 empresas tengan la autorización de la autoridad en Estados Unidos.

9.2 Postura de la Comisión Europea sobre la Certificación

Sobre este tema la Comisión Europea expresó en el 2010 su preocupación en relación con los mecanismos de autorregulación que actualmente existen en el sistema Europeo, indicando que "l*as disposiciones actuales de la Directiva sobre protección de datos relativas a la autorregulación, es decir, la posibilidad de elaborar códigos de conducta, apenas se han utilizado hasta ahora y las partes involucradas del sector privado no las consideran satisfactorias"*[206].

Asimismo señaló que:

> "…*la Comisión examinará la posibilidad de crear* ***regímenes europeos de certificación*** *(por ejemplo, «distintivos de protección de la intimidad») para los procesos, tecnologías, productos y servicios que sean conformes a las normas de protección de la intimidad. Esta medida no sólo proporcionaría una orientación a las personas que utilizan estas tecnologías, productos o servicios, sino que sería importante en cuanto a la responsabilidad del responsable del tratamiento, pues ayudaría a probar que ha cumplido efectivamente sus obligaciones (véase el apartado 2.2.4). Por supuesto, habría que garantizar la fiabilidad de tales distintivos de protección de la intimidad, así como su compatibilidad con las obligaciones legales y las normas técnicas internacionales".*

[206] Comisión Europea, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, *Un enfoque global de la protección de los datos personales en la Unión Europea*, Bruselas, 4 de noviembre de 2010, COM(2010) 609 final.

Siguiendo esta línea, el 25 de enero del presente año 2012, la Comisión Europea presentó una propuesta para reformar radicalmente el sistema europeo de protección a los datos personales. Mediante la entrega de un "paquete de reformas",[207] esta Comisión ha iniciado un proceso legislativo cuyo fin último es la adopción de un Reglamento General de Protección de Datos[208] que tendría efectos directos e inmediatos en todos los países de UE, unificando con ello la protección de datos personales para que ésta tenga un nivel comunitario.

Una de las modificaciones es precisamente el establecimiento de un sistema de certificación comunitario:

Artículo 39. Certificación

1. *Los Estados miembros y la Comisión promoverán, en particular a nivel europeo, la creación de **mecanismos de certificación** en materia de protección de datos y de sellos y marcados de protección de datos que permitan a los interesados evaluar rápidamente el nivel de protección de datos que ofrecen los responsables y los encargados del tratamiento. Los mecanismos de certificación en materia de protección de datos contribuirán a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores y las diferentes operaciones de tratamiento.*
2. *La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y requisitos aplicables a los **mecanismos de certificación en materia de protección de datos** contemplados en el apartado 1, en particular las condiciones de concesión y revocación, así como los requisitos en materia de reconocimiento en la Unión y en terceros países.*

[207] Véase *"Commission proposes a comprehensive reform of the data protection rules"* en European Commission Directorate-General for Justice: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[208] El nombre completo del Reglamento propuesto es: *Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

> 3. *La Comisión podrá establecer **normas técnicas** para los mecanismos de certificación y los sellos y marcados de protección de datos, y mecanismos para promover y reconocer los mecanismos de certificación y los sellos y marcados de protección de datos. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 87, apartado 2.*

Sin embargo, la reforma aún no ha sido aprobada por lo que no se generado mayor información sobre este nuevo sistema.

9.3 Modelos relevantes de Certificación

Si bien el asunto de la acreditación-certificación sigue siendo objeto de discusión en la Unión Europea y por APEC particularmente, en la actualidad podemos señalar la existencia de dos modelos en práctica , como son el 1) European Privacy Seal y 2) el Privacy Mark del Japón, que se detallaron como esquemas de autorregulación en las entregas previas de este reporte final, pero de cuyas aportaciones en este rubro en especial de la certificación se hace ahora una síntesis.

9.3.1 European Privacy Seal (EuroPriSe)

EuroPriSe comenzó como un proyecto financiado por el programa eTEN[209] de la Comisión Europea en junio de 2007[210] coordinado por el Centro Independiente Regional de Protección de Datos Schleswig-Holstein (ULD).

[209] Para mayor información: http://europa.eu/legislation_summaries/information_society/strategies/l24226e_es.htm [fecha de consulta: 15 de marzo de 2012].

[210] Los países participantes en este proyecto fueron Austria, Francia, Alemania, Eslovaquia, España, Suecia, Holanda y Reino Unido. El monto de la financiación comunitaria fue de 1,239,000 euros y la duración de junio de 2007 a noviembre de 2008. Información disponible en: https://www.european-privacy-seal.eu/about-europrise/from-project-to-service-1/index.html [fecha de consulta: 15 de marzo de 2012].

Gracias al éxito obtenido durante la fase de proyecto, en marzo de 2009 fue adoptado por la ULD como un programa permanente. A partir de entonces, forman parte de este proyecto además ocho *Project Partners*[211].

Este sello certifica que un producto o servicio de TI, facilita su uso de forma compatible con la regulación europea de protección de datos personales, tomando en cuenta la legislación de los Estados miembros. En ese sentido, los criterios de certificación están basados principalmente en la Directiva Europea de Protección de Datos (95/46/EC) y la Directiva sobre Privacidad y Comunicaciones Electrónicas (2002/58/EC).

9.3.1.1 Fases

El modelo de certificación de EuroPriSe está dividido en *dos fases*:

a) En primer lugar, el fabricante o vendedor de un producto o servicio en TI encarga a un experto o centro de evaluación *acreditado*[212] que realice una evaluación del mismo[213]. El experto realizará una comprobación técnica y jurídica del producto o servicio en cuestión en dos pasos: 1) Análisis del producto en relación con la funcionalidad, el área jurídica de aplicación y la realización técnica; y 2) Comprobación de que el producto o servicio cumple con los criterios de evaluación del catálogo de criterios europeos. Finalmente plasmará los resultados en un informe de evaluación confidencial para el fabricante.

[211] Los *Project Partners* son: Agencia de Protección de Datos de la Comunidad de Madrid, la Commission Nationale de l'informatique et des libertés, la Austrian Academy of Science, Ernst & Young, London Metropolitan University, Tüv It, Borking Consultancy y VaF.

[212] Estos expertos y el centro de evaluación deben haber recibido la aprobación de *EuroPriSe*. Actualmente han sido admitidos y registrados más de 130 profesionales en 16 países: Austria, Alemania, Bélgica, Croacia, Finlandia, Irlanda, Países Bajos, Portugal, Eslovaquia, España, Suecia, Suiza, además de Argentina, Taiwán, Reino Unido y Estados Unidos de América. A la fecha Alemania y España son los países que cuentan con más expertos registrados.

[213] Véase https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html

b). En una segunda fase, el fabricante o solicitante presenta el informe de evaluación a un *organismo de certificación*[214], cuya finalidad será garantizar que los certificados responden a un mismo nivel de exigencia.

En consecuencia, el organismo de certificación revisará la metodología, la coherencia y la integridad de los informes. Cualquier diferencia entre los expertos y el organismo se resuelve mediante discusiones entre el fabricante, los expertos y el organismo de certificación:

Aprobado el producto por el organismo de certificación, concederá al solicitante el certificado del Sello de Privacidad Europeo (EuroPriSe) con una vigencia de *dos años*. El solicitante proporcionará un informe público al organismo de certificación, quien lo publicará en la página web de EuroPriSe.

9.3.1.2 Objetos y Sujetos

EuroPrise trata de establecer:

a) Un procedimiento voluntario de certificación válido en toda Europa;

b) Un procedimiento transparente y basado en criterios fiables;

[214] Se trata de una Agencia de Protección de Datos. A la fecha, esta función la ha ejercido la ULD. El encargado de la coordinación y acreditación de estos organismos será el European Privacy Seal Board.

c) La certificación por una autoridad independiente;

d) Demostrar que la privacidad debe ser implementada en productos o servicios;

e) La auditoría de productos o servicios tecnológicos a través de informes públicos.

EuroPriSe está dirigido:

1. A productos y servicios tecnológicos cuya finalidad sea el almacenamiento de datos personales;

2. A expertos jurídicos e informáticos;

3. A Agencias de Protección de Datos que pueden actuar como Autoridades de Certificación.

9.3.1.3 Acreditación/admisión de Expertos

De acuerdo con el EuroPriSe Expert Admission Criteria[215], aquellas personas que deseen obtener la acreditación como expertos deben cubrir los siguientes requisitos[216]:

a) Capacidad: Los requisitos de calificación son:

[215] Disponible en https://www.european-privacy-seal.eu/experts/admission-procedure

[216] En la parte inicial del programa sólo se permitirá la acreditación de personas físicas. No obstante, el proyecto prevé en etapas subsecuentes la posibilidad de acreditar a personas jurídicas. Véase Evaluation Centre, en EuroPriSe Concepts and Definitions. Disponible en https://www.european-privacy-seal.eu/about-europrise/glossary/Wording-and-Definitions%20v1-0.pdf

- Experiencia profesional general: tres años con educación superior o cinco años sin ella[217].
- Experiencia profesional suficiente en auditoría, evaluación relacionada con protección de datos, ya sea en aspectos legales o técnicos.
- Los expertos legales deben acreditar además: título en derecho.

El periodo de experiencia profesional será relativo al tiempo dedicado a asuntos de privacidad. Para el caso de los solicitantes con un grado de educación superior, bastará demostrar una experiencia profesional relacionada con protección de datos de al menos 15 meses completos de trabajo dentro de los últimos 4 años.

Sin un grado de educación superior, se requerirá contar con 30 meses completos de trabajo en los últimos 8 años. En caso de no cumplir este requisito podrá otorgarse una acreditación como "Experto Junior" (*Junior Expert*) siempre que todos los demás requisitos sean cumplidos. Los Expertos Junior podrán llevar a cabo evaluaciones siempre que sea bajo la supervisión y responsabilidad de un Experto de EuroPriSe.

b) Examen: La evaluación de capacitación sirve para entrenar a los expertos en condiciones similares a los proyectos de certificación en la realidad. Dentro de una certificación, la evaluación es dirigida por un experto legal y uno técnico, quienes elaboran un reporte de evaluación a petición del solicitante. Así, la evaluación es el documento nuclear o clave en una certificación.

[217] Esta experiencia puede demostrarse, por ejemplo, si el solicitante se desempeñó como *data protection officer* o especialista/abogado en seguridad informática IT. También los certificados o grados de educación superior, así como examines estatales, certificados profesionales (CISSP, CISM, GAIC), admission a la barra o acreditación de acuerdo con esquemas similares de certificación (por ejemplo, acreditación como auditor ISO 27000 o de Criterios Comunes de evaluación de laboratorios) demuestran experiencia necesaria y pueden ser tomados en cuenta.

La calidad de la evaluación es determinante para el proceso de certificación, su duración y éxito. En consecuencia es requisito indispensable cursar un taller (workshop) ofrecido por EuroPriSe, requiriéndose además completar y presentar un reporte en inglés tras haber culminado la preparación en dicho taller[218].

c) Confiabilidad: La comprobación de la confiabilidad implica la revisión de antecedentes penales (no haber sido condenado por fraude, corrupción, etc.), revisión de comportamiento profesional (por ejemplo, no haber violado códigos de conducta de asociaciones profesionales), así como revisiones de antecedentes financieros (no haber estado en concurso (banca rota), suspensión de actividades, adeudos vencidos, etc.). Estas revisiones pueden ser llevadas a cabo tanto con ayuda de los registros públicos (ejemplo, certificado de no antecedentes penales, no adeudos o buena conducta), así como por declaraciones hechas por los propios expertos solicitantes[219].

d) Independencia: Los expertos deben de ser independientes. Esto implica que los solicitantes no tengan un interés económico o de otra índole (contratos, etc.) con sus clientes y no haber estado involucrados en el desarrollo del producto o del servicio. También se considera que la independencia está comprometida, si el total de las utilidades obtenidas del cliente representan el 80% o más de las ganancias totales del experto. Los expertos también deben demostrar independencia respecto de la estructura interna de su organización.

[218] El próximo taller tendrá lugar en Kiel, en el Hotel Steigenberger Conti Hansa en mayo de 2012. Para mayor información consúltese: https://www.european-privacy-seal.eu/experts/expert-workshops
[219] Véase por ejemplo Self-Declaration Form for Legal Experts. Disponible en: https://www.european-privacy-seal.eu/experts/admission-procedure/Expert%20Admission-self%20declarations-legal-v201009.pdf

e) Auto-declaración: El proceso de admisión requiere la presentación de una declaración sobre competencia, confiabilidad y seguro de cobertura amplia y suficiente que responda por la responsabilidad en que pueda incurrir por daños ocasionados durante las evaluaciones[220].

Validez de la acreditación/admisión: La admisión es otorgada por tres años. Dicha admisión puede prolongarse si el experto conduce una evaluación dentro de tres años posteriores a su admisión. Si no lleva a cabo ninguna evaluación, el experto deberá someterse a un nuevo programa de entrenamiento para actualizarse y demostrar su competencia legal o técnica actual en privacidad y protección de datos.

Ahora bien, para la **prolongación de la admisión** existen diferentes opciones por las que los expertos pueden optar[221]:

1. Presentación de un informe de evaluación: En este caso la admisión se prolonga automáticamente. Si por ejemplo un experto presenta un informe el 15 de marzo de 2011, su admisión se prolonga hasta el 14 de marzo de 2013. Si presenta un nuevo reporte el 16 de agosto de 2012, su admisión se prolonga hasta el 15 de agosto de 2014.

2**. Participación en el programa de entrenamiento de EuroPriSe:** El registro en el programa debe hacerse antes de la culminación de la vigencia de la admisión. El experto debe acudir al curso dentro de los dos meses siguientes a que concluya la admisión previa.

[220] Véase por ejemplo *Self-Declaration Form for Legal Experts: Declaration on Proficiency, Reliability and Insurance.* Disponible en: https://www.european-privacy-seal.eu/experts/admission-procedure/Expert%20Admission-self%20declarations-legal-v201009.pdf
[221] Disponible en: https://www.european-privacy-seal.eu/experts/admission-procedure/Expert%20Admission%20Prolongation%20FS-201012.pdf

3. Herramienta de aprendizaje en línea EuroPriSe (e-learning tool): Similar al programa de entrenamiento pero diseñado para plataforma en línea. El experto debe alcanzar un puntaje de 80% para pasar el examen y obtener la prolongación de su admisión. El examen puede tomarse en cualquier tiempo, y dos veces por año. El examen debe tomarse antes de concluir la admisión, y acreditarse a más tardar dentro del mes siguiente a la terminación de la vigencia.

Una vez admitidos, la información de contacto de los expertos podrá ser publicada en un registro público en el sitio web de EuroPriSe junto con sus intereses especiales y calificaciones a fin de ayudar a los interesados a encontrar a los expertos apropiados.

9.3.1.4 Certificación

Para auxiliar en la certificación de los productos y servicios de IT, el programa EuroPriSe elaboró los Criterios de Certificación EuroPriSe, basados principalmente en la Directiva Europea de Protección de Datos (95/46/EC) y la Directiva sobre Privacidad y Comunicaciones Electrónicas (2002/58/EC).

Este catálogo consiste en una serie de preguntas divididas en cuatro rubros:

I) Visión general y aspectos fundamentales
II) Legitimidad del procesamiento de datos
III) Medidas técnicas y de operación
IV) Derechos de los titulares de los datos

Cabe mencionar que estos criterios no son conclusivos ya que en el proceso de auditoría o evaluación es posible que sea necesario además comprobar otros requerimientos (ejemplo, estándares CEN CWA-15499 para auditorías en materia de protección de datos personales o bien, tratándose de seguridad informática, la ISO 27001).

Algo importante a destacar, es que los procesos de certificación pueden variar según se trate de un producto de TI o bien, de un servicio. Esto es así, ya que la evaluación de un producto de TI implica generalmente el análisis de documentación, evaluación de configuraciones y pruebas del producto en laboratorio, mientras que la evaluación de un servicio de TI puede llegar a implicar la realización de auditorías *in situ.*

9.3.1.5 Pasos del Experto Evaluador

En síntesis, los pasos que el Experto Evaluador debe llevar a cabo son:

Paso 1) Un análisis del Objeto de la Evaluación (ToE) y el ambiente (incluyendo tipos de información procesada, servicios y temas de regulación).

Paso 2) Determinación de los criterios aplicables del Catálogo de Criterios EuroPriSe.

Paso 3) Evaluación de acuerdo con los requisitos establecidos en el paso 2.

Paso 4) Elaboración del Reporte de Evaluación que contenga:

a) Análisis del paso 1;
b) Análisis del paso 2;
c) Evaluación de acuerdo con los requisitos; y

d) Resultado general.

Reportes. Una vez concluido el proceso de certificación, se contará con los siguientes reportes[222]:

1) Reporte de evaluación confidencial elaborado por el experto técnico y el experto legal.
2) Un reporte sintetizado que será público, escrito por los propios expertos, resumiendo los hallazgos más relevantes y su evaluación. Este reporte es elaborado en colaboración con el Organismo de Certificación y el solicitante y será publicado en la página de EuroPriSe.
3) Un reporte de certificación, elaborado por el Organismo de Certificación, resumiendo todos los detalles necesarios del proceso de certificación. Es confidencial y servirá solo para propósitos internos.

9.3.2 Privacy Mark System de Japón[223]

Debido a la demanda creciente de medidas efectivas para la protección de la información personal que pudieran ser implementadas tan pronto como fuera posible, así como por instrucciones del Ministro de Economía de Japón, JIPDEC (Japan Information Procesing Development Corporation) una asociación privada sin fines de lucro, creada para impulsar el desarrollo y la seguridad de las nuevas tecnologías, desarrolló el Sistema PrivacyMark, iniciando sus operaciones en abril de 1998.

[222] Véase EuroPriSe, Concepts and Definitions, p. 4.
[223] http://privacymark.org/

El mecanismo de certificación de PrivacyMark es muy similar a cualquier sello de confianza, pues consiste en conceder el derecho de desplegar y utilizar el sello "PrivacyMark" a las empresas que cumplan con una serie de requisitos, durante un plazo renovable de *dos años*.

9.3.2.1 Marco legal

El 30 de mayo de 2003, en Japón fue promulgada la Ley de Protección de Datos personales (Ley No. 57 de 2003), la cual establece por primera vez obligaciones generales para el sector privado.

El sello PrivacyMark fue ajustado a fin de servir como una herramienta útil a la hora de demostrar el cumplimiento de la normativa aplicable por parte de las empresas en materia de protección de datos personales. Además, el sistema se encuentra de conformidad con los Estándares Industriales Japoneses (JIS Q 15001:2006) (Personal Information Protection Management System – Requirements) emitidos por el Ministerio de Economía de Japón.

Cabe mencionar que JIPDEC obtuvo su acreditación en junio de 2005 por parte del Ministerio de Economía, Comercio e Industria para funcionar como una Organización Autorizada para la Protección de Información Personal, de acuerdo con el artículo 37 de la Ley de Protección Datos, lo que le permite realizar determinadas funciones con valor legal en materia de privacidad y datos personales[224].

[224] Article 37 (1) A juridical person (which includes an association or foundation that is not a juridical person with a specified representative or manager; the same applies in (b) of item (iii) of the next article) that intends to conduct any of the businesses enumerated in the following items for the purpose of ensuring the proper handling of personal information by a business operator handling personal information, may be authorized as such by the competent minister:

9.3.2.2 Operación y Desarrollo

La operación y el desarrollo del sistema PrivacyMark están a cargo de JIPDEC, quien a su vez puede acreditar a asociaciones, empresas y organizaciones que deseen proporcionar el servicio de certificación PrivacyMark como organismos de evaluación de la conformidad.

Para ello, las empresas que deseen brindar este servicio deben someterse a una evaluación directamente ante JIPDEC. Si conforme a los criterios de evaluación de JIPDEC la empresa cumple con los requisitos para ser acreditada, se celebra un contrato con la empresa de acuerdo con los formatos previamente establecidos[225].

Mediante este contrato JIPDEC otorga una licencia de uso temporal a la entidad evaluadora, que le permite el uso del PrivacyMark. Además, JIPDEC entrega a la empresa un Certificado de Acreditación de PrivacyMark. La vigencia del contrato es de *2 años* contados desde la fecha de cierre del contrato.

9.3.2.3 Requisitos para ser acreditado como organismo de evaluación de la conformidad (Conformity Assesment Body).

Pueden fungir como Organismos de Evaluación de la Conformidad (OEC) las asociaciones comerciales y otras organizaciones (sociedades civiles y

(i) The processing under the provision of Article 42 of complaints about the handling of personal information of such business operations handling personal information as are the targets of the business (hereinafter referred to as "target entities")
(ii) The provision of information for target entities about the matters contributing to ensuring the proper handling of personal information.
(iii) In addition to what is listed in the preceding two items, any business necessary for ensuring the proper handling of personal information by target entities

[225] Este contrato debe ser celebrado dentro de los tres meses siguientes a la acreditación, de lo contrario, ésta perderá validez.

mercantiles) dedicadas al manejo de datos personales, siempre que cumplan los requisitos siguientes:

1) Contar con recursos suficientes, incluyendo personal de tiempo completo para las revisiones y evaluaciones que implica la correcta operación de PrivacyMark.

2) Contar con experiencia suficiente sobre el manejo y protección de datos personales.

Los documentos necesarios para solicitar la acreditación como Organismo de Evaluación de la Conformidad son:

1) Formato de solicitud,
2) Copia certificada del acta constitutiva,
3) Estatutos de la asociación,
4) Lineamientos de la industria.

Además deberá ser presentada la siguiente información:

- ✓ Nombre
- ✓ Nombre del representante
- ✓ Dirección
- ✓ Número de teléfono
- ✓ Número de empleados
- ✓ Número de miembros
- ✓ Documentos sobre la Seguridad de los Datos Personales
- ✓ Documentos sobre el Sistema interno de revisión, evaluación y certificación de Privacy Mark

- ✓ Nombre y posición del personal de tiempo completo encargado de operar el Privacy Mark
- ✓ Nombre de la unidad del personal de tiempo completo de Privacy Mark
- ✓ Nombres de los órganos/agencias relacionadas

De acuerdo con el artículo 24 de las *Rules for the Establishment and Operation of the PrivacyMark System* (REOPS), no podrán ser acreditadas como organismos evaluadores aquellos que se ubiquen en alguno de los siguientes supuestos:

1) Se les haya negado la acreditación como organismo evaluador dentro de los tres últimos meses previos a la solicitud.

2) Aquellos a los que se les haya retirado la acreditación como organismos evaluadores dentro de los dos últimos años[226].

3) Las organizaciones que no cumplan los requisitos establecidos en el párrafo primero del artículo 5; esto es, ser una asociación empresarial, empresa privada u otro similar, con experiencia suficiente y reconocida en el manejo y protección de datos personales.

La información debe presentarse ante el Organismo de Acreditación (JIPDEC) la cual evaluará la información conforme al citado *Criteria for PrivacyMark Conforminity Assessment Body.*

Para acreditar a una empresa como Organismo Evaluador, JIPDEC tomará en cuenta, además de las causas establecidas en el artículo 24, lo siguiente:

[226] Las causales de retiro de la acreditación se encuentran en las REOPS.

1) La existencia de una estructura clara y completa, así como de una base responsable, necesaria para la realización de las actividades de certificación de PrivacyMark.

2) La ausencia de factores internos y externos que puedan obstaculizar las actividades del órgano encargado de evaluar la conformidad de PrivacyMark, así como el mantenimiento de la confiabilidad.

3) La designación de un punto permanente de contacto para las atenciones de quejas, consultas, etc. relacionadas con las certificaciones de PrivacyMark.

4) Medidas de seguridad, incluyendo aquellas necesarias para mantener la confidencialidad y prevención de filtraciones hacia el exterior, respecto de la documentación y cualquier otra información proporcionada por las empresas durante los procedimientos de certificación.

Cuando sea especialmente necesario, JIPDEC podrá solicitar que el solicitante permita una revisión en sus establecimientos.

La determinación de JIPDEC sobre la acreditación es notificada al solicitante dentro de un mes, contado desde la fecha de presentación de la solicitud. Cumplido lo anterior, el organismo evaluador acreditado debe elaborar un reglamento propio a fin de operar el Sistema PrivacyMark, los cuales deben contemplar disposiciones equivalentes al menos a los capítulos 2 a 4 de los *Rules for the Establishment and Operation of the Privacy Mark System*. Dichos lineamientos deberán ser registrados ante JIPDEC.

Una vez acreditada la organización es registrada y publicada en el sitio web de JIPDEC. Para ello, JIPDEC mantiene un registro en línea que muestra la información siguiente:

1) Nombre de la organización acreditada y de su representante

2) Dirección

3) Descripción del negocio

4) Fecha de acreditación

5) Información sobre el agente responsable así como de la unidad o punto de contacto designado para atender consultas o quejas

Cuando sea necesario para la operación adecuada del Sistema PrivacyMark, JIPDEC puede requerir a los organismos acreditados le presenten informes sobre la situación que guardan sus operaciones. Este reporte podrá implicar revisiones por parte de JIPDEC de las instalaciones del organismo acreditado.

Cuando de las revisiones realizadas se advierta la necesidad de adoptar medidas específicas, JIPDEC, mediante deliberación del Comité de PrivacyMark, puede recomendar o requerir al organismo acreditado adoptar dichas medidas.

En todo caso, JIPDEC se reserva el derecho de retirar la acreditación en los siguientes supuestos:

a) Cuando se adviertan distorsiones o irregularidades en la documentación de solicitud;
b) El organismo acreditado falsee información en los reportes que JIPDEC le solicite; o bien, cuando no atienda, sin causa justificada, los requerimientos que éste le haga; y cuando
c) Sobrevenga una causal de imposibilidad para realizar las funciones, como las que se refiere el párrafo 3 del artículo 24.

Una vez cancelada la acreditación, el organismo debe devolver el certificado de acreditación a JIPDEC. La decisión es publicada en el registro de organismos acreditados de JIPDEC.

La cancelación de una acreditación de un organismo evaluador, de ningún modo deja sin efectos las certificaciones que éste haya hecho. Sin embargo, JIPDEC, en estos casos como en otros, puede tomar las medidas necesarias para supervisar su funcionamiento de acuerdo con el artículo 36 de las REOPS.

Por su parte, JIPDEC puede llevar a cabo directamente las funciones de certificación, en los casos en que una empresa solicitante no se ubique en el campo de especialidad de los organismos evaluadores que se encuentren funcionando a la fecha.

9.3.2.4 Requisitos para ser una empresa certificada y obtener el Sello PrivacyMark

El Sistema PrivacyMark está diseñado para evaluar y certificar empresas que operen en Japón. Para ser acreedora al Sello PrivacyMark, las empresas deben cumplir con lo siguiente:

1) Establecer un sistema de protección y administración de la información personal, de conformidad con la JIS Q 15001 (revisada en 2006).

2) No encontrarse en alguno de los siguientes supuestos:

a) Haber solicitado la revisión y haber sido rechazado durante los tres meses previos a la nueva solicitud;
b) Que su certificación haya sido revocada o el uso del sello cancelado dentro del año anterior a la solicitud;
c) No haber completado en el periodo de prueba los requerimientos en relación con violaciones a los estándares sobre filtración de información personal o la invasión de derechos e intereses de las personas; y
d) En cuanto a los miembros ejecutivos y operadores, que no hayan transcurrido al menos dos años desde el cumplimiento de una sentencia recaída por violaciones a la Ley de Protección de Datos Personales.

La empresa privada que solicite la certificación de PrivacyMark, debe presentar la siguiente documentación ante el organismo evaluador, o en su caso, ante JIPDEC:

- La solicitud en el formato predeterminado;
- Documento oficial que certifique la existencia del solicitante;
- Acta constitutiva y estatuto de la empresa, así como un documento en donde se explique la relación del objeto del negocio y el tratamiento de los datos personales;
- Lista de directores y auditores;

- Sistema de Administración y Protección de la Información Personal;
- Otras regulaciones relacionadas con la información personal;
- Declaración de que el solicitante no se encuentra dentro de uno de los supuestos establecidos en el artículo 8; y
- Cualquier otra documentación que el organismo evaluador o JIPDEC consideren necesario.

Solo pueden ser certificadas aquellas empresas que tengan establecimientos en Japón. Solo en determinados casos, las empresas extranjeras podrán ser certificadas a través del PrivacyMark System.

Cuando se presente la solicitud, la empresa deberá pagar los honorarios previamente establecidos ya sea al organismo evaluador o a JIPDEC según se trate. El organismo evaluador o JIPDEC en su caso no inicia el procedimiento de revisión y evaluación hasta que los honorarios hayan sido pagados y, si los honorarios no son pagados dentro del mes siguiente, el procedimiento de certificación es cancelado. En estos casos, los solicitantes no pueden demandar la devolución de los honorarios pagados.

El sello PrivacyMark es otorgado solamente a aquellas empresas que cumplan con los requisitos establecidos en la JIS Q 150001: 2006 y la legislación en materia de protección de datos personales. Para ello, el organismo certificador, o JIPDEC directamente, realiza un proceso de investigación y evaluación, haciendo énfasis en lo siguiente:

1) Presencia de un Sistema de Administración de Datos Personales[227] para la protección y seguridad apropiada de la información personal.
2) Designación de un administrador o encargado de los datos personales, designación clara de las responsabilidades y los roles para la seguridad de la información, y presencia de otros sistemas necesarios para la protección de datos.
3) Capacitación al menos una vez al año para aquellos que recojan, usen, o provean información personal.
4) Establecimiento de una unidad especial para la atención de usuarios y clientes, incluyendo solicitudes, quejas y consultas.
5) Presencia de medidas de seguridad de la información apropiadas para evitar accesos no autorizados, filtración de la información, así como para mantener la confidencialidad.
6) Presencia de medidas apropiadas para garantizar de seguridad de la información cuando ésta es proporcionada externamente o su procesamiento se realiza mediante subcontratación, incluyendo la conclusión de los contratos relacionados con la información personal, y la división de responsabilidades.

Esta revisión puede implicar la realización de investigaciones en el establecimiento del solicitante. Los gastos que esta revisión implique, incluyendo viáticos, son pagados por el solicitante.

En caso de no obtener la acreditación, el solicitante puede volver a someter su petición ante JIPDEC una vez que hayan transcurrido tres meses desde la decisión de rechazo.

[227] Privacy Management System, es un requisito necesario establecido por la JIS Q 15006:2006.

En caso de que se presenten cambios en los asuntos reportados en los documentos de la solicitud, la empresa privada debe dar aviso rápidamente al organismo evaluador o a JIPDEC. En el caso de que una empresa certificada se fusione o divida, el organismo evaluador o JIPDEC volverá a evaluar y decidir si la nueva empresa fusionada o dividida puede recibir la certificación de PrivacyMark.

El organismo evaluador (o JIPDEC en su caso) debe mantener registros para administrar y publicitar a las empresas que han obtenido la certificación de PrivacyMark, señalando la siguiente información:

1) Nombres de las empresas privadas y de sus representantes

2) Dirección de la empresa

3) Descripción de las actividades relacionadas con el tratamiento de datos personales

4) Nombre y dirección del organismo evaluador que otorgó la certificación

5) Fecha de certificación, de su renovación en su caso, y el periodo de vigencia

6) Fecha de conclusión del contrato

7) Información de la unidad de contacto para atención a clientes

9.4 Sistema de Acreditación de APEC

Como se comentó en la fase anterior a este trabajo, al tratar el tema del Cross-Border Privacy Rules (CBPR) System de APEC, entre las finalidades principales del Marco de Privacidad de APEC se encuentra el desarrollo de la protección a la privacidad y a la información personal, especialmente para evitar las consecuencias dañinas que ocasionan las intrusiones no autorizadas y el mal uso de la información.

La idea es que las organizaciones globales que obtienen, acceden, usan y procesan datos en las Economías de APEC, desarrollen e implementen enfoques uniformes dentro de sus propias organizaciones para el acceso y uso global de los datos personales.

Así, el apartado IV del Marco de Privacidad llama a las Economías a desarrollar un sistema voluntario de reglas transfronterizas de privacidad para la región (Cross-border Privacy Rules System o CBPRs) en la que participarán las organizaciones que manejen datos personales entre las Economías miembro de APEC.

Este sistema, aprobado en noviembre de 2011[228], se compone de una serie de procedimientos y mecanismos para hacer efectiva la protección de la privacidad en la transferencia internacional de datos personales, a través de procedimientos de certificación de organizaciones y el cumplimiento eficaz de los principios de APEC.

[228] Véase APEC, *Declaración de Honolulu: Hacia una economía regional perfecta*, Noviembre 12-13 2011, Honolulu, Hawai, Estados Unidos.

Las organizaciones que decidan participar en el Sistema CBPR deberán implementar políticas y prácticas de privacidad que sean consistentes con el programa CBPR respecto de toda la información personal que obtengan o reciban y que esté sujeta a la transmisión transfronteriza a otra economía participante de APEC.

Estas prácticas y políticas de privacidad serán evaluadas por un Agente Responsable reconocido por APEC, quién para otorgar la certificación, se asegurará de que la organización cumpla con los requisitos que establece el programa CBPR.

Las Economías podrán solicitar al Panel Conjunto de Vigilancia (JOP) la acreditación de Agentes Responsables para que operen en su jurisdicción, que podrán ser la propia Autoridad Competente sobre Privacidad, una organización privada de su Economía, o bien, una organización que opere como Agente Responsable en otra Economía.

La acreditación por parte de APEC como Agente de Responsabilidad solo durará un año, por lo que, un mes antes del vencimiento deberá solicitarse la renovación. Además el JOP se reserva la facultad de revisar el cumplimiento de los Agentes Responsables, solicitar a las Autoridades Competentes iniciar investigaciones sobre su funcionamiento, y solicitar la suspensión como Agente Responsable en cualquier tiempo.

Una vez que una organización ha sido certificada por un Agente Responsable para participar en el sistema CBPR, estas prácticas y políticas de privacidad se convierten en vinculantes para el Participante y podrán hacerse efectivas por la autoridad competente a fin de asegurar la conformidad con los requisitos del programa CBPR.

Asimismo, aquellas organizaciones que hayan obtenido la certificación anual de participación en el CBPR aparecerán dentro de un listado de organizaciones certificadas en el sitio web de APEC[229], con la finalidad de hacer saber a los consumidores u otros interesados sobre sus políticas de privacidad y su adecuación con el sistema de APEC.

Si bien la participación de las economías en el CBPR es voluntaria, para que el sistema sea efectivo, es necesario que sus reglas puedan ser ejecutables por los Agentes Responsables y las Autoridades Competentes. Es por ello que en ocasiones podrá resultar necesario que las Economías adecuen sus ordenamientos normativos a fin de facilitar y hacer efectivo su cumplimiento.

9.4.1 APEC Data Privacy Pathfinder

Las Economías de APEC aprobaron en la reunión de Sidney, Australia, en 2007, el APEC Data Privacy Pathfinder, diseñado al interior del Sub-grupo de Privacidad[230]. Este acuerdo consiste en un conjunto de compromisos dirigidos a desarrollar el Sistema de Reglas de Privacidad Transfronterizas (CBPRs).

Como ya se señaló, el objetivo del sistema de protección de datos de APEC es incentivar a las organizaciones a que desarrollen sus propias reglas de privacidad que regulen el flujo de información personal internacional.

Las Economías de APEC reconocieron que las organizaciones, (empresas, compañías, etc.) tienen un interés muy fuerte en la protección de la información personal de sus clientes y que muchas de las compañías ya han

[229] Véase Proyecto 4, APEC Website Guidelines, 2009/SOM1/ECSG/DPS/012.

[230] El Sub-Grupo de Privacidad de APEC fue creado en 2003 dentro del Grupo de Manejo de Comercio Electrónico (ECSG) de APEC para abordar todos los temas relacionados con privacidad. El grupo se reúne dos veces al año y reporta sus avances al ECSG quien en última instancia reporta directamente a los Ministros de APEC.

diseñado procedimientos y prácticas empresariales para asegurarse que la información personal se encuentra protegida.

Para lograr sus objetivos, el APEC Data Privacy Pathfinder tiene como propósito el desarrollo de nueve proyectos[231], agrupados en cuatro categorías que corresponden a los objetivos primarios del CBPRs:

1) Autoevaluación

✓ Proyecto 1. Guía de autoevaluación para las empresas.

2) Revisión del cumplimiento

✓ Proyecto 2. Criterios de reconocimiento de los Agentes Responsables del sector público o privado.
✓ Proyecto 3. Proceso de revisión de cumplimiento de los CBPRs.
✓ Proyecto 4. Directorios y contactos de los Agentes Responsables y organismos.

3) Reconocimiento/aceptación

✓ Proyecto 5. Directorio de las autoridades de protección de datos personales y privacidad.

4) Resolución de conflictos y aplicación

✓ Proyecto 6. Formato para la realización de acuerdos de cooperación.
✓ Proyecto 7. Formato para el manejo de quejas transfronterizas.

Adicionalmente, existen otros dos proyectos que no corresponden directamente a uno de las cuatro finalidades primordiales del CBPRs: Proyecto 8. Alcance y gobernanza del sistema CBPRs y Proyecto 9. Implementación de un programa piloto.

[231] Véase APEC Data Privacy Pathfinder: Project Work Plan, 2007/SOM3/ECSG/DPS/004.

9.4.2 CBPR Intake Questionnaire (Cuestionario de Auto-evaluación)[232]

Este documento auxiliará a los Agentes Responsables en su función de certificación ya que será el primer paso en el proceso de evaluación para determinar si las políticas de privacidad de organización son suficientes o no para participar en el CBPRs.

El cuestionario está dividido en nueve apartados que corresponden a los principios del Marco de Privacidad de APEC. Cabe señalar que este cuestionario podrá ser complementado por los Agentes Responsables para obtener una mayor claridad sobre puntos específicos durante el proceso de revisión a una organización.

Los nueve apartados básicos son:

I.- General: Requiere información general de la empresa Solicitante (nombre; lista de afiliados o subsidiarias; datos generales de contacto; tipo de información que cubrirá la certificación; países en que se obtiene información; y países a los que se transfiere información).

II.- Aviso (preguntas 1-4): Esta sección está enfocada a asegurar que los particulares conocen las políticas de privacidad de la empresa Solicitante, hacia donde se transferirá la información, el propósito y uso de la información, así como asegurar que, sujeto a las consideraciones establecidas en el apartado II, los particulares saben en qué momento su información personal es recopilada, hacia donde es transferida, el propósito y uso que se le dará[233].

[232] Véase Proyecto 1, CBPR Intake Questionnaire, 2011/SOM1/ECSG/DPS/020.
[233] Nota: Esta sección contiene un apartado de situaciones en donde el principio de Aviso no es exigible, o no aplica.

III.- Limitaciones a la obtención (preguntas 5-7): Está sección está dirigida a asegurar que la recopilación de información está limitada a aquellos propósitos declarados por la organización.

IV.- Uso de la información personal (preguntas 8-13): Las preguntas en esta sección buscan inquirir acerca de si el uso de la información personal está restringido a los propósitos por los cuales fue obtenida, o bien, otros fines que sean compatibles o estén relacionados con el principal. La aplicación de este principio requiere considerar la naturaleza de la información, el contexto de la obtención, y el uso que se le pretende dar. El criterio fundamental para determinar si un propósito es compatible o relacionado con el principal, es si el uso extendido surge de, o sirve para, alcanzar el primero. El uso de la información personal para "propósitos compatibles o relacionados" se puede extender, por ejemplo, a asuntos como la creación y uso de una base centralizada de datos para manejar personal de manera efectiva y eficiente, así como procesar el pago de empleados por un tercero.

V.- Elección: Las preguntas de esta sección se relacionan con el principio de elección sobre el uso, recolección y revelación de la información personal. No obstante, este principio reconoce que existen ciertos supuestos en donde el consentimiento puede ser implícito, o donde puede que no sea necesario proveer de un mecanismo para ejercitar el derecho de elección. Para tal efecto, la sección proporciona un listado de estas situaciones.

VI.- Integridad de la información (preguntas 21-25): Esta sección inquiere si el controlador de la información mantiene la fidelidad y completitud de los registros y si los mantiene actualizados.

VII.- Garantías de seguridad (preguntas 26-35): Busca asegurar que la información personal sea protegida mediante garantías razonables de seguridad a fin de prevenir pérdidas o acceso, destrucción, uso, modificación o revelación no autorizados.

VIII.- Acceso y corrección (preguntas 36-38): Las preguntas de esta sección buscan conocer si los particulares tienen la posibilidad de acceder y corregir su información. Esta sección incluye condiciones específicas de lo que se consideraría razonable para la provisión de acceso directo a la información y requiere que existan mecanismos para comprobar la identidad del usuario previo el otorgamiento del acceso. Los detalles de los procedimientos de acceso dependen de la naturaleza de la información en cuestión. Por esta razón, en ciertos casos puede resultar imposible, impracticable o innecesario el cambio, supresión o eliminación de información.

IX.- Responsabilidad (preguntas 39-51): Están dirigidas a saber si el Solicitante es responsable del cumplimiento de los principios anteriores. Adicionalmente, busca conocer si también es responsable cuando transfiere información a terceros, asegurándose de que el receptor protegerá la información de acuerdo con dichos principios. Como en los supuestos anteriores, existen excepciones a esta regla, como cuando no hay una relación directa entre el transmisor y el receptor. En esos casos, se puede optar por otros mecanismos, como la obtención del consentimiento del titular de los datos. Además, en los casos en donde la revelación es requerida por la ley del país en cuestión, la empresa sería excusada de cualquier obligación de debida diligencia o consentimiento.

9.4.3.- Accountability-Agent Recognition Criteria[234]

Estos criterios fueron publicados por el foro en el año 2011 y establecen los requisitos necesarios para que un Agente Responsable pueda participar en el CBPRs de APEC. De acuerdo con el documento, el interesado en participar como Agente Responsable debe presentar este formato y la documentación de soporte necesaria para una revisión inicial a la oficina o autoridad gubernamental correspondiente. La oficina o autoridad enviará toda la información recibida al Panel Conjunto de Vigilancia (Joint Oversight Panel o JOP) a efecto de que el Solicitante sea reconocido por APEC como Agente Responsable del CBPRs.

Los criterios que deberán ser cubiertos por los Agentes Responsables son:

Conflicto de intereses:

1) Requisitos generales:

   a) Un Agente Responsable debe estar libre de conflictos de intereses reales o potenciales a fin de participar en el CBPRs. Esto implica la posibilidad del Agente Responsable de realizar todas las tareas relacionadas con procedimientos de certificación y participación continua en el sistema CBPR, libre de cualquier influencia que pudiera comprometer su juicio profesional, objetividad e integridad.

   b) El Agente Responsable deberá poder demostrar a las Economías que posee garantías internas, estructurales y procedimentales para

[234] Véase Proyecto 2, Accountability Agent Recognition Criteria 2010/SOM1/ECSG/DPS/011. Este documento incluye los formatos que serán usados en el proceso de acreditación de los Agentes Responsables.

atender conflictos de intereses reales o potenciales. Dichas garantías pueden consistir en:

- Políticas escritas para la revelación de conflictos de intereses potenciales y, cuando proceda, la inhibición del Agente de un asunto particular. Dicha inhibición será requerida en casos en donde el Agente está relacionado con el Solicitante o Participante y esto pudiera dar lugar a un riesgo de que el juicio profesional, la integridad o la objetividad del Agente se vea comprometido.
- Políticas escritas para la revisión interna de posibles conflictos de intereses con Solicitantes y Participantes.
- Publicación de estándares de certificación para Solicitantes y Participantes.
- Mecanismos para reportar regularmente a la autoridad gubernamental sobre certificaciones de nuevas Solicitantes, auditorías de Participantes ya existentes y solución de controversias.
- Mecanismos para la publicación obligatoria de reportes de casos en ciertas circunstancias.

2) Requisitos en relación con Solicitantes y Participantes específicos:

a) En ningún momento un Agente Responsable podrá tener afiliación directa o indirecta con un Solicitante o Participante, de modo que pueda verse afectada la capacidad del Agente para rendir una decisión justa respecto de su certificación y posterior participación en el CBPRs. Estas afiliaciones pueden conducir a la inhibición del Agente conforme al criterio antes señalado.

b) En el caso de otro tipo de afiliaciones que puedan verse remediadas por la existencia de garantías estructurales u otros procedimientos asumidos por el Agente, estas deberán ser comunicadas inmediatamente al JOP, junto con una explicación de las garantías adoptadas para asegurar que dicha afiliación no compromete el actuar del Agente. Estas afiliaciones pueden consistir en:

- Funcionarios del Solicitante o Participante que sirvan en la mesa directiva del Agente Responsable con capacidad de voto, o viceversa;
- Acuerdos económicos relevantes o relaciones comerciales entre el Agente y el Solicitante o Participante, distintas a los cobros de honorarios por la certificación y participación en el CBPRs; o
- Cualquier otra afiliación que permita al Solicitante o Participante ejercer indebidamente influencia en el Agente respecto de su certificación y participación en el CBPRs.

c) Fuera de las situaciones establecidas en los criterios, el Agente Responsable deberá abstenerse de prestar servicios mediante remuneración, interés o beneficio, a los Solicitantes o Participantes, como pueden ser:

- Servicios técnicos o de consultoría relacionados con el desarrollo o implementación prácticas y procedimientos de privacidad del Solicitante o Participante;

- Servicios técnicos o de consultoría relacionados con su declaración o política de privacidad; o
- Servicios técnicos o de consultoría relacionados con sus garantías de seguridad.

d) Un Agente Responsable puede comprometerse a prestar servicios técnicos o de consultoría a un Solicitante o Participante, distintos a aquellos que se refieran a su certificación o posterior participación en el CBPRs. Cuando esto ocurra, el Agente Responsable comunicará al JOP:

- la existencia del compromiso; y
- una explicación de las garantías adoptadas para asegurar que el Agente permanece libre conflictos de interés derivados de dicho acuerdo (estas garantías pueden consistir en dividir el personal que prestará los servicios técnicos o de consultoría, de aquél que realice las funciones a que se refieren estos criterios: certificación, recertificación, monitoreo, solución de controversias, etc.).

e) La provisión de servicios a que se refieren las secciones 3 a 6 no se considerarán servicios de consultoría conforme a las prohibiciones anteriores.

3) Además de hacer del conocimiento del JOP todas las inhibiciones descritas en la Sección 1 (b)(i), el Agente Responsable también deberá revelar al JOP aquellas actividades o negocios identificados en la sección 1 (b) que pudieran considerarse conflictos de intereses, pero que no resultaron en una inhibición. Dicha revelación deberá

incluir una descripción de las razones por las que no se inhibió y las medidas adoptadas por el Agente para evitar o remediar cualquier resultado perjudicial que pueda surgir del conflicto de intereses.

Requisitos del programa

4) El Agente Responsable evaluará a los Solicitantes a través un conjunto de requisitos de programa que comprenderán todos los principios del Marco de Privacidad de APEC, en particular, relacionados con la transmisión transfronteriza de datos y que además cumplirán los requisitos del CBPRs desarrollados y aprobados por las Economías miembro. (Nota: los Agentes Responsables podrán cobrar honorarios a los Participantes por la prestación de este servicio, sin que ello implique una de las prohibiciones señaladas en párrafos precedentes).

Proceso de certificación

5) Un Agente Responsable debe contar con un proceso comprehensivo para revisar las políticas y prácticas de los Solicitantes que pretendan participar en el CBPRs, así como para verificar su adecuación con los requisitos de programa del Agente. El proceso de certificación incluye:

- Una evaluación inicial de la conformidad que incluirá la verificación de los formatos de autoevaluación llenados por el Solicitante, y que podrá incluir además entrevistas personales o telefónicas, inspecciones del sistema de datos personales, escaneos de los sitios web, o herramientas automatizadas de seguridad.
- Un reporte comprehensivo para el Solicitante destacando los hallazgos del Agente en relación con el nivel de conformidad del Solicitante con los requisitos del programa. Cuando se haya

encontrado que no se cumple alguno de los requisitos del programa, el reporte deberá incluir una lista de cambios que el Solicitante deberá cumplir a fin de obtener la certificación para participar en el CBPRs.

- Verificación de que los cambios señalados en el párrafo anterior han sido realizados por el Solicitante.
- Certificación de que las políticas del Solicitante se encuentran de conformidad con los requisitos de programa del Agente. Cuando un Solicitante ha obtenido dicha certificación, es denominado en este documento como Participante del CBPRs.

Monitoreo y proceso de revisión de la conformidad

6) El Agente Responsable deberá tener procedimientos escritos comprehensivos diseñados para asegurarse de la integridad del proceso de certificación y para monitorear que el Participante cumpla durante el periodo de certificación con los requisitos de programa.

7) En adición, cuando existan suficientes motivos para el Agente para creer que un Participante se ha involucrado en una práctica que pudiera constituir un incumplimiento del programa, deberá iniciar inmediatamente un proceso de revisión para verificar su conformidad. Cuando se haya encontrado algún incumplimiento con alguno de los puntos del programa, el Agente notificara al Participante las correcciones que el Participante deberá hacer en un tiempo razonable que para tal efecto señalara el Agente. El Agente verificara que los cambios requeridos han sido realizados propiamente por el Participante dentro del tiempo establecido.

Recertificación y declaración anual

8) El Agente requerirá a los Participantes declarar anualmente sobre su adherencia a los requisitos del CBPR. Se llevaran a cabo revisiones regulares comprehensivas para asegurar la integridad de la recertificación. Cuando ha habido un cambio sustancial en la política de privacidad del Participante (determinado de forma razonable y de buena fe por el Agente Responsable), se iniciara inmediatamente un proceso de revisión. Este proceso de recertificación incluye:

a) Una evaluación del cumplimiento, que incluirá la verificación de los formatos de autoevaluación actualizado por el Participante, y que además incluirá entrevistas personales o telefónicas, inspecciones del sistema de datos personales, escaneos de los sitios web, o herramientas automatizadas de seguridad.

b) Un reporte integral para el Participante destacando los hallazgos del Agente en relación con el nivel de conformidad del Participante con los requisitos del programa. Cuando se haya encontrado que no se cumple alguno de los requisitos del programa, el reporte deberá incluir una lista de cambios que el Participante deberá cumplir a fin de obtener la recertificación.

c) Verificación de que los cambios señalados en el párrafo anterior han sido realizados por el Participante.

d) Notificación al Participante de que se encuentra en cumplimiento con los requisitos del programa y que ha obtenido su recertificación.

Procedimientos para la Solución de Controversias

9) El Agente Responsable deberá tener un mecanismo para recibir e investigar las quejas sobre los Participantes y para resolver las diferencias entre los quejosos y los Participantes sobre un incumplimiento de los requisitos del programa, así como un mecanismo para la cooperación sobre resolución de controversias con otros Agentes de Responsabilidad reconocidos por las Economías de APEC cuando sea posible. Un Agente Responsable puede optar por no proveer directamente el mecanismo de solución de controversias. El mecanismo puede ser contratado por el Agente a un tercero que brinde este servicio. Cuando el servicio sea contratado por un Agente la relación deberá estar concertada al momento de que el Agente Responsable es acreditado bajo el CPBRs de APEC.

10) El proceso de solución de controversias, ya sea proporcionado directamente o por un tercero, incluirá los siguientes elementos:

a) Un proceso para recibir quejas y determinar si la queja se refiere a las obligaciones del Participante bajo el programa, así como que la queja presentada entra dentro del alcance de los requisitos del programa.
b) Un proceso para notificar al quejoso la determinación que recaiga sobre el punto anterior.
c) Un proceso para investigar las quejas.
d) Un proceso confidencial y oportuno para resolver las quejas. Cuando se haya encontrado algún incumplimiento con alguno de los puntos del programa, el Agente notificara al Participante las correcciones que el Participante deberá hacer en un tiempo razonable que para tal efecto señalara el Agente.

e) Notificación por escrito al quejoso y al participante, de la resolución adoptada por el Agente o tercero contratado.
f) Un proceso para obtener el consentimiento del particular antes de compartir su información personal con la autoridad, cuando se solicite su auxilio.
g) Un procedimiento para hacer públicas las estadísticas sobre el tipo de quejas recibidas por el Agente o el tercero contratado y sobre las resoluciones adoptadas, así como para comunicar dicha información a las autoridades gubernamentales.
h) Un procedimiento para publicar de forma anónima, notas de casos de una selección de quejas resueltas ilustrando interpretaciones típicas o significantes, así como resoluciones relevantes.

Mecanismos para hacer cumplir los requisitos del programa

11) El Agente Responsable deberá tener la facultad de poder hacer efectivos los requisitos del programa sobre los Participantes, ya sea mediante contrato o por ley.

12)El Agente Responsable deberá tener procedimientos para notificar al Participante inmediatamente sobre el incumplimiento con los requisitos del programa del Agente y para requerir al Participante la corrección de la falta en un tiempo específico.

13) El Agente Responsable deberá tener procedimientos para imponer las siguientes penalidades, que serán proporcionales al daño o posible daño que resulte de la violación, en los casos en que el Participante haya incumplido con los requisitos del programa y no haya corregido la falta en el tiempo que le haya sido señalado. (Nota: Además de las penalidades enlistadas a continuación, el Agente podrá ejecutar

contratos relacionados con derechos legales y, cuando aplique, aquellos relacionados con derechos de propiedad intelectual ejecutables por un tribunal).

a) Requerir al Participante que corrija la falta dentro de un tiempo específico, y en caso de no hacerlo, expulsar al Participante del programa.
b) Suspender temporalmente el derecho del participante a mostrar el sello del Agente Responsable.
c) Nombrar al Participante haciendo público su incumplimiento.
d) Someter la violación a la autoridad correspondiente. (Nota: esta sanción debe reservarse a aquellos casos en que la violación implica un incumplimiento a la ley).
e) Otras penalidades (incluyendo pecuniarias) en tanto que se consideren apropiadas por el Agente Responsable.

14) El Agente Responsable someterá el asunto a la autoridad correspondiente para revisión y posible ejecución, cuando el Agente considere que, conforme a sus procedimientos de revisión, el Participante no ha cumplido con el CBPRs dentro del tiempo establecido, siempre que dicha falta pueda considerarse razonablemente como una infracción a la ley aplicable.

15) En los casos en que sea posible, el Agente Responsable responderá a las solicitudes de las entidades de las Economías de APEC que se relacionen con dicha Economía y con actividades del CBPRs del Agente.

9.4.4 APEC Cooperation Arrangement for Cross-Border Privacy Enforcement (CPEA)

Este documento fue aprobado por los Ministros de APEC en noviembre de 2009, y comenzó a funcionar el 16 de julio de 2010. Tiene como objetivos principales:

1).- Facilitar el intercambio de información entre las Autoridades de Privacidad Competentes en las Economías de APEC (entre las que se pueden encontrar los Comisionados de Privacidad, Autoridades de Protección de Datos o de Protección de Consumidores que apliquen la normativa de privacidad).

2).- Proporcionar mecanismos para promover la cooperación transfronteriza entre las autoridades participantes en el programa CBPR.

3).- Facilitar la cooperación entre las Autoridades de Privacidad en la ejecución de las CBPR.

4).- Incentivar el intercambio de información y la cooperación en la investigación y ejecución de la privacidad con Autoridades distintas a las de las economías de APEC, incluso asegurando que el acuerdo de cooperación pueda funcionar perfectamente en conjunto con otros acuerdos regionales, como aquellos derivados de las recomendaciones de la OCDE.

El CPEA crea un marco para el intercambio voluntario de información, la solicitud y la provisión de asistencia para actividades relacionadas con la privacidad. El acuerdo está abierto a cualquier Autoridad de los miembros de APEC, y está diseñado con la finalidad de hacer más efectiva la aplicación

de los principios establecidos en el Marco de Privacidad y en el CBPRs de APEC. Mediante este acuerdo se facilita la cooperación en temas de investigación, obtención de pruebas sobre posibles violaciones a la privacidad, entre otros.

De acuerdo con este Acuerdo de Cooperación, una Economía puede tener más de una Autoridad de Privacidad Competente, siempre que cada una de ellas cumpla con los criterios establecidos en el párrafo 4.1, es decir, que se trate de un organismo público que sea responsable de la aplicación de las leyes de privacidad, y que además tenga facultades para conducir investigaciones o iniciar procedimientos de cumplimiento o ejecución.

El documento se integra de la siguiente forma:

- Entrada en vigencia del Acuerdo de Cooperación (párrafo 3);
- Definiciones y limitaciones legales (párrafos 4, 6 y 7);
- Papel del Administrador (párrafo 5);
- Como participar y dejar de participar en el Acuerdo (párrafo 8);
- Cooperación transfronteriza (párrafo 9);
- Confidencialidad (párrafo 10);
- Compartir información (párrafo 11); y
- Asuntos varios (intercambio de oficiales, diferencias, revisión) (párrafos 12 a 15).

Además, se encuentran adjuntos los siguientes documentos:

- Formato para la solicitud de asistencia (Anexo A);
- Formato para la designación de un punto de contacto (Anexo B); y

- Formato para la presentación sintetizada de las prácticas, políticas y actividades de las Autoridades Competentes participantes.

Actualmente hay cinco Autoridades de Privacidad participando en el CPEA:

- Oficina del Comisionado de Información de Australia (OAIC)
- Oficina del Comisionado de Privacidad de Nueva Zelanda (NZOPC)
- Comisión Federal de Comercio de los Estados Unidos (USFTC)
- Oficina del Comisionado de Privacidad de Datos Personales de Hong Kong, China (PCPD)
- La Oficina del Comisionado de Privacidad de Canadá (OPCC)

Los Administradores conjuntos son el Secretario de APEC, la OAIC de Australia, la NZOPC de Nueva Zelanda, y la FTC de Estados Unidos.

9.4.5 Charter of the Apec Cross-Border Privacy Rules System Joint Oversight Panel

La Gobernanza del CBPRs de APEC requiere de mecanismos eficientes para la administración del sistema, que responda a los principios de simplicidad, transparencia, reducción de costos, y responsabilidad ante los Miembros de APEC.

A fin de satisfacer estas necesidades, se estableció un Panel Conjunto de Vigilancia (JOP por sus siglas en inglés) compuesto por las economías y bajo la dirección del Sub-grupo de Privacidad de APEC, cuyas funciones de administración, gobierno y procedimientos principales se encuentran en el

Charter of the Apec Cross-Border Privacy Rules System Joint Oversight Panel.

Además de establecer la composición y funcionamiento del JOP, este documento señala la forma en que las Economías de APEC comenzarán a formar parte del CBPR, así como la forma en que dejarán de participar ya sea voluntaria u obligatoriamente. El JOP estará conformado por representantes de tres Economías de APEC, por un periodo de dos años, sujeto a la aprobación del Grupo de Manejo de Comercio Electrónico, quien además nombrara a un Presidente por el mismo periodo de entre las tres economías.

X.- SELLOS DE CONFIANZA

10.1 Consideraciones Generales

En materia de sellos de confianza, durante las cuatro entregas previas a este reporte final se fueron analizando diversos casos y en este apartado solo se comentan aquellos que tienen relevancia respecto del modelo que se está promoviendo en México, a fin de ser considerados como referencia en los procesos de emisión de parámetros; ya sea por su afinidad con la cultura jurídica mexicana o por los vínculos comerciales de nuestro país.

También en un entrega previa se consideró que en países de modelos de autorregulación pura, como es el caso de Estados Unidos, cobran especial relevancia sellos de confianza, muchos de ellos con efectos multinacionales, como Trust-e, Business Seal for the Web (del Better Business Bureau), VeriSign, Mc Afee, Webassured, ESRB Privacy Online Children's Certification Seal, Privo's Seal of Approval, etc. los cuales contienen especificaciones especiales.

Debido a que entre estas marcas existe competencia, sus propuestas comerciales para colocar los sellos de confianza ha implicado la exposición de las ventajas y desventajas que tiene cada uno de ellos. Se ha señalado por ejemplo que Trust-e se autocalifica como el sello de privacidad[235] por excelencia, y afirma que VeriSign Trust Seal, McAfee Secure Trustmark, Comodo HackerProof Seal o el GeoTrust SSL Certificates son sellos para garantizar seguridad[236]; y que “otros” son sellos que garantizan buenas

[235] Privacy seals verify that a website has strong information privacy practices outlined in its privacy policy and can also indicate that a site is subject to scans to detect privacy vulnerabilities.
[236] Security seals verify that a website uses technology to protect your personal information (like SSL encryption) and/or it is subject to scans to detect the presence of malicious entities (like malware) or site vulnerabilities (like cross-site scrip

prácticas comerciales[237], tales como BBB Accredited Business Seal, buySAFE Seal, Bizrate Customer Certified Seal o el Shopping.com's Trusted Store Seal. Lo importante de todos ellos es que participan como agentes certificadores del Safe Harbor Privacy Principle y pueden ser considerados como relevantes en la construcción de los modelos mexicanos para distintos sectores.

Se destaca que conforme al Departamento de Comercio de Estados Unidos el sello de confianza otorgado para el flujo transfronterizo de datos entre Estados Unidos y la Unión Europea ha sido un éxito, ya que las personas que cuentan con esta certificación suelen cumplirlo, lo que no impide a la autoridad de iniciar un proceso en contra por violentar el modelo[238]. Pero una problemática a la que se ha enfrentado la autoridad de Estados Unidos es el engaño de las empresas, ya que solo dura un año la vigencia del sello por lo que siguen utilizándolo luego de que expira.

Quizás por eso la UE y la APEC inclusive estén considerando que la tendencia de la autorregulación pura sea reemplazada por una mayor injerencia de la autoridad y con mecanismos reforzados de certificación, ya que no cubre las expectativas de la autoridad ni de los consumidores.

Por lo que respecta a las promociones de sellos de confianza para la región, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) ha venido desarrollando desde 2007 diversas actividades en coordinación con la Asociación Latinoamericana de Integración (ALADI)[239], el Grupo Especial de Asuntos Tecnológicos de la Cancillería Argentina y el

[237] Reputation & Reliability Seals verify that a website is operated by a legitimate business entity and/or that a website has sound business practices as determined by consumers or a third-party.

238 Véase Department of Commerce, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" pág. 44 http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf

[239] http://www.aladi.org/

Reino de España, con la finalidad de fortalecer sus capacidades, compartir las experiencias regulatorias e incentivar el desarrollo de grupos de trabajo multidisciplinarios y especializados en los aspectos legales del comercio electrónico. Entre sus resultados destacan los acuerdos del Grupo de Trabajo denominado "Grupo Montevideo", que promovió la instrumentación de dos proyectos piloto, entre los que al 2008 se encontraba el "**Proyecto Piloto de Sello de Confianza Regional**".

Para llevarlo a cabo, se suscribió un Memorándum de Entendimiento por parte de la Asociación Mexicana de Internet (AMIPCI) con TradeSafe y ECNetwork de Japón, SOSA de Taiwán, el Instituto de Comercio Electrónico de Corea del Sur; CommerceNet y Case Trust de Singapur y TRUSTe de los Estados Unidos, que –a la fecha de este acuerdo- eran los principales proveedores de servicios de sellos de confianza de la región Asia Pacífico y que conforman –como antes se indicó- la Asia-Pacific Trustmark Alliance (ATA)[240].

El compromiso conjunto por definir un marco normativo mínimo para facilitar la adopción, el uso y el reconocimiento recíproco de sellos de confianza a nivel de Iberoamérica continúa en proceso. La Red Iberoamericana de Protección de Datos[241] surge así en respuesta a la necesidad de fomentar e implementar el Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los países iberoamericanos, a que elaboren una regulación normativa en esta materia a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

[240] UNCTAD. Estudio sobre las perspectivas de la armonización de la ciberlegislación en América Latina. UNCTAD/DTL/STICT/2009/1. NACIONES UNIDAS. Nueva York y Ginebra, Junio 2009. Pág. 1

[241] http://www.redipd.org/ (Fecha de consulta: 4 de noviembre de 2011).

Es importante señalar que los Sellos o Marcas de Confianza generalmente son distintivos que se otorgan cuando los responsables han pasado por un proceso de adhesión a un código deontológico o de buenas prácticas y/o a esquemas de certificación (verificación, auditoría, etc.) previos. Si se toman como referencia los sellos European Privacy Seal (EuroPriSe) y el Privacy Mark (Japón), no queda duda que la certificación es esencial para emitir un sello. Si se revisan las nuevas propuestas de APEC y la Comisión Europea comentadas anteriormente, la tendencia es hacia un esquema de autorregulación basado en la certificación.

Ya se ha comentado que sin el ánimo de prejuzgar sobre el éxito de uno u otro modelo, se debe analizar que algunos sellos de confianza no han prosperado, pues cuando se estudió el Proyecto i+Confianza del 2002, que comparó 19 marcas o sellos de confianza (10 de Europa, 7 de América y 1 de Asia), resulta que en diez años algunos modelos se quedaron en el camino y otros han ido adquiriendo fortaleza en el ámbito del comercio electrónico. De aquellos sellos estudiados, -como ya antes se anotó- subsiste la mitad: Trusted Scop, Qweb, Trust-e, Web Assured, Hon Code, Confiar-e, [G] ahora como Confianza Online, AGACE y AENOR. BBBOnline Reliability y BBBOnline Privacy se fusionaron en Better Business Bureau, que tiene el “Business Seal for the Web”.

Aunque en Europa existen importantes sellos o marcas de confianza, o bien, códigos de buenas prácticas, tales como los reconocidos en Alemania (Trusted Shops), Francia (Bureau Veritas Web Value), Italia (e-com-quality mark) o Suiza (Hon Code) en este proyecto se han considerado preliminarmente los basados en las directivas de la Unión Europea, ATA o APEC.

10.2 El Sello Confianza Online de España

Considerando el número creciente de entidades adheridas al sistema que permite el uso del sello Confianza Online, a continuación se presenta una relación de las actividades a que se dedican los diversos prestadores de servicios de la sociedad de la información que actualmente ostentan este distintivo en sus páginas web; lo cual permite apreciar el alcance del comercio electrónico y de los diversos productos y servicios que pueden comercializarse a través de este medio:

- Alimentos y Bebidas
- Alquiler de Coches
- Animales y Mascotas
- Antigüedades
- Artes y Diseño Gráfico
- Artículos para Adultos
- Asociaciones/Organizaciones sin Ánimo de Lucro
- Banca y Servicios Financieros
- Belleza y Cosmética
- Bordados
- Bricolaje y Herramientas
- Buscadores
- Búsqueda de Empleo
- Calzado
- Centrales de Medios
- Compra colectiva
- Comunicación y relación públicas
- Construcción e industria
- Consumibles
- Deportes y Fitness
- Desarrollos y Diseño Web
- Disfraces y Artículos de Fiesta
- Electrodomésticos
- Electrónica
- Electrónica de consumo
- Energía
- Espectáculos y Venta de Entradas
- Ferretería
- Floristería y Jardinería
- Fontanería
- Grandes Superficies
- Hogar y Decoración
- Hostelería y Restauración
- Informática
- Instituciones y Administraciones Públicas
- Joyería
- Juguetes
- Lencería
- Libros y Revistas
- Loterías, Juegos de Azar y Apuestas
- Marketing Online
- Medios de Comunicación
- Mensajería y Transporte
- Moda
- Museos y

- Cerámica
- Coaching
- Coches, motos y accesorios
- Comercio electrónico
- Papelería
- Peluquería y Estética
- Perfumería y Droguería
- Piscinas y Spa
- Productos de Consumo
- Productos Ecológicos
- Publicidad y Marketing
- Redes Sociales
- Regalos
- Formación
- Fotografía
- Fundaciones
- Gourmet
- Relaciones Personales
- Ropa y Accesorios para Bebés
- Salud y Parafarmacia
- Seguros
- Servicios de Seguridad
- Servicios Financieros e Inmobiliarios
- Servicios Profesionales
- Telecomunicaciones
- Telefonía Fija y Móvil
- Galerías de Arte
- Música
- Neumáticos y Talleres
- Ocio y Tiempo Libre
- Óptica
- Telemarketing
- Teletienda
- Transporte
- Viajes y Turismo
- Videojuegos y Películas
- Vinos
- Webs de Venta Privada
- Webs Personales
- Otros

La lista de entidades adheridas puede ser consultada en la siguiente dirección: http://www.confianzaonline.es/adheridos/entidades-adheridas/#

Obtención y utilización. El principio de funcionamiento del Sello Confianza Online lo constituye la adhesión al código tipo que consta inscrito ante la AEPD. Al efecto, el artículo 32.1 de este código establece: "*Las empresas que se adhieran a éste Código de Conducta podrán identificarse con la exhibición en sus webs del Sello de Confianza de Comercio Electrónico y Publicidad Interactiva como distintivo de la adhesión al presente sistema de autorregulación.*"

Se dispone también que al pulsar sobre el Sello de Confianza se proporcionará acceso a la información relativa al sistema de autorregulación normado por el código, y en especial a:

- Las normas éticas plasmadas en el Código Ético,
- Al funcionamiento de los mecanismos extrajudiciales de resolución de controversias encargados del control de su aplicación –permitiendo incluso la presentación de reclamaciones online, y
- Al listado de las empresas y entidades adheridas a este sistema de autorregulación.

Como medida de protección a la integridad del sello de confianza, el artículo 32.2 del código establece expresamente:

> *Dado su objeto esencial, que es el de constituir una marca distintiva colectiva, el sello no podrá ser dispuesto ni, en todo caso, utilizado de tal forma que pueda ser considerado:*
> *- como una marca propia de la empresa usuaria,*
> *- o como una garantía de calidad de los productos o servicios ofrecidos.*

Finalmente, como medida de extensión del nivel de protección que se pretende brindar a través de este medio, conviene destacar el sistema de solicitud de adhesión a Confianza Online, también previsto en su artículo 32:

> *4. Para la obtención del Sello de Confianza será necesario que la empresa adherida lo solicite a la Secretaría del sistema. Recibida la solicitud, la Secretaría enviará un acuse de recibo de la misma. La Secretaría solicitará a la empresa peticionaria la documentación necesaria que acredite la identidad de la empresa solicitante y además podrá solicitar cualquier aclaración o documentación complementaria necesaria para la obtención del Sello de Confianza* ***así como proponer las medidas que crea necesarias para una mejor adecuación a lo establecido en el presente Código****. Si, en tal supuesto, no se produce ninguna comunicación entre la empresa solicitante y la Secretaría en los tres meses siguientes a las peticiones o propuestas de la Secretaría, se entenderá caducado el procedimiento de solicitud del sello, pudiendo la empresa pedir su reanudación en cualquier momento.*

5. Una vez que la Secretaría del sistema acuerda el otorgamiento del Sello de Confianza la empresa deberá comprometerse formalmente al cumplimiento de sus condiciones de utilización. La Secretaría podrá, en todo momento, apreciar y controlar las condiciones de utilización del sello y tomar todas las medidas útiles en caso de utilización anómala. A estos efectos, las empresas adheridas se comprometen a aplicar sin demora y sin reserva las instrucciones de utilización que les sean comunicadas por la Secretaría.

10.3 Distintivos de confianza con regulación específica

En España también, se deben reconocer sellos de confianza para ámbitos específicos:

La protección del consumidor en la sociedad de la información y el comercio electrónico. En relación con un ámbito eminentemente relacionado con la protección de datos personales, en España encontramos la regulación nacional de un distintivo que permite reconocer a aquéllos prestadores de servicios de la sociedad de la información que habiendo adoptado códigos de conducta con características específicas ofrecen garantías a los consumidores de productos y servicios ofrecidos y adquiridos online.

Este distintivo tiene su origen en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Esta Ley dispuso, en su Disposición Final Octava, que en el plazo de un año a partir de la entrada en vigor de la misma,[242] el Gobierno aprobaría "*un distintivo que permita identificar a los prestadores de servicios que respeten códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros contenidos, la*

[242] Esta Ley fue publicada en el Boletín Oficial del Estado el 12 de julio de 2002, y entró en vigor a los tres meses de dicho acto legislativo.

adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores, en los términos que reglamentariamente se establezcan."

El primer ordenamiento emitido para llevar a efecto la Disposición Final de referencia fue el Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimiento de concesión; sin embargo, debido a la presentación de diversas oposiciones en relación con la regulación de competencias que deberían pertenecer también a las comunidades autónomas españolas, se optó por derogar este Real Decreto y emitir uno nuevo que cumpliera con la misma función, respetando las competencias que originaron diversas observaciones.

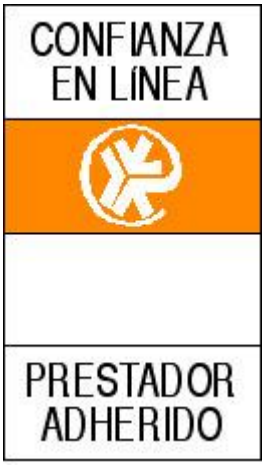
Finalmente, el 8 de octubre de 2005 fue publicado en el Boletín Oficial del Estado el "*Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión*", que actualmente regula el denominado "*distintivo público de confianza en línea*".

De dicha norma, procede destacar a los efectos del presente estudio, lo siguiente:

- **Objeto de la norma** (artículo 1): "*regular el distintivo que podrán mostrar los prestadores de servicios que se adhieran a códigos de conducta que cumplan las condiciones previstas en [el mismo], en cumplimiento de lo previsto en la disposición final octava de la Ley*

34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico." Este Real Decreto también establece *"las condiciones que deben reunir tales códigos de conducta, la concesión y retirada del distintivo y el procedimiento aplicable.*"

- **Denominación y forma del distintivo** (artículo 2): Se dispone que el distintivo se denominará "distintivo público de confianza en línea" y que su formato será el siguiente:



- **Ámbito de aplicación** (artículo 3): Las disposiciones del Real Decreto analizado son aplicables a "*las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores que adopten códigos de conducta destinados a regular las relaciones entre prestadores de servicios de la sociedad de la información y los consumidores y usuarios, cuando la adhesión a tales códigos conceda el derecho al uso y administración del distintivo público de confianza en línea*." También será aplicable a los prestadores de servicios de la sociedad de la información que hagan uso de dicho distintivo.

- **Ámbito y contenido de los códigos** (artículo 4). Sobre el ámbito de los códigos de conducta regulados por esta norma, llama la atención que se refiere a códigos de ámbito nacional **o superior**; cuestión que resulta obvia en virtud del tipo de actividad desarrollada por los prestadores de servicios que pueden adherirse a estos códigos, que en muchas ocasiones ofrecen sus servicios o venden sus productos más allá de las fronteras nacionales.

  En cuanto a su contenido, se exige que "*además de los otros requisitos exigidos en este Real Decreto, los códigos de conducta deben respetar la legalidad vigente e incluir, como mínimo, con suficiente grado de precisión:*"

  a) Las garantías concretas que ofrecen a los consumidores y usuarios que mejoren o incrementen las reconocidas por el ordenamiento jurídico.
  b) Un sistema de resolución extrajudicial de conflictos de entre los previstos en el *artículo 7*.
  c) Los compromisos específicos que asumen los prestadores de servicios adheridos en relación con los problemas concretos planteados a los consumidores y usuarios del sector, identificados según la información de los promotores del código y la que, al efecto, les faciliten las asociaciones de consumidores y las administraciones públicas sobre las reclamaciones presentadas por los consumidores y usuarios.
  d) El ámbito de las actividades del prestador de servicios sometidas al código, que, al menos, englobará alguna de las siguientes áreas:
     i. las comunicaciones comerciales o la información precontractual,

ii. la contratación y los procedimientos de solución de quejas o reclamaciones (cuando estos sean distintos de los sistemas de resolución extrajudicial de conflictos a los que se refiere el *artículo 7*).

- **Sistemas de regulación extrajudicial de conflictos** (artículo 7): Se establece que los códigos de conducta que pretendan obtener el distintivo público analizado, deberán establecer, como medio de solución de controversias entre los prestadores de servicios y los consumidores y usuarios:

  a) el sistema arbitral de consumo[243] u
  b) otro sistema de resolución extrajudicial de conflictos que figure en la lista que publica la Comisión Europea sobre sistemas alternativos de resolución de conflictos con consumidores y que respete los principios establecidos por la normativa comunitaria a este respecto[244].

  La adhesión de los prestadores de servicios a uno de los sistemas mencionados en el apartado anterior **es requisito necesario para la incorporación de los prestadores de servicios a los códigos de conducta**.

Frente a todo lo anterior, y sin siquiera entrar en el análisis del procedimiento de concesión, administración y retirada del distintivo público de referencia, conviene valorar que en la práctica:

[243] Ver Real Decreto 231/2008, de 15 de febrero, por el que se regula el Sistema Arbitral de Consumo.

[244] Ver http://ec.europa.eu/consumers/redress_cons/schemes_en.htm

- Pocas Comunidades Autónomas han implementado el sistema de concesión del distintivo[245].
- Pocas entidades han presentado solicitudes para convertirse en promotoras del distintivo[246].
- El Instituto Nacional del Consumo español (http://www.consumo-inc.gob.es/home.htm) **no ha publicado en su página web la información a que se refiere el artículo 13.1 del Real Decreto analizado**, es decir: "*los códigos de conducta a los que se conceda el distintivo regulado en este Real Decreto; la relación de las entidades promotoras de dichos códigos y la de los prestadores de servicios adheridos; las sanciones impuestas a los prestadores de servicios por incumplimiento, si son públicas, especialmente cuando lleven aparejada la suspensión o expulsión del prestador de servicios del código o de la entidad promotora o la retirada del* distintivo público de confianza en línea*, y la dirección establecida para la presentación de quejas por incumplimiento de los códigos y la de los órganos de resolución extrajudicial de conflictos previstos en los códigos de conducta.*"

Frente a estos hechos, las siguientes consideraciones relativas al "distintivo público de confianza en línea" aparecen pertinentes:

a) Se trata de una iniciativa necesaria en el entorno de la sociedad de la información en lo general y en las actividades de comercio electrónico en lo particular.

b) Evidentemente, la legislación analizada promueve la autorregulación mediante la adopción de códigos de conducta que, en este caso, deberán ser formulados por "entidades promotoras".

[245] Cfr. "*Garantías de navegación segura: análisis de los sellos y códigos de confianza en comercio electrónico*", ANETCOM, España en http://video.anetcom.es/editorial/guia_navegacion_segura.pdf.
[246] *Ídem*.

c) La promoción de "sistemas de resolución extrajudicial de conflictos" (ADRs) en cualquier código de conducta que deseé obtener el uso del distintivo público también resulta valorable en el entorno de la sociedad de la información, especialmente si tomamos en cuenta lo dispuesto por el artículo 7.2 del Real Decreto 1163/2005: "*En los procedimientos de resolución extrajudicial de conflictos […], podrá hacerse uso de medios electrónicos en la medida en que lo posibilite su normativa específica y con las condiciones previstas en ella.*"

d) No obstante todo lo anterior, la participación de diversos niveles de gobierno parece haber dispersado el control sobre este distintivo público, llegándose al extremo de no existir información pública sobre el número y la identidad de aquellas entidades promotoras a quienes se ha concedido el uso del distintivo.

Desde un punto de vista investigativo, esta falta de información desincentiva la recomendación del modelo adoptado, sin que ello signifique que el entorno que regula la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico en España no amerite el impulso de la autorregulación por parte de sus actores.

10.4 European Privacy Seal (EuroPriSe)

Como antes se comentó, EuroPriSe comenzó como un proyecto financiado por el programa eTEN[247] de la Comisión Europea en junio de 2007[248]

[247] Para mayor información: http://europa.eu/legislation_summaries/information_society/strategies/l24226e_es.htm [fecha de consulta: 15 de marzo de 2012].

[248] Los países participantes en este proyecto fueron Austria, Francia, Alemania, Eslovaquia, España, Suecia, Holanda y Reino Unido. El monto de la financiación comunitaria fue de 1,239,000 euros y la duración de junio de 2007 a noviembre de 2008. Información disponible en: https://www.european-privacy-seal.eu/about-europrise/from-project-to-service-1/index.html [fecha de consulta: 15 de marzo de 2012].

coordinado por el Centro Independiente Regional de Protección de Datos Schleswig-Holstein (ULD).

El Sello Europeo de Privacidad (EuroPriSe) es en realidad una evolución del *Guetesiegel*, un certificado regional de privacidad desarrollado y emitido por el ULD Alemán[249]. La adaptación de los criterios de certificación del Guetesiegel a EuroPriSe fue determinada por un enfoque paneuropeo.

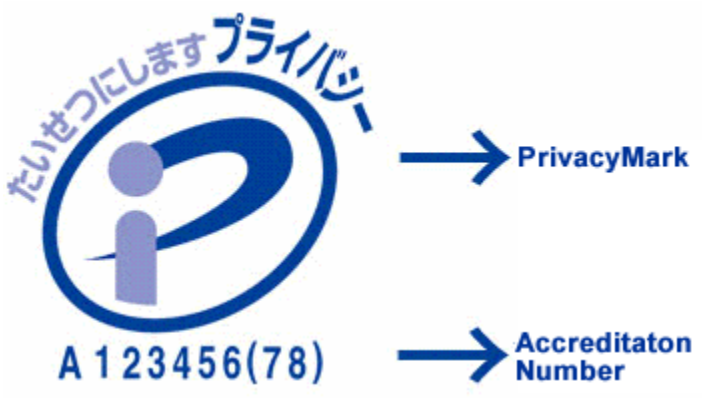
A la fecha se han otorgado 21 certificados a los siguientes productos: Procampaign, Nugg.Ad Ptn, V3 Self-Certification, Kiwivision Privacy Pro, E-Pacs 3.0, Novocard, Pseudodat, Riser, Ixquick, Certified Privnote, Solution Builder, Valid-Pos, eBGempresa, telemed.net, Iberemec CRM, ICAM Legal Aid Solution, Ixquick, BGNetPlus, DiaDirekt, Microsoft Software Protection Platform y wunderloop.

10.5 PrivacyMark

El mecanismo de certificación de PrivacyMark es muy similar, como se indicó con antelación, a cualquier sello de confianza, pues consiste en conceder el derecho de desplegar y utilizar el sello “PrivacyMark” a las empresas que cumplan con una serie de requisitos, durante un plazo renovable de *dos*

[249] Cfr. EuroPriSe, *Final Report*. Disponible en: https://www.european-privacy-seal.eu/results/deliverables/Final%20Report

años. El sello PrivacyMark es una marca registrada propiedad de JIPDEC:



10.6 "Distintivo de Confianza Persus[250]

En España, el "Código Tipo de Protección de Datos Personales del Fichero Verazpersus" tiene por objeto establecer "*las condiciones de organización y régimen de funcionamiento del fichero VERAZ-PERSUS, con el objeto de ofrecer a los beneficiarios unas garantías más amplias que las contenidas en la normativa dictada en materia de protección de datos de carácter personal.*" [251]

[250] https://www.equifax.es/equifaxnet/persus.html)

[251] "Código Tipo de Protección de Datos Personales Del Fichero Verazpersus" de Soluciones Veraz Asnef-Equifax, art. 2.

10.7 Webtrust[252]

Conforme a la información que proporciona la propia empresa, WebTrust es el sello de confianza, calidad y seguridad que se concede a la "página Web" de la empresa que, previamente ha obtenido un Informe Favorable de Auditoría Independiente, por una Firma de Auditoría Habilitada para la Prestación de Servicios WebTrust al cumplir, durante un cierto periodo de tiempo, los Criterios y Principios WebTrust, establecidos por las entidades promotoras y licenciatarias del sello; Instituto Americano de Auditores Públicos de Cuentas (AICPA), Instituto Canadiense de Auditores de Cuentas (CICA), e Instituto de Auditores Censores Jurados de Cuentas de España (IACJCE).

La misma empresa señala que WebTrust, además de cubrir la totalidad de requisitos, es el único sello en la red, certificado de calidad, homologado a nivel internacional y con vigencia ya en más de 19 países, emitido por **Auditores Independientes**, y respaldado por las más importantes Agrupaciones de Auditores Internacionales.

WebTrust253 – AICPA/CICA, US, Canadá. Como parte de la información que proporciona el organismo empresarial se destaca que un agente certificado otorga los sellos de SysTrust y WebTrust una vez realizada la evaluación que indique el cumplimiento de una organización de los principios de privacidad.

De los sellos mencionados el que está enfocado a la protección de datos personales es el sello WebTrust, que certifica el proceso de integridad, confidencialidad y fiabilidad de los sistemas de privacidad. Una vez que el

[252] www.webtrust.es

253 Véase página de Internet de WebTrust. Disponible en línea: http://www.webtrust.org

auditor da el visto bueno o aprobación con los resultados de la evaluación proporciona el sello WebTrust que podrá ser visualizado en la página web del cliente; con lo que, según menciona el organismo, los consumidores tendrán la certeza de que la organización cuenta con un elevado nivel de compromiso en la protección de datos personales.

10.8 The Asian-Pacific Trustmark Alliance (ATA)[254]

Como se ha venido señalando, distintas organizaciones de naciones de Asia, Europa y América han integrado una alianza denominada Asian-Pacific Trustmark Alliance (ATA) que se encuentra en proceso de pasar de ser una estrategia de los países de Asía-Pacífico, a conformar una organización más global que se conocerá como **Global Trustmark Alliance** (GTA).

Su finalidad primordial es promover el comercio electrónico seguro dentro de la jurisdicción de cada país que conforma la alianza, pero también ser un esquema promotor de la confianza en el entorno transfronterizo.

México forma parte de esta alianza a través de la AMIPCI (Asociación Mexicana de Internet, A.C.)[255], que fundada en 1999, reúne a las empresas vinculadas a la industria de Internet en México y su misión es integrar al sector y promover el desarrollo de las TIC como motor económico en los sectores público y privado. Esta organización ha promovido el Sello de Confianza AMPICI:

[254] http://www.ataportal.net/introduction.html
[255] Sitio Web: http://www.amipci.org.mx/

Conforme a su propia información corporativa, el Sello de Confianza AMIPCI® es un distintivo otorgado para sitios de Internet en México, a través de un sello electrónico con un certificado digital adjunto, que reconoce a los negocios o instituciones que promueven el cumplimiento de la privacidad de la información y están legítimamente establecidos. La forma de obtener el Sello de Confianza AMIPCI® se ha comentado en entregables previos.

SEGUNDA PARTE

Recomendaciones Generales

I.- VENTAJAS DE INCORPORACIÓN A ESQUEMAS DE AUTORREGULACIÓN VINCULANTE

Antes de emitir parámetros de los mecanismos y medidas de autorregulación a los que se refiere el artículo 44 de la LFPDPPP, es importante conocer algunas ventajas de los esquemas de autorregulación vinculante que operan en las principales regiones del orbe; tal y como se expone en los Términos de Referencia de este proyecto[256].

1.1 Experiencias en la Unión Europea

En primer lugar el sistema de autorregulación de la Unión Europea (UE) presenta una ventaja considerable debido al tipo de mercado o región económica dentro del cual tendrían incidencia aquellos códigos de conducta aprobados por el Grupo de Trabajo del Artículo 29 (GT29).

Este sistema mantendrá sus características esenciales tras la aprobación y entrada en vigor (de fecha incierta en la fecha de entrega) del *Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*,[257] que además prevé la creación de ***sellos y marcas de protección de datos por vía de certificación*** (artículo 39 de la Propuesta del Reglamento de referencia).

[256] Términos de Referencia. Pág. 14 de 20. Apartado sobre "metodología de trabajo". Inciso c), subinciso a.
[257] El texto en español de la propuesta presentada por la Comisión Europea puede ser consultada aquí (PDF): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

Respecto al sistema de códigos de conducta así como al de sellos de confianza, no es posible en este momento determinar si las disposiciones de la propuesta presentada mantendrán su texto en su versión final.

En todo caso, se trata de códigos de conducta "comunitarios" con efectos en los 27 países que al día de hoy conforman a la UE. En este sentido, aquéllas organizaciones cuyos códigos obtuvieren aprobación para tener efectos en toda la UE pueden, por este solo hecho, ostentar una categoría que al día de hoy pocos han siquiera intentado alcanzar.

La aprobación de un código para la UE no parece un objetivo fácil de alcanzar, ya que además de tratarse de un espacio geográfico de dimensiones considerables, hemos de tener en cuenta que el GT29 está conformado por los directores/comisionados de cada una de las autoridades nacionales de protección de datos personales de los 27 países de la UE, más el Supervisor Europeo de Protección de Datos (EDPS)[258].

A propósito de lo anterior, y como ya ha sido resaltado, al día de hoy el GT29 únicamente ha dado su visto bueno a un Anexo del Código de Conducta para el uso de datos personales en el marco del marketing directo promovido de la FEDMA (Federation of European Direct and Interactive Marketing); organización que no duda en recalcar que es la única que ha negociado y obtenido la aprobación del indicado Grupo de Trabajo[259].

Cuantitativamente hablando, el sistema de códigos de conducta comunitarios dista de ser calificado como "exitoso" debido a que se trata de un sistema

[258] Para más información sobre los miembros del Grupo de Trabajo del Artículo 29, consultar: http://ec.europa.eu/justice/policies/privacy/workinggroup/members_en.htm#edps.
[259] Ver: http://www.fedma.org/index.php?id=57.

que únicamente ha dado su aprobación al código de conducta de una sola organización europea.

En contrapartida, el ámbito de validez de la Directiva de Protección de Datos (aún vigente) permite considerar que aquellas organizaciones que decidan emprender la tarea de obtener la aprobación del GT29 a su proyecto de código de conducta, lo verán sometido a un riguroso examen; con lo cual es posible inferir que aquellos que la obtengan habrán elaborado un código que ofrece un alto grado de protección a los datos personales de aquellos titulares relacionados con el sector en que la organización proponente actúa[260].

En este sentido, el prestigio de la entidad verificadora y su grado de especialización pueden ser empleados como elementos altamente positivos, trasladables hacia aquéllas entidades que obtengan la aprobación o registro de sus códigos de conducta.

1.2 España

Por otro lado, y bajo el análisis efectuado durante la realización del presente informe, resulta necesario indicar que aparece claro que la Agencia Española de Protección de Datos (AEPD) no ha llevado a cabo una campaña o acción

[260] Conviene indicar que el artículo 4.1 del Documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo Artículo 29 (aprobado el 10 de septiembre de 1998) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp13_es.pdf), prevé:

4.1 El Grupo de Trabajo determinará si los códigos de conducta presentados:

- se atienen o no a lo dispuesto en las Directivas y, en su caso, a las disposiciones nacionales adoptadas en cumplimiento de las mismas,
- reúnen las oportunas condiciones de calidad y coherencia interna y ofrecen un valor añadido suficiente con respecto a las Directivas y otras normas sobre protección de datos aplicables, evaluando, en particular, si el proyecto de código se centra suficientemente en los problemas específicos de protección de datos de la organización o el sector al que está destinado a aplicarse, y si aporta soluciones suficientemente claras a dichos problemas.

coordinada para impulsar la adopción de los "códigos tipo" previstos por el artículo 32 de la LOPD.

Como ejemplo de ello la propia identificación y accesos a estos códigos, en la página web de la AEPD, no es del todo inmediata: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php.

Aquellos modelos que han sido identificados -en entregas previas- son relevantes desde un punto de vista comparativo (frente a los códigos comunitarios o los del Reino Unido), pero no deja de llamar la atención que desde la entrada en vigor de la LOPD y hasta la fecha, únicamente se cuente con 13 códigos tipo como objeto de estudio comparativo.

También llama la atención que la propia AEPD no haya publicado al día de hoy el número de afiliados a los diversos códigos tipo cuyo registro ha concedido. Lo anterior no debe interpretarse en demérito de aquellos códigos que han obtenido su registro ante la AEPD.

Tal y como ya ha sido resaltado en capítulos anteriores, se trata de códigos que han sido adoptados, propuestos y registrados dentro de sectores que tratan datos mayoritariamente "sensibles". Son códigos tipo que destacan por su interés en demostrar que, en aquéllas actividades de mayor incidencia en la privacidad de las personas, han decidido implementar medidas que garanticen la seguridad de los datos personales que deben tratar en el curso de sus actividades.

En este sentido, la adopción de "códigos tipo" o de conducta en sectores específicos de determinadas actividades económicas debería ser interpretado como positivo a efecto de generar interés en su adopción, ya que no es lo mismo adoptar un código tipo o de conducta sobre los datos de

"visitantes" de las instalaciones de una empresa, que sobre los datos de "pacientes de un hospital", "alumnos", "empleados", o "clientes de una entidad financiera". El grado de protección que debe adoptarse en razón de los datos tratados, simplemente, no es el mismo.

Interesa, dada la experiencia española (y europea en general), concientizar que estamos frente a diferentes escenarios; recalcar que cada responsable trata datos personales en función de su actividad principal y que no es posible emitir criterios particulares, sino principios generales de protección de datos personales, ineludibles para ellos como sujetos al cumplimiento de la legislación aplicable sobre la protección de datos personales.

La adopción de reglas sobre protección de datos personales no debe basarse, en primer lugar, sobre el tipo de **actividad particular** del responsable, sino sobre la existencia comprobada de un tratamiento de datos. A partir de este principio, la **actividad particular** del responsable será la referencia.

Conforme a lo anterior, el impulso de reglas, procedimientos y **códigos de conducta sectoriales** se presenta como la mejor opción en el momento que vive la legislación y, especialmente el sector TI mexicano.

La experiencia española demuestra, por un lado, que sí existen sectores interesados en adoptar este tipo de códigos, que están dispuestos a autorregularse. Pero también demuestra que la autorregulación debe promoverse e impulsarse tanto a nivel general como sectorial.

En el caso del sector TI debe considerarse de alta relevancia en relación con las acciones de impulso anteriormente referidas. El caso del *Código de Conducta de Confianza Online* se identifica como un modelo adecuado para

analizar la conveniencia de reproducir aquéllas disposiciones más relevantes, siempre tomando en consideración la legislación vigente en nuestro país.

Conforme a lo anterior, los adquirentes de estos productos podrán solicitar a sus fabricantes información que permita determinar si éstos son capaces de cumplir con las medidas de seguridad exigidas para el tipo de datos o tratamiento que la legislación vigente en España requiere. Una medida similar sería deseable en la legislación mexicana, pero además extendida hacia el sector TI.

1.3 Reino Unido

Por otro lado, una primera conclusión respecto del Reino Unido, es que no brinda referencias suficientes para extraer de su sistema de autorregulación alguna información relevante sobre "ventajas de incorporación" a esquemas de autorregulación vinculante[261].

En todo caso, conviene recordar que en este país ha sido la autoridad encargada de aplicar la legislación sobre protección de datos personales -la *Information Commissioner's Office*-, la cual ha actuado como impulsora de "códigos de buenas prácticas" en materia de protección de datos, que ésta misma se ha encargado de publicar y difundir[262].

[261] Tal y como hemos indicado, a día de hoy únicamente existe un código de conducta externo aprobado por la ICO: el *Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998*, cuyo texto puede ser consultado en este link (PDF): http://www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf

[262] Todos los códigos de buenas prácticas analizados pueden ser accedidos desde este link: http://www.ico.gov.uk/for_organisations/data_protection.aspx.

1.4 Estados Unidos

Ahora bien, en entregas anteriores se ha enfatizado que la tendencia de la autorregulación pura tiende a ser reemplazada en países regidos por el derecho anglosajón por una mayor injerencia de la autoridad (más vinculante), ya que los modelos laxos no están cubriendo las expectativas de la autoridad ni de los consumidores en ciertos temas.

Es por ello que en Estados Unidos la Casa Blanca emitió el estudio intitulado "Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy", que incluye una carta de derechos del consumidor en materia de privacidad (Consumer Privacy Bill of Rights), la cual contiene principios para proteger los datos personales y que tiene por objeto pasar al Congreso para ser Ley; o bien, servir de base para crear códigos de conducta consolidados por medio de consultas públicas.

En la experiencia de Estados Unidos ha resultado más idóneo promover los modelos de autorregulación en donde haya consulta pública, debido a que incrementa la confianza con sus consumidores y sus condiciones competitivas. Lo anterior en contraste con los avisos de privacidad que han tenido poca efectividad respecto a los consumidores, ya que son complejos y poco prácticos.

Ante esta referencia se recomienda que en México se armonicen las prácticas de autorregulación en materia de protección de datos personales para evitar la pulverización de los esquemas.

No obstante que en el modelo estadounidense se ha obligado a las empresas a ampliar sus medidas para otorgar mayor protección a los

consumidores, ésta tiene la ventaja de estar diseñado de manera flexible para sortear con rapidez los problemas no contemplados en la dinámica tecnológica.

Es de destacar el esfuerzo de la Federal Trade Comission (FTC) en proteger a más grupos de consumidores como a la comunidad de habla hispana en Estados Unidos con la emisión de informes y prestar ayuda en español.

En otro rubro el modelo norteamericano de protección de datos de menores de edad parece ser insuficiente por solo contemplar a niños menores de 13 años. Sin embargo, para el rango de 13 a 17 años se ha sugerido crear un marco *ad hoc* que no interfiera con su libertad de expresión y su desarrollo personal.

Se menciona lo anterior, para considerar que hay sectores que se encuentran en una especial situación de vulnerabilidad quienes requieren de esquemas de autorregulación vinculante que contengan medidas reforzadas para proteger sus derechos de privacidad y autodeterminación informativa.

1.5 Canadá

Por otro lado en Canadá, el Código Modelo para la Protección de Datos Personales puede ser tomado como referencia por las organizaciones de ese país para crear y operar sus propios Códigos de Protección de Datos Personales (*Code for the Protection of Personal Information*), con los elementos mínimos señalados en el código modelo.

Si bien ese modelo tiene ventajas porque los responsables en el tratamiento de datos personales tienen un modelo institucional en el cual basarse para acoger la autorregulación, se han presentado problemas por parte de las

autoridades canadienses sobre cuáles serían los datos personales que estarían en el ámbito de protección de la ley y de los esquemas de autorregulación.

Para tal propósito ha diferenciando la información personal de la actividad comercial y ha expandido la protección a las fotografías, la dirección de correo electrónico para negocios, el número de identificación ligado a un empleado y la dirección IP (computer Internet Protocol).

1.6 Experiencias de los códigos de privacidad

Es importante señalar que en el derecho comparado se ha encontrado que los códigos de privacidad son el mecanismo de autorregulación más usual previsto hasta ahora en las legislaciones. Con diferentes nombres (códigos de buenas prácticas, códigos de conducta, códigos deontológicos, códigos tipo, etc.) casi todos hacen referencia a normas de comportamiento adoptadas por los propios destinatarios de sus previsiones, ya sea sectores empresariales, asociaciones gremiales o profesionales. Los hay señalados en la Ley y los elaborados por las propias empresas, las asociaciones representativas o la industria.

La ventaja que tienen los códigos es que se pueden formular para un sector determinado o abrirse a varios de ellos. Al convenirse un código, una gran cantidad de personas físicas o morales del sector privado que traten datos personales están en posibilidades de “sumarse” o adherirse a un texto deontológico sin necesidad de hacer erogaciones elevadas, salvo, que la adhesión implique algún procedimiento de certificación y/o el otorgamiento de algún tipo de distintivo que demuestre el cumplimiento de las reglas previstas en el código.

El entorno digital tiene sus particularidades, y en este ámbito no han quedado claros los efectos jurídicos que las legislaciones otorgan a estos códigos, o cuáles son los incentivos para adoptarlos, ya que la mayoría de las legislaciones se limita a señalar que estos serán “inscritos” o “registrados” ante la autoridad correspondiente. La reducción de multas en México (paliativos) o los incentivos reputacionales, deben ser promovidos para motivar su práctica.

En el caso de Estados Unidos, de 2001 a 2010 fueron ventilados 29 casos contra diversas empresas por violentar la seguridad de datos personales, de ellos, cinco se debieron a incumplir su propio código de privacidad, los demás fueron por no tomar los cuidados necesarios para prevenir los ataques más comunes, disponer de manera inadecuada los datos personales de sus clientes y por compartir sus bases de datos con terceros no autorizados (ver reporte 3).

En estos casos la autoridad estadounidense ha ordenado implementar programas de seguridad, así como obtener **auditorías por parte de terceros** imparciales para hacer efectivos dichos programas. Además ha obtenido indemnizaciones a su favor y compensaciones a usuarios.

Para considerar que los códigos tienen ventajas competitivas, se requiere que contengan elementos de representatividad, complementariedad, publicidad y registro, revisión, revocación, contenido, evaluación, temporalidad y alcance, y costos de formulación y adopción. Con un enfoque estrictamente de “marketing”, esos deben ser elementos recomendados como básicos.

1.7 Experiencias de los sellos de confianza

En el caso del flujo transfronterizo Estados Unidos-Europa, el Departamento de Comercio de Estados Unidos ha considerado efectivos los sellos de confianza, ya que las personas que cuentan con estos distintivos suelen cumplirlo, lo que no impide a la autoridad de iniciar un proceso en contra por violentar el modelo. Se pueden colegir que allá este modelo de autorregulación es ventajoso para quienes deseen formar parte de una red comercial internacional, pero no está claro para otros sectores de la economía.

Para que tengan efectividad estos sellos, las autoridades y los organismos autorregulatorios deben anticipar problemáticas tales como el engaño de las empresas que los siguen usando después de que expiran. Quizás por eso la UE y la APEC están considerando que la tendencia de la autorregulación pura sea reemplazada por una mayor injerencia de la autoridad, ya que no cubre las expectativas de la autoridad ni de los consumidores.

Para que se consideren “ventajosos” los Sellos o Marcas de Confianza, se han encontrado opiniones en el sentido de que son efectivos si –y solo sí- los responsables han pasado por un proceso de adhesión a un código deontológico o de buenas prácticas y/o a esquemas de certificación (verificación, auditoría, etc.) previos.

Cuando en entregas previas se comentaron a nivel referencial los sellos European Privacy Seal (EuroPriSe) y el Privacy Mark (Japón), ha parecido concluyente que la certificación es esencial para emitir un sello. Sin embargo, México debe crear un esquema de certificación por etapas (auditorías, verificaciones) pues los rigores (técnicos y temporales) previstos

en la legislación sobre metrología y normalización no hacen viable implementar una acreditación-certificación en corto plazo.

Hoy día, el Sello de Confianza de la Asociación Mexicana de Internet, A.C. (AMIPCI)[263] ha mostrado tener la madurez para insertar a México en los nuevos paradigmas de la autorregulación.

Es claro que la autorregulación es voluntaria. Pero seleccionar un modelo por la sola ventaja de la reducción de sanciones por parte del IFAIPD, no implica que se cuente con los otros estímulos que el mercado genera por sí mismo.

1.8 Síntesis sobre las ventajas de los esquemas de autorregulación

Con la intención de resumir las ventajas que tienen los modelos de autorregulación en el campo de la protección de datos personales, nos permitimos enlistar las más relevantes, tanto para la industria, la autoridad y sobre todo, los titulares de los datos personales:

1.8.1.- Prevención

El establecimiento de esquemas o modelos de autorregulación tienen una función eminentemente preventiva, ya que permitirá mitigar o en su caso establecer mecanismos para mediar entre las partes y que los daños o perjuicios que determinadas acciones puedan causar sean resueltas en un ambiente de particulares.

1.8.2.- Solución de controversias

a) Permite el establecimiento de formas de mediación o resolución de controversias a través de procedimientos *ad hoc* para cada sector y

[263] http://www.sellosdeconfianza.org.mx/

atendiendo las necesidades propias de una industria o iniciativa privada.

b) A través de mecanismos de solución de controversias que son propuestos por la autorregulación se pueden prever procedimientos que resulten eficaces, pero sobre todo que el tiempo de atención y resolución sea corto.

c) Los procedimientos que se establecen en los mecanismos de autorregulación para la solución de controversias podrían resultar de menor costo, que de aquellos procedimientos en los que tiene intervención la autoridad.

d) Los modelos de autorregulación permitirán que la intervención de la autoridad en la solución de conflictos sea menos frecuente, lo que permitirá que las cargas de trabajo de las autoridades no se dispare.

e) La autorregulación tiene más ventajas cuando contiene soluciones alternativas de conflictos, que no limitan ni excluyen el derecho de los titulares de datos personales para acudir a las vías legalmente establecidas para resolver cualquier inconformidad derivada del tratamiento de sus datos personales o de la atención a sus solicitudes de ejercicio de los derechos ARCO.

f) Los esquemas de mediación y resolución de controversias que aportan la mayoría de las organizaciones promotoras de la autorregulación, podrían ser consideradas como parte del servicio que presten los agentes responsables y las organizaciones certificadoras.

1.8.3.- Consideraciones reputacionales

a) Se considera que la adopción de un mecanismo de autorregulación contribuye en buena medida al capital de imagen, ya que los usuarios,

adherentes, etcétera, proyectarán una imagen de responsabilidad y respeto a la protección de los datos personales.

b) Con la proyección de compromiso y responsabilidad en la protección de datos personales, las personas físicas o morales que adopten algún modelo de autorregulación lograrán en cierta medida establecer una relación de confianza con sus clientes o usuarios.

1.8.4.- Beneficios económicos y competitivos:

a) La adopción de mecanismos de autorregulación no solo representará beneficios a los usuarios, clientes o adherentes; ya que para las personas físicas o morales que los adopten representará beneficios económicos pues tendrán más posibilidades de establecer relaciones comerciales a nivel internacional.

b) Uno de los requerimientos para que la autorregulación sea efectiva redundará en beneficios para las partes, por un lado promoverá la sana competencia y por otro, requerirá de brindar más información al consumidor.

c) Uno de los insumos de la economía digital son los datos personales de usuarios, clientes o adherentes, por lo que la adopción de mejores prácticas en temas de privacidad, permitirá el sano desarrollo de la economía nacional en su conjunto.

d) Es muy útil para el desarrollo económico integrar al régimen jurídico aquellas normas que de facto son necesarias para organizar y pactar buenas prácticas a través de códigos deontológicos, sin tener que pasar por todo el proceso legislativo, en tanto se da la coexistencia y complementariedad de los marcos normativos.

e) Los mecanismos de autorregulación deben servir para auxiliar a las autoridades competentes para llevar a cabo su función de protección de la privacidad, así como acercar mecanismos internacionales para promover y hacer cumplir la protección de la privacidad, así como para mantener el flujo continuo de la información entre las Economías y con sus socios comerciales.

f) Los sellos de confianza han logrado que un amplio conjunto de usuarios hayan creado confianza y aumentado la participación a través de todos sus canales en línea, incluyendo sitios web, aplicaciones móviles, publicidad, servicios de nube, análisis de negocio y marketing por correo electrónico.

g) Para incrementar la interoperabilidad (jurídica) global entre países a través del desarrollo de modelos de privacidad con un proceso de consulta, y reforzando la cooperación para eliminar las barreras para el intercambio de datos. Las empresas que realizan flujo transfronterizo de datos deben enfrentarse al cumplimiento de múltiples jurisdicciones, ya que existe poca armonía entre las leyes extranjeras.

h) La adopción de códigos de conducta puede constituir un elemento distintivo para aumentar la competitividad del sector TI frente a otras opciones del mercado, ya que actores de este sector que prestan servicios como alojamiento (hosting) o atención al cliente (call centers) son altamente requeridos por empresas europeas.

1.8.5.- Privacidad a la medida

a) Una ventaja importante de los modelos de autorregulación es que, para su adecuación a la realidad o necesidades de un sector, industria

o empresas no es necesario seguir un procedimiento complejo (como es el caso del ámbito normativo), resultando procesos ágiles.

b) La autorregulación permitirá la aplicación de exigencias legales de forma sencilla y atendiendo necesidades y realidades de los diferentes modelos de negocios existentes en el ámbito digital.

c) Es de gran ventaja la flexibilidad con la que se pueden adaptar los mecanismos de autorregulación a los cambios tecnológicos que son adoptados por los distintos sectores.

d) A través de la autorregulación se permite regular "temas" muy específicos y complejos, como es el caso de la protección de datos personales de menores.

e) Entre las ventajas de la autorregulación se encuentra que se promueve la autonomía privada de la voluntad; entendiéndose este concepto como el principio jurídico-filosófico que les atribuye a los individuos un ámbito de libertad, dentro del cual pueden regular sus propios intereses; permitiéndoles crear relaciones obligatorias entre ellos, que deberán ser reconocidas y sancionadas en las normas de derecho.

f) Diversos investigadores mencionan las ventajas de la autorregulación sobre la regulación estatal para Internet, enunciando que estas son su mayor prontitud, flexibilidad y eficacia; el aprovechamiento de la experiencia acumulada de la industria; y que los recursos gubernamentales son limitados. La autorregulación permite que – si existe voluntad-, se implemente regulación más eficaz, provista de mecanismos de sanción dentro del ámbito privado.

g) Los mecanismos de certificación en materia de protección de datos contribuyen a la correcta aplicación de las leyes o reglamentos sobre

protección de datos personales, teniendo en cuenta las características específicas de los distintos sectores y las diferentes operaciones de tratamiento.

h) Los códigos de ética tienen como consecuencia, por lo general, una mínima carga jurídica en comparación a la ley. Se inclinan a ser solo simples recomendaciones y no contienen mecanismos limitantes.

i) Para que sean ventajosos los esquemas de autorregulación se requiere que dispongan de herramientas que los hagan eficaces. Dentro de estos mecanismos se han sugerido:

(1) Establecer medios ágiles, efectivos y gratuitos en caso de inobservancia del código para que la persona no solo exija el respeto de sus derechos y libertades sino que se convierta en un "fiscalizador" de la gestión del administrador de sus datos personales,
(2) Consagrar mecanismos de control interno y externo de verificación del cumplimiento de los códigos, y
(3) Prever sanciones por el incumplimiento de los códigos.

1.8.6.- Complementariedad

a) Los mecanismos de autorregulación tienen por objeto complementar y hacer efectiva la aplicación de la ley. En algunos casos como se ha visto en el estudio, tienden a sustituir la normatividad.

b) La autorregulación es una manera de promover las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

c) Los códigos de conducta elaborados por organizaciones sectoriales comerciales y profesionales han sido definidos como “un puente” entre las reglas sustantivas de las leyes de protección de datos y su instrumentación a nivel operativo.

d) El éxito del modelo de corregulación depende en gran medida de la oportunidad que se brinde al público y a los principales interesados, de comentar y examinar la propuesta de Código de Privacidad, máxime cuando éstos tienen por objeto sustituir la protección que brinda la ley.

e) Para los Estados miembros de la Unión Europea es importante alentar 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 sus directivas.

f) Para la legislación mexicana, la autorregulación en materia de protección de datos personales tiene como finalidad complementar la legalidad, con lo que se quiere decir que los esquemas que se adopten servirán para organizar y pactar buenas prácticas a través de códigos deontológicos, sin tener que pasar por todo el proceso legislativo, en tanto se da la coexistencia y complementariedad de los marcos normativos.

g) Para la sociedad mexicana representa una oportunidad valiosa de ahondar en el uso de buenas prácticas en acatamiento del principio de responsabilidad, uno de los ocho ejes de observancia ineludible en materia de privacidad.

h) Aunque no ha demostrado ser un modelo con alta participación, la autorregulación debe seguir considerándose una alternativa para promover mejores prácticas en materia de protección de datos personales.

1.8.7.- Confianza

a) Los modelos de autorregulación pueden ser la vía que permita el desarrollo del comercio electrónico, permitiendo crear una ambiente de confianza entre los usuarios y los responsables, pues con la adopción de los mecanismos se mostrará el compromiso y responsabilidad en la protección de datos personales.

b) Para los usuarios tiene como ventaja observar cuáles empresas se encuentran adheridas al mecanismo de autorregulación que mejor atienda a sus necesidades.

c) Con la autorregulación se alientan mecanismos que eliminan el mayor número posible de obstáculos al desarrollo del comercio electrónico, tales como la desconfianza de los consumidores en las páginas web que ofrecen productos o servicios.

d) En el ciberespacio, el objetivo central de la autorregulación es generar confianza en la interacción de los usuarios de Internet; y en este sentido se busca equiparar las acciones y las gestiones en un marco ético para mejorar la calidad de un servicio en el mundo del Internet.

e) Con el marco de trabajo adecuado, las verificaciones, los balances, la vigilancia y los controles, la autorregulación es -con mucho- una ruta más atractiva que la promulgación de leyes por el gobierno central.

f) Los códigos de privacidad otorgan cierta flexibilidad a las organizaciones en el cumplimiento de sus obligaciones. Fue ideado como un mecanismo para favorecer la seguridad y la confianza de los consumidores y usuarios ya que permite a la industria y a sus clientes elaborar un marco de protección que se ajuste a sus necesidades.

g) En un gran número de países es importante el establecimiento de parámetros, prácticas y sellos de confianza para los negocios por Internet, a fin de ampliar la confianza del público en las empresas que realicen comercio electrónico y cuenten con alguno o todos los sellos adheridos a su Programa que posee tres sellos de confianza para los sitios en Internet.

h) La representatividad de los mecanismos de autorregulación es un elemento que puede resultar fundamental para la certeza y operatividad de los códigos, toda vez que ayuda a reducir el grado de confusión en que puede caer un consumidor o usuario frente a un sector o industria fragmentada.

1.8.8.- Beneficios sociales

a) Los medios de comunicación masiva como la radio, la televisión, la prensa escrita, la publicidad e Internet, ya cuentan con mecanismos de autorregulación, muchas veces relacionados con la metodología y la selección de determinados contenidos que puedan afectar severamente a la sociedad, o bien, con prácticas comerciales.

b) Siguiendo a Frank Kuitenbrouwer señala que la autorregulación puede servir para varios fines en relación con el proceso legislativo: La autorregulación puede tener la intención de evitar la legislación; la autorregulación puede ser usada para anticipar la legislación; la

autorregulación puede servir para instrumentar la legislación; y la autorregulación también puede complementar la legislación.

c) La autorregulación permite compensar insuficiencias y limitaciones, favoreciendo así que las actividades objeto de la misma se ajusten a sus propios valores y normas: De ahí que se considere un complemento adecuado de la regulación, principalmente en sectores de especial conflictividad respecto de derechos fundamentales.

d) Cada ámbito del ciberespacio es factible de regularse con el propósito de otorgar confianza a los usuarios. Los esfuerzos para regular el Internet, principalmente en el campo del comercio electrónico son, en primer lugar, justificables como una alternativa ante la sociedad de la información que carece de límites territoriales y por lo tanto jurídicos, pero la autorregulación es un instrumento idóneo para contribuir a que las estructuras de gobierno puedan atender y resolver las problemáticas derivadas del Internet.

e) Para la APEC cualquier esquema de protección que se adopte, ya sea legislativo, autorregulación, o de cualquier otra índole, debería prevenir el mal uso de la información personal y el daño que con ello se pueda ocasionar a los particulares, siempre de manera proporcional tomando en cuenta la probabilidad y severidad del daño que pueda representar la obtención de información.

f) En materia laboral, los códigos de buenas prácticas son útiles pues logran un equilibrio entre las legítimas expectativas de los trabajadores acerca del correcto tratamiento de su información personal y los intereses legítimos de los empleadores para llevar sus propios negocios, en el marco de la ley.

g) Un adecuado procedimiento de otorgamiento de sellos de confianza se construye sobre una sólida base de transparencia y la rendición de cuentas respecto a la recopilación y uso de información personal.

h) Por lo que respecta a los principios sustantivos, hay grandes ventajas en las prácticas sugeridas, como son: asignar a una persona para proteger los datos personales, capacitar personal en materia de privacidad y cuidar sus transferencias de datos con terceros; pero también en la capacitación de los consumidores en materia de privacidad sobre las herramientas disponibles para ejercer sus derechos.

i) La consulta pública de los mecanismos de autorregulación es valiosa porque implica que las compañías, grupos de industrias, defensores privados, grupos de consumidores, víctimas, académicos, empresas internacionales, autoridades locales, y en general cualquier otro grupo relevante interesado en el proceso de desarrollar códigos de conducta den soluciones creativas a diversos problemas.

j) Los mecanismos de autorregulación exitosos prevén fórmulas para evaluar periódicamente la eficacia de los instrumentos de autorregulación, midiendo el grado de satisfacción de los afectados y, en caso necesario, actualizando el contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

k) Quienes adoptan un modelo de autorregulación promueven en su organización o en la de sus afiliados una intensa reorganización de sus sistemas de seguridad de la información y un cambio de cultura en el personal que trata datos personales, indispensables para alcanzar

los niveles de protección que la mayoría de las legislaciones exigen para el tratamiento de este tipo de datos.

1.9 Desventajas

1. La autorregulación pura tiene la ventaja de que se ajusta a las necesidades de cada industria, pero ofrece poca protección a los usuarios o titulares de de los datos personales.

2. Los códigos de conducta sin intervención de la autoridad incrementan la certeza, especificidad y dinamismo de las empresas, pero tienen la desventaja de que no son conocidos por los usuarios.

3. Las políticas de privacidad son útiles hacia el interior de las empresas, pero tienden a ser muy extensas, complejas e incomprensibles para los consumidores. Las empresas limitan su responsabilidad frente su cliente con solo informarlos acerca de cómo será usada su información, pero los usuarios no tienen control de esas prácticas, por lo que pierden interés y dejan de ejercer sus derechos.

4. El sello de confianza otorgado para el flujo transfronterizo de datos entre Estados Unidos y la Unión Europea ha sido un éxito, ya que las personas que cuentan con esta certificación suelen cumplirlo, pero deben existir mecanismos de verificación (algunos costosos) para que la autoridad inicie un proceso por violentar el modelo.

II.- CRITERIOS EN MATERIA DE CERTIFICACIÓN O VERIFICACIÓN

Ahora bien, uno de los aspectos que la SE ha solicitado a la CANIETI en los Términos de Referencia de este proyecto, es el relativo a analizar "criterios para ser una entidad verificadora"[264] que aborde los procesos del tratamiento de datos personales en los ámbitos de la autorregulación.

Se trata de un planteamiento relevante, no solo porque el artículo 83 del Reglamento de la LFPDPPP contemple la certificación como elemento -aunque optativo de la autorregulación-, sino porque desde un punto de vista competitivo no deben soslayarse las nuevas propuestas de la Comisión Europea y APEC encaminadas hacia un nuevo esquema de autorregulación basado en la certificación.

2.1 Unión Europea

Al respecto la primera idea a considerar es el caso de la UE, personificado por el GT29, modelo que no parece resultar paradigmático para México en cuanto a su integración, especialidad y facultades. En efecto, el GT29 (y el grupo que previsiblemente le sustituirá: el *Consejo Europeo de Protección de Datos*)[265] está conformado por las cabezas de las autoridades nacionales de protección de datos de los Estados Miembros de la Unión Europea, más el Supervisor Europea de Protección de Datos.

[264] Términos de Referencia. Pág. 14 de 20. Apartado sobre "metodología de trabajo". Inciso c), subinciso b.
[265] Ver artículo 64 de la propuesta de la UE

Así, el GT29 concentra para sí cualquier propuesta de código de conducta de ámbito comunitario, con independencia del sector o actividad a que éste se refiera, ya que por su propia naturaleza y con origen en la Directiva de Protección de Datos, es la única entidad con capacidad para "verificar" o "certificar" que un código de conducta se ajusta a las disposiciones comunitarias y (en su caso) nacionales de protección de datos.

La Directiva de Protección de Datos no prevé que el GT29 pueda conceder a otras entidades u organizaciones europeas la capacidad a nivel comunitario para que funjan como certificadoras o verificadoras del cumplimiento de la normativa europea sobre protección de datos y, con ello, ser responsables de autorizar códigos de conducta sectoriales u otorgar o permitir el uso de sellos distintivos sobre protección de datos.

Lo anterior, sin embargo, no significa que este Grupo no pueda llevar a cabo la aprobación de códigos de conducta comunitarios orientados al establecimiento de una entidad verificadora europea, como parte de un esquema de autorregulación que cumpla con las disposiciones comunitarias de la materia.

2.2 España

Por lo que hace a las disposiciones de la LOPD española y de su Reglamento, se ha encontrado que no prevén ni disponen de criterios o requisitos específicos para adoptar la forma de entidad verificadora. Como tal, debemos recordar que el artículo 32.3 de la LOPD únicamente dispone:

> *3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de*

> *acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción* ***cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia****, debiendo, en este caso, el Director de la Agencia Española de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.*

De ahí que solo pueda afirmarse, en plena congruencia con la naturaleza de este medio de autorregulación, que su contenido, la naturaleza de la entidad verificadora y la organización interna que se determine adoptar únicamente tienen como límite el cumplimiento de las disposiciones legales, reglamentarias y administrativas vigentes y aplicables; tarea que en realidad no es sencilla, tomando en consideración que el cumplimiento de todos los principios que rigen el tratamiento de datos personales debe configurarse a partir de consideraciones tanto técnicas como legales, a la vez que deben estar diseñadas para el tipo de actividad o sector en el que actúan las organizaciones que decidan adoptarlo.

En todo caso, la información analizada hasta ahora permite determinar los siguientes elementos comunes al tipo de organizaciones que en España han adoptado un “código tipo”:

- En la mayoría de los casos, se trata de organizaciones con representatividad en el sector en el que actúan, agrupaciones de profesionales o de agentes económicos dedicados a una actividad concreta.
- En menor medida, encontramos códigos de conducta adoptados por entidades individuales, cuya actividad y tipo de datos personales tratados son relevantes desde un punto de vista jurídico y con énfasis en los derechos de los titulares.

No parece entonces que el legislador español haya optado por la vía de definir criterios para certificadores o entidades verificadoras en materia de protección de datos, sino que ciñe su aprobación individual al cumplimiento de la ley. Sin embargo, sí podemos identificar una disposición legal que establece obligaciones específicas para las "entidades promotoras" de un sello de confianza, en materia de comercio electrónico y protección de los consumidores.

Es decir, nos referimos al distintivo público de confianza en línea, regulado por el Real Decreto 1163/2005, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión, que en su artículo 9 dispone:

> *Artículo 9. Obligaciones de las entidades promotoras de los códigos de conducta.*
>
> *Las entidades promotoras de códigos de conducta regulados en este real decreto tendrán las siguientes obligaciones:*
>
> *a) Administrar el «distintivo público de confianza en línea», facilitar y gestionar su utilización por los prestadores de servicios adheridos al código de conducta adoptado por ellas y que, conforme a lo previsto en el artículo 7.3, le acrediten su adhesión al sistema extrajudicial de resolución de conflictos previsto en el código de conducta.*
>
> *Las entidades promotoras, asimismo, deberán informar al órgano administrativo competente para la concesión y retirada del distintivo sobre las adhesiones al código de conducta de nuevos proveedores de servicios o sobre las bajas, mediante la comunicación quincenal de las variaciones producidas.*
>
> *b) Mantener accesible al público información actualizada sobre las entidades promotoras, el contenido del código de conducta, los procedimientos de adhesión y de denuncia frente a posibles incumplimientos del código, los sistemas de resolución extrajudicial de*

conflictos que promueve el código y los prestadores de servicios adheridos a este en cada momento.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

c) Remitir al órgano administrativo competente para la concesión y retirada del distintivo una memoria anual sobre las actividades realizadas para difundir el código de conducta y promover la adhesión a este, ***las actuaciones de verificación del cumplimiento del código*** *y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado, las sanciones impuestas y cualquier otro aspecto que las entidades promotoras deseen destacar.*

d) ***Evaluar periódicamente la eficacia del código de conducta****, midiendo el grado de satisfacción de los consumidores y usuarios y, en su caso, actualizar su contenido para adaptarlo a los cambios experimentados en la tecnología, en la prestación y uso de los servicios de la sociedad de la información y en la normativa que les sea aplicable.*

Esta evaluación deberá contar con la participación del Consejo de Consumidores y Usuarios en los términos previstos en el artículo 6 y tendrá lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

Los resultados de la evaluación se comunicarán a la Comisión Europea y al órgano administrativo competente para la concesión y retirada del distintivo.

e) Favorecer la accesibilidad de las personas que tengan alguna discapacidad o sean de edad avanzada a toda la información disponible sobre el código de conducta.

Ahora bien, donde se han establecido muchos requisitos para reconocer a una entidad certificadora (como ha sido el caso para protección de menores) ha llevado a que en países, como Estados Unidos, muy pocos organismos obtengan la autorización de la autoridad.

2.3.- México

Al acercarnos al derecho mexicano, encontramos que el Reglamento de la LFPDPPP da relevancia a la certificación, aunque de manera **opcional**:

> **Certificación en protección de datos personales**
> **Artículo 83**. Los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales.
>
> En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley.
>
> **Personas físicas o morales acreditadas**
> **Artículo 84.** Las personas físicas o morales acreditadas como certificadoras tendrán la función principal de certificar que las políticas, programas y procedimientos de privacidad instrumentados por los responsables que de manera voluntaria se sometan a su actuación, aseguren el debido tratamiento y que las medidas de seguridad adoptadas son las adecuadas para su protección. Para ello, los certificadores podrán valerse de mecanismos como verificaciones y auditorías.
>
> El procedimiento de acreditación de los certificadores a los que refiere el párrafo anterior, se llevará a cabo de acuerdo con los parámetros que prevé el artículo 43, fracción V de Ley. Estos certificadores deberán garantizar la independencia e imparcialidad para el otorgamiento de certificados, así como el cumplimiento de los requisitos y criterios que se establezcan en los parámetros en mención.

Cuando se analizó el sentido del Reglamento en materia de acreditación y certificación (epígrafe 4.5 y apartado IX de este reporte), se abrevó en la primera fuente hermenéutica disponible para determinar el alcance de estos conceptos: la Ley Federal sobre Metrología y Normalización, publicada en el Diario Oficial de la Federación el 1 de julio de 1992.

Como previamente se asentó, acreditación y certificación son dos conceptos que forman parte de la llamada Evaluación de la Conformidad**,** la cual consiste en la "determinación del grado de cumplimiento con las normas oficiales mexicanas o la conformidad con las normas mexicanas, las normas internacionales u otras especificaciones, prescripciones o características. Comprende, entre otros, los procedimientos de muestreo, prueba, calibración, certificación y verificación"[266].

A nuestro juicio, la certificación para el ámbito de la protección de datos personales no es un esquema de autorregulación, sino una herramienta optativa que tiene la ventaja de garantizar que los responsables, encargados o terceros, responden adecuadamente al principio de responsabilidad expresado en algún esquema de autorregulación.

Ello lo deducimos de la normatividad aplicable, según la cual "(…) *los esquemas de autorregulación vinculante* ***podrán incluir*** ***la certificación*** *de los responsables en materia de protección de datos personales. En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley.*"

La cuestión es determinar qué tipo de certificación resulta aplicable al ámbito de la protección de datos personales, debido a que el tema de certificación actualmente solo tiene como referencia legal lo dispuesto en la citada Ley Federal sobre Metrología y Normalización, en la cual se prevé que ésta es el procedimiento por el cual se asegura que un producto, proceso, sistema o

[266] 266 Véase al respecto: http://www.ema.org.mx/ema/ema/index.php?option=com_content&task=blogcategory&id=85&Itemid=109

servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales.

Dentro de los esquemas de la Evaluación de la Conformidad, la certificación sirve para determinar el grado de cumplimiento con las normas oficiales mexicanas o la conformidad con las normas mexicanas, las normas internacionales u otras especificaciones, prescripciones o características. La duda salta en el sentido de si los parámetros de las medidas de autorregulación pueden o no crear reglas de acreditación/certificación paralelas o distintas a aquellas normas.

A pesar de la ventajas que tienen la acreditación y la certificación, un primer análisis indica que su aplicabilidad se enfoca a procedimientos y métodos establecidos en las NOM, NMX y/o en su defecto a las normas internacionales; por lo que se podría pensar que definir sus alcances no corresponde al ámbito de meros PARÁMETROS.

Una primera interpretación indica que los Parámetros no pueden exceder los alcances de la Ley de Metrología y Normalización, ni mucho menos de su Reglamento, donde su artículo 71 contempla los requisitos para operar una entidad de acreditación.

Es decir, con un espíritu crítico o un juicio muy estricto, un parámetro –de rango inferior a un Reglamento- no podría crear nuevas reglas de acreditación/certificación, salvo que se “convenga” que esos conceptos tienen otro sentido en materia de protección de datos personales. Con un espíritu propositivo, la acreditación a que se refiere el Reglamento de la LFPDPPP podría definirse con un sentido práctico para estimular la adopción de esquemas de autorregulación, sobre todo si se toma en cuenta que finalmente la autorregulación es voluntaria y que el IFAIPD no pierde –en

ningún momento- sus facultades para verificar que los responsables cumplen con la ley y sus principios en materia de protección de datos personales.

Las ventajas de la certificación no están en duda. Sin embargo, cuando se adentra a los temas costo-beneficio, saltan aquellos factores (económicos) que un organismo acreditador o bien un organismo certificador tienen que contemplar, tales como: gastos de inspección, cuotas de verificación, gastos de acompañamiento, gastos administrativos, instalaciones adecuadas, equipo especializado, diseño de métodos confiables, sistemas de calidad de mejora continua, auditorías periódicas, personal calificado, etc., amén del interés que tendrían los responsables por cubrir el costo derivado.

Ante estas consideraciones debe tenerse en cuenta quién asume los gastos, ya que si bien la empresa es la que decide someterse a un modelo de certificación, podría afectarse al consumidor final, sobre todo en mercados con bajo nivel de competencia.

Un parámetro sobre autorregulación que incluya la acreditación/certificación debe ponderar los impactos que tendría desde un punto de vista "motivacional" si se crean nuevas obligaciones; se hacen más estrictas las obligaciones existentes; si crea o modifica trámites; si afecta derechos o prestaciones para los particulares; y si establece definiciones, clasificaciones, que conjuntamente con otra disposición afecten o puedan afectar los derechos, obligaciones, prestaciones o trámites de los particulares.

2.4 Modelos de referencia

Es importante insistir que la Comisión Europea expresó en el 2010 su preocupación en relación con los mecanismos de autorregulación que actualmente existen en el sistema Europeo, indicando que "l*as disposiciones*

actuales de la Directiva sobre protección de datos relativas a la autorregulación, es decir, la posibilidad de elaborar códigos de conducta, apenas se han utilizado hasta ahora y las partes involucradas del sector privado no las consideran satisfactorias"[267].

"La Comisión –dijo- examinará la posibilidad de crear ***regímenes europeos de certificación*** *(por ejemplo, «distintivos de protección de la intimidad») para los procesos, tecnologías, productos y servicios que sean conformes a las normas de protección de la intimidad […]*

Independientemente de las desventajas económicas que pudiera tener la certificación, actualmente existen modelos ya utilizados y en práctica en materia de acreditación y certificación. Aunque son muy estrictos sus métodos, dos modelos han resultado interesantes para los efectos de este estudio: el **European Privacy Seal (EuroPriSe)** y el **Privacy Mark en Japón** (véase epígrafe 9.3 de este reporte).

EuroPriSe, que comenzó en junio de 2007, es un ejemplo –aunque quizás poco paradigmático para México en la etapa de inmadurez de la autorregulación- que resulta útil para determinar también qué cuestiones se certifican: procesos, servicios, productos, actividades, personas o expertos.
En efecto, este modelo de certificación de EuroPriSe nos sirve –como se explica en el epígrafe 9.3.1 de este reporte) de referencia en cuanto a sus *fases*:

[267] Comisión Europea, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, *Un enfoque global de la protección de los datos personales en la Unión Europea*, Bruselas, 4 de noviembre de 2010, COM(2010) 609 final

1) En primer lugar, el fabricante o vendedor de un producto o servicio en TI encarga a un experto o centro de evaluación *acreditado*[268] que realice una evaluación del mismo[269]. El experto realizará una comprobación técnica y jurídica del producto o servicio en cuestión en dos pasos: 1) Análisis del producto en relación con la funcionalidad, el área jurídica de aplicación y la realización técnica; y 2) Comprobación de que el producto o servicio cumple con los criterios de evaluación del catálogo de criterios europeos. Finalmente plasmará los resultados en un informe de evaluación confidencial para el fabricante.

2) En una segunda fase, el fabricante o solicitante presenta el informe de evaluación a un *organismo de certificación*[270], cuya finalidad será garantizar que los certificados responden a un mismo nivel de exigencia.

En consecuencia, el organismo de certificación revisará la metodología, la coherencia y la integridad de los informes. Cualquier diferencia entre los expertos y el organismo se resuelve mediante discusiones entre el fabricante, los expertos y el organismo de certificación. Aprobado el producto por el organismo de certificación, concederá al solicitante el certificado del Sello de Privacidad Europeo (EuroPriSe) con una vigencia de *dos años*. El solicitante proporcionará un informe público al organismo de certificación, quien lo publicará en la página web de EuroPriSe.

[268] Estos expertos y el centro de evaluación deben haber recibido la aprobación de *EuroPriSe*. Actualmente han sido admitidos y registrados más de 130 profesionales en 16 países: Austria, Alemania, Bélgica, Croacia, Finlandia, Irlanda, Países Bajos, Portugal, Eslovaquia, España, Suecia, Suiza, además de Argentina, Taiwán, Reino Unido y Estados Unidos de América. A la fecha Alemania y España son los países que cuentan con más expertos registrados.

[269] <https://www.european-privacy-seal.eu/about-europrise/project-fact-sheet/fact-sheet-es.html>

[270] Se trata de una Agencia de Protección de Datos. A la fecha, esta función la ha ejercido la ULD. El encargado de la coordinación y acreditación de estos organismos será el European Privacy Seal Board.

Otra cuestión que aporta EuroPrise como ejemplo, es lo relativo al objeto de la certificación: un procedimiento voluntario de certificación válido en toda europa; un procedimiento transparente y basado en criterios fiables; la certificación por una autoridad independiente; demostrar que la privacidad debe ser implementada en productos o servicios; o la auditoría de productos o servicios tecnológicos a través de informes públicos. EuroPriSe también nos da una idea de a quiénes está dirigido su proceso de certificación o verificación: a productos y servicios tecnológicos cuya finalidad sea el almacenamiento de datos personales; a expertos jurídicos e informáticos; o agencias de Protección de Datos que pueden actuar como Autoridades de Certificación.

Y el otro modelo -aunque también muy estricto- en materia de certificación lo encontramos en el Privacy Mark System de Japón[271] (comentado en el epígrafe 9.3.2 de este reporte), cuyo mecanismo certificación es muy similar a cualquier sello de confianza, pues consiste en conceder el derecho de desplegar y utilizar el sello "PrivacyMark" a las empresas que cumplan con una serie de requisitos, durante un plazo renovable de *dos años*.

Con base en ello, la JIPDEC (Japan Information Procesing Development Corporation) puede acreditar a asociaciones, empresas y organizaciones que deseen proporcionar el servicio de certificación PrivacyMark como organismos de evaluación de la conformidad. Para ello, las empresas que deseen brindar este servicio deben someterse a una evaluación directamente ante JIPDEC. Si conforme a los criterios de evaluación de JIPDEC la empresa cumple con los requisitos para ser acreditada, se celebra un contrato con la empresa de acuerdo con los formatos previamente establecidos.

271 http://privacymark.org/

Mediante este contrato JIPDEC otorga una licencia de uso temporal a la entidad evaluadora, que le permite el uso del PrivacyMark. Además, JIPDEC entrega a la empresa un Certificado de Acreditación de PrivacyMark. La vigencia del contrato es de *2 años* contados desde la fecha de cierre del contrato.

Para los efectos del parámetro que debe expedirse en México, este esquema japonés ofrece algunos elementos que pueden servir de referencia para determinar los requisitos para ser acreditado como organismo de evaluación de conformidad (Conformity Assesment Body).

Con base en esas reglas, pueden fungir como Organismos de Evaluación de la Conformidad (OEC) las asociaciones comerciales y otras organizaciones (sociedades civiles y mercantiles) dedicadas al manejo de datos personales, siempre que cumplan los requisitos citados en el epígrafe 9.3.2 de este reporte.

En cuanto al tema de los requisitos para ser una empresa certificada y obtener un certificado, también es importante considerar el modelo del PrivacyMark, pues está diseñado para evaluar y certificar empresas que operen en Japón, algo útil para los parámetros domésticos que deben expedirse en México

En el terreno de las recomendaciones, el Sistema de Acreditación de APEC descrito en el epígrafe 9.4 de este reporte, aporta también más elementos para los temas de acreditación/certificación que deben incorporarse a los parámetros de los mecanismos de autorregulación en materia de datos personales, aunque sus reglas están más dirigidas al ámbito transfronterizo y se encuentran en proceso de construcción.

En efecto, el contenido del Cross-Border Privacy Rules (CBPR) System, generado en el Marco de Privacidad de APEC, se basa en la idea de que las organizaciones globales que obtienen, acceden, usan y procesan datos en las Economías de APEC, desarrollen e implementen enfoques uniformes dentro de sus propias organizaciones para el acceso y uso global de los datos personales.

Así, el apartado IV del Marco de Privacidad llama a las Economías a desarrollar un sistema voluntario de reglas transfronterizas de privacidad para la región en la que participarán las organizaciones que manejen datos personales entre las economías integrantes de APEC. Este sistema, aprobado en noviembre de 2011272, se compone de una serie de procedimientos y mecanismos para hacer efectiva la protección de la privacidad en la transferencia internacional de datos personales, a través de procedimientos de certificación de organizaciones y el cumplimiento eficaz de los principios de APEC.

Las organizaciones que decidan participar en el Sistema CBPR deberán implementar políticas y prácticas de privacidad que sean consistentes con el programa CBPR respecto de toda la información personal que obtengan o reciban y que esté sujeta a la transmisión transfronteriza a otra economía participante de APEC.

Estas prácticas y políticas de privacidad serán evaluadas por un Agente Responsable reconocido por APEC, quién para otorgar la certificación, se asegurará de que la organización cumpla con los requisitos que establece el programa CBPR.

272 Véase APEC, *Declaración de Honolulu: Hacia una economía regional perfecta*, Noviembre 12-13 2011, Honolulu, Hawai, Estados Unidos.

Las Economías podrán solicitar al Panel Conjunto de Vigilancia (JOP) la acreditación de Agentes Responsables para que operen en su jurisdicción, que podrán ser la propia Autoridad Competente sobre Privacidad, una organización privada de su Economía, o bien, una organización que opere como Agente Responsable en otra Economía.

La acreditación por parte de APEC como Agente de Responsabilidad solo durará un año, por lo que, un mes antes del vencimiento deberá solicitarse la renovación. Además el JOP se reserva la facultad de revisar el cumplimiento de los Agentes Responsables, solicitar a las Autoridades Competentes iniciar investigaciones sobre su funcionamiento, y solicitar la suspensión como Agente Responsable en cualquier tiempo.

Una vez que una organización ha sido certificada por un Agente Responsable para participar en el sistema CBPR, estas prácticas y políticas de privacidad se convierten en vinculantes para el Participante y podrán hacerse efectivas por la autoridad competente a fin de asegurar la conformidad con los requisitos del programa CBPR.

Asimismo, aquellas organizaciones que hayan obtenido la certificación anual de participación en el CBPR aparecerán dentro de un listado de organizaciones certificadas en el sitio web de APEC (APEC Website Guidelines, 2009/SOM1/ECSG/DPS/012), , esto con la finalidad de hacer saber a los consumidores u otros interesados sobre sus políticas de privacidad y su adecuación con el sistema de APEC y elevar su nivel de confianza.

Si bien la participación de las economías en el CBPR es voluntaria, para que el sistema sea efectivo, es necesario que sus reglas puedan ser ejecutables por los Agentes Responsables y las Autoridades Competentes. Es por ello que en ocasiones podrá resultar necesario que las Economías armonicen sus ordenamientos jurídicos a fin de facilitar y hacer efectivo su cumplimiento.

III.- MECANISMOS DE VERIFICACIÓN Y CONTROL

Unión Europea

Sobre este tema en particular previsto en los Términos de Referencia de este proyecto[273], y muy vinculado al apartado anterior, se enfatiza que a nivel europeo (comunitario) el GT29 se constituye como la única entidad verificadora y controladora del cumplimiento de los códigos de conducta sobre protección de datos, sólo podemos destacar que en el ámbito de la UE existen los mecanismos que el propio GT29 publicó en 1998 bajo el título de "*Documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo".*

Dicho documento no profundiza en los mecanismos de verificación y control que podrían ser implementados para comprobar el cumplimiento de los principios, procedimientos, sistemas, o modelos de organización implementados para cumplir con los objetivos de protección de los datos personales; sin embargo, debemos considerar que en el ámbito de actuación del GT29 estos mecanismos se encuentran subsumidos en las facultades a que se refieren los artículos 30.1.d) y 30.3, que indican:

> *Artículo 30*
> *1. El Grupo tendrá por cometido:*
> *[…]*
> *d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.*
> *[…]*
> *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.*

[273] Términos de Referencia. Pág. 14 de 20. Apartado sobre "metodología de trabajo". Inciso c), subinciso e.

Por lo que se refiera a España en particular, los ejemplos más relevantes permiten identificar los siguientes mecanismos de verificación y control:

a. Procedimientos debidamente regulados en los propios códigos tipo.

b. Conformación de órganos colegiados tanto para acciones de verificación y control, como para la eventual expulsión de cualquier miembro que incumpliere el código tipo y, en su caso, la retirada de la autorización para hacer uso del distintivo o sello de confianza que forma parte del sistema de autorregulación.

c. Posibilidad de admitir denuncias tanto internas como externas, por incumplimiento de las disposiciones del código tipo.

El sistema de códigos de buenas prácticas puesto en práctica en el Reino Unido no brinda información sobre mecanismos de verificación y control relacionados con códigos de conducta o de buenas prácticas adoptados por organizaciones o empresas en lo particular.

APEC

De lo ya expuesto acerca del **APEC Data Privacy Pathfinder** diseñado al interior del Sub-grupo de Privacidad[274], un Agente Responsable debe contar con un proceso comprehensivo para revisar las políticas y prácticas de los Solicitantes que pretendan participar en el CBPRs, así como para verificar su adecuación con los requisitos de programa del Agente.

[274] El Sub-Grupo de Privacidad de APEC fue creado en 2003 dentro del Grupo de Manejo de Comercio Electrónico (ECSG) de APEC para abordar todos los temas relacionados con privacidad. El grupo se reúne dos veces al año y reporta sus avances al ECSG quien en última instancia reporta directamente a los Ministros de APEC.

Aunque ya se ha expuesto en el apartado 9.4 de este reporte, se subraya que el proceso de certificación incluye una evaluación inicial de la conformidad que incluirá la verificación de los formatos de autoevaluación llenados por el Solicitante, y que podrá incluir además entrevistas personales o telefónicas, inspecciones del sistema de datos personales, escaneos de los sitios web, o herramientas automatizadas de seguridad.

Asimismo debe llevar un reporte comprehensivo para el Solicitante destacando los hallazgos del Agente en relación con el nivel de conformidad del Solicitante con los requisitos del programa. Cuando se haya encontrado que no se cumple alguno de los requisitos del programa, el reporte deberá incluir una lista de cambios que el Solicitante deberá cumplir a fin de obtener la certificación para participar en el CBPRs; una verificación de que los cambios señalados en el párrafo anterior han sido realizados por el Solicitante; y una certificación de que las políticas del Solicitante se encuentran de conformidad con los requisitos de programa del Agente. Cuando un Solicitante ha obtenido dicha certificación, es denominado en este documento como Participante del CBPRs.

La recertificación y declaración anual es otro elemento importante para APEC, así como lo relativo a los mecanismos para hacer cumplir los requisitos del programa, pues señala que el Agente Responsable deberá tener la facultad de poder hacer efectivos los requisitos del programa sobre los Participantes, ya sea mediante contrato o por ley y deberá tener procedimientos para imponer determinadas penalidades en los casos en que el Participante haya incumplido con los requisitos del programa y no haya corregido la falta en el tiempo que le haya sido señalado

El modelo de APEC exige además que el Agente Responsable someterá el asunto a la autoridad correspondiente para revisión y posible ejecución, cuando el Agente considere que, conforme a sus procedimientos de revisión, el Participante no ha cumplido con el CBPRs dentro del tiempo establecido, siempre que dicha falta pueda considerarse razonablemente como una infracción a la ley aplicable. En los casos en que sea posible, el Agente Responsable responderá a las solicitudes de las entidades de las Economías de APEC que se relacionen con dicha Economía y con actividades del CBPRs del Agente.

IV. PRINCIPIOS GENERALES A SEGUIR POR LAS EMPRESAS Y PRINCIPIOS ESPECÍFICOS POR SECTOR EN EL ÁMBITO DE LAS TI, DE ACUERDO A LO ESTABLECIDO EN LAS REGLAS DE OPERACIÓN DE PROSOFT

4.1 Premisas

Dentro de los Términos de Referencia del presente proyecto, la metodología previa a la conformación de los parámetros de los mecanismos o medidas de autorregulación vinculante, implica la formulación de recomendaciones para desarrollar principios generales a seguir por las empresas y principios específicos por sector en el ámbito de las TI, de acuerdo a lo establecido en las Reglas de Operación del Proyecto de Desarrollo de la Industria del Software (Prosoft)[275].

Como contexto, los objetivos de dichas Reglas de Operación de Prosoft 2.0 para el desarrollo de las TI son los siguientes:

> ***2. Objetivos***
>
> ***2.1*** *Objetivo General*
>
> *Contribuir al desarrollo del sector de tecnologías de la información buscando su crecimiento en el largo plazo en el país para así favorecer la competitividad nacional e internacional.*
>
> ***2.2*** *Objetivos Específicos*
>
> ***a)*** *Promover las exportaciones y la atracción de inversiones de TI;*
>
> ***b)*** *Elevar la cantidad y calidad del capital humano del sector de TI;*
>
> ***c)*** *Promover la adopción de un marco legal que impulse el uso y la producción de TI;*
>
> ***d)*** *Incentivar la adopción de TI ofertadas por empresas del sector ubicadas en el país;*

[275] Acuerdo mediante el cual se dan a conocer las Reglas de Operación del Programa para el Desarrollo de la Industria del Software (PROSOFT) para el ejercicio fiscal 2012 (DOF 23 de diciembre de 2011)

e) *Crear una base más amplia de empresas y agrupamientos del sector de TI, así como elevar la competitividad de los mismos;*

f) *Promover que las empresas del sector de TI alcancen niveles internacionales en capacidad de procesos, y*

g) *Aumentar las opciones y posibilidades de acceso a recursos financieros para el sector de TI.*

Dado este entorno programático, se comenta primeramente que a partir de las disposiciones de la Directiva de Protección de Datos de la Unión Europea, que al día de hoy constituye la referencia y origen de todas las legislaciones nacionales sobre protección de datos en cada uno de los Estados Miembros de la Unión Europea, se identifican determinados principios generales y específicos que deben ser observados en el ámbito de las TI, trasladados al ámbito de la LFPDPPP y Reglamento. Asimismo, de los modelos estudiados pueden extraerse más elementos para desarrollar principios de autorregulación en el ámbito nacional.

Al efecto, es importante tomar en consideración que el sector de las TI, por su íntima relación con el tratamiento de datos personales, debe ser un referente de cumplimiento frente a sus clientes y usuarios. En su caso, debe ser capaz de impulsar, a través de sus actividades y servicios, el cumplimiento de la normativa de protección de datos.

4.2 Principios generales

Como Principios Generales, se proponen los siguientes:

a. Toda industria y/o empresa del sector de las TI deberá conocer y respetar los principios que rigen el tratamiento de datos personales. A tales efectos, los agentes económicos deberán garantizar la realización de cursos de capacitación a todos los niveles, para

aquellas personas que traten datos personales con motivo de sus funciones o responsabilidades.

b. Deberá fomentarse el deber de confidencialidad como principio ineludible de cualquier persona que por razón de sus funciones o responsabilidades trata datos personales.

c. Se deberá garantizar el respeto de los derechos de los titulares de datos personales, entre otras medidas, a través de la debida implementación de procedimientos para la atención de solicitudes de derechos ARCO y la designación de la persona o departamento a que se refiere el artículo 30 de la LFPDPPP.

d. Se deberán identificar todos los sistemas de información que traten datos personales para determinar si los mismos cumplen con los niveles de seguridad exigibles para el tipo de datos que tratan.

e. Deberán adoptarse las medidas internas de cada organización que permitan programar, en el menor tiempo posible, la ejecución del análisis de brecha a que se refiere el artículo 61, fracción V del Reglamento de la LFPDPPP. Lo anterior, sin perjuicio de la necesidad de tomar en consideración cualesquiera otras de las acciones a que se refiere dicho artículo 61.

f. En su caso, deberán llevarse a cabo todas las acciones correctoras necesarias para que los sistemas de información que traten datos personales cumplan con las medidas necesarias para garantizar la seguridad de los datos personales.

g. Debe eliminarse la práctica consistente en la “conservación indefinida” de los soportes manuales en que se tratan datos personales y fomentarse la eliminación periódica de los datos personales tratados mediante dispositivos electrónicos, cuando en ambos casos se

hubiere cumplido la finalidad para la cual fueron recabados y no exista disposición legal que disponga su conservación por un tiempo mayor.

h. Siempre que su actividad lo permita, el sector de la TI deberá procurar la implantación de la "oficina sin papeles" en sus propias actividades.

i. Toda organización es responsable de las transferencias de datos (nacionales e internacionales) que deban realizarse con motivo de su actividad. En su caso, deberá asegurarse la legalidad de la transferencia, si esta se realiza para finalidades distintas de aquéllas que originaron la obtención de los datos.

j. Ninguna página web, propiedad de las empresas que participan en el sector de las TI, podrá carecer de una Política de Privacidad y, en su caso, de los Avisos de Privacidad legalmente exigibles si a través de las mismas se recaban datos personales.

4.3 Principios particulares

En este apartado, se busca anotar principios específicos para el ámbito de las TI, acentuadas a algunos subsectores particularmente relevantes en el tratamiento de datos personales en el entorno digital.

A) Empresas dedicadas al diseño, desarrollo, producción, explotación, mantenimiento y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos, custodia y administración de información:

a. Toda empresa que procese, custodie o administre datos personales por cuenta de terceros es un **encargado** en los términos a que se

refieren los artículos 3, fracción IX de la LFPDPPP y 49 de su Reglamento. Dichas empresas deberán regular este tratamiento mediante la adopción de las disposiciones contractuales (u otro instrumento jurídico) a las que se refiere el artículo 51 del Reglamento de la LFPDPPP.

b. Los encargados deberán cumplir con todas las medidas de seguridad exigibles conforme al tipo de datos personales tratados o en virtud de la finalidad del tratamiento. Ningún encargado debe tratar datos personales si sus productos, tecnologías o servicios asociados no cumplen con dichas medidas de seguridad.

c. Los empleados de los encargados deben ser consientes del deber de confidencialidad que asumen si tratan datos personales.

B) Empresas dedicadas al desarrollo de software y hardware:

a. Las empresas que desarrollen software que será destinado al tratamiento de datos personales deberán asegurarse de que sus productos permitirán a los usuarios el cumplimiento de las medidas de seguridad exigibles en virtud del tipo de datos personales que serían tratados o en relación con la finalidad del tratamiento.

b. Los fabricantes de hardware deberán asegurarse de que sus productos garantizan la disponibilidad, accesibilidad e integridad de la información en ellos tratada.

C) Empresas dedicadas a la prestación de servicios de TI o Business Process Outsourcing (BPO):

a. Si la prestación de los servicios conlleva el tratamiento de datos personales, estas empresas estarán actuando como encargados y, por lo tanto, deberán cumplir las disposiciones de la LFPDPPP y de su Reglamento aplicables.

b. En concreto, deberán regular la relación con sus clientes mediante la adopción de las disposiciones contractuales (u otro instrumento jurídico) a las que se refiere el artículo 51 del Reglamento de la LFPDPPP.

c. Los empleados de este tipo de empresas deben ser consientes del deber de confidencialidad que asumen si tratan datos personales.

D) Medios creativos digitales, redes, aplicaciones o cualquier otra tecnología de la información que permiten el intercambio, almacenamiento y/o procesamiento informatizado o por medios físicos de datos:

a. Las empresas dedicadas a estas actividades deben asegurar que las tecnologías empleadas aseguran la integridad de los datos personales intercambiados.

b. También deben garantizar que, durante su transferencia, no pueda tener acceso a la información ninguna persona que no se encuentre debidamente autorizada.

c. En el caso de llevar a cabo el registro de comunicaciones electrónicas, estas empresas deberán asegurarse que cuentan con el consentimiento de los titulares para ello o, en su caso, que existe legislación que autorice a realizar dicho registro.

E) Niños y Adolescentes. Siguiendo con las políticas de Estados Unidos, en 1998 fue promulgada la Children's Online Privacy Protection Act (COPPA) y el 21 de abril de 2000 entró en vigor la Children's Online Privacy Protection Rule, ambas con el propósito de proteger la información personal de los niños menores de 13 años que fueran obtenidos vía Internet.

Para ello el prestador del servicio debe ser parte de un modelo de autorregulación aprobado por la FTC. Las páginas de Internet obtienen un sello de confianza con el cual pueden obtener los datos personales de los menores con un permiso autentificado de los padres.

En su informe del 2010 de la FTC, se sugirió al Congreso otorgar protección a los adolescentes entre 13 y 18 años, ya fuera con la ampliación del rango de protección de la COPPA, o con una legislación especial. Ampliar la cobertura de la ley sería complejo, ya que existe una gran diferencia de comportamiento en línea y uso del Internet, incluso limitar el uso a este sector de la población podría ser contrario a la constitución por restringir su libertad de expresión y el derecho a recibir información.

F) Flujo Transfronterizo de Datos. Un principio en este rubro deriva de la Directiva 95/46/EC de la Unión Europea, conforme a la cual sólo pueden realizarse intercambios de datos con países que tengan una legislación similar que garantice una protección adecuada de datos personales. Para tal propósito fueron acordados los Safe Harbor Privacy Principles entre la Unión Europea y el Departamento de Comercio de los Estados Unidos, por lo que las empresas que cumplieran con estos requerimientos podían pedir un sello de confianza a dicho departamento con el objetivo de realizar intercambio transfronterizo de datos con la vigencia de un año. En la actualidad más de

2,700 empresas son parte del programa de flujo transfronterizo de datos con la Unión Europea276.

G) Educación. No se quiere omitir que el caso del nuevo marco norteamericano también llama a la industria a incrementar sus esfuerzos para educar a los consumidores en materia de privacidad y las herramientas disponibles para ejercer sus derechos, por lo que hay principios adicionales que debemos considerar, tales como:

La **opción simplificada** es un principio que permea en Estados Unidos, a fin de que las compañías simplifiquen las opciones del consumidor, conforme a los siguientes conceptos:

a. No es necesario otorgar una opción antes de recabar y usar datos personales para prácticas consistentes en una transacción o en la relación entre la compañía y el consumidor, o las requeridas o autorizadas por la ley.
b. Para prácticas que requieren una opción por parte del consumidor, las compañías deben ofrecer la elección al momento y en el contexto en el cual el consumidor realiza la decisión acerca de sus datos. Las compañías deben obtener el consentimiento expreso de los consumidores antes de usar sus datos de manera diferente a los propósitos con que fueron obtenidos; o para obtener información sensible para ciertos propósitos.

Igualmente se está exigiendo mayor **transparencia**, y al efecto se pide a las empresas que:

276 Véase White House, nota 1 *supra*, pág. 33.

a. Los avisos de privacidad sean más claros, cortos y estandarizados para una mejor comprensión y comparación de sus prácticas de privacidad.
b. Las compañías provean a los consumidores acceso razonable a su propia información, dicho acceso debe depender de la sensibilidad de los datos o la naturaleza del uso.
c. Todos los interesados incrementen sus esfuerzos para educar a los consumidores sobre las prácticas comerciales en materia de privacidad.

H) Otros principios derivados del *habeas data*:

1) Estimular una política dirigida a las empresas consistente en "No realizar seguimiento" (**Do not track**).
2) Mejorar las **políticas de privacidad en dispositivos móviles**, debido a que en los últimos años ha aumentado su uso y capacidades.
3) Llamar a los consultores (Data Brokers) a **cumplir con estándares de privacidad** para incrementar la transparencia de sus servicios.
4) Extender su trabajo a los **grandes proveedores de plataformas**, tales como proveedores de servicios de Internet, desarrolladores de sistemas operativos, buscadores y redes sociales, con el objetivo de incrementar sus niveles de privacidad a favor de los consumidores.
5) **Promover la autorregulación con la creación de códigos vinculantes (enforceable).** Acerca de este último punto, el Departamento de Comercio de Estados Unidos, con el apoyo de los principales actores de cada industria han comenzado un proyecto para facilitar el desarrollo de **códigos de conducta para sectores específicos**. La Comisión ha visto este esfuerzo de manera favorable y llama a las compañías, asociaciones y empresas de autorregulación a adoptar los principios contenidos en el marco normativo.

TERCERA PARTE

Recomendaciones para la redacción de Parámetros de los Esquemas de Autorregulación Vinculante en materia de Protección de Datos Personales en Posesión de los Particulares

I.- CONSIDERACIONES GENERALES

Una manera de resumir o condensar los hallazgos de los trabajos de comparación de los modelos de autorregulación en materia de privacidad y protección de datos personales en el ámbito específico de las TI, así como para generar recomendaciones concretas en la materia, es formular un primer borrador que sirva de base o *guide line* para que se emitan los denominados "*parámetros para el correcto desarrollo de los mecanismos y medidas de autorregulación*" que aunque no fueron solicitados a CANIETI por la Secretaría de Economía, se consideró oportuno elevar esta respetuosa propuesta.

Es importante señalar que con ese objetivo ha sido necesario determinar primeramente la metodología de redacción de los *parámetros,* es decir, su "formato", ya que estos modelos normativos no figuran en ningún tipo de texto conocido formalmente hasta la fecha, al menos desde el punto de vista de una norma que tenga efectos generales con ese nombre. De ahí que se hayan explorado distintos esquemas, resultando el más pertinente el que se asemeja a un reglamento administrativo.

Las consideraciones al respecto han sido necesarias para evitar que se confundan los parámetros con otras normas de la pirámide jurídica, tales como lineamientos, decretos, acuerdos, directivas, criterios, manuales, metodologías, NOM, NMX, reglas de operación, patrones, resoluciones, u otro tipo de normas que derivan de los sistemas de normalización o estandarización.

Y acerca de los efectos jurídicos de un "parámetro" se señaló con antelación que no figuran expresamente dentro de los actos administrativos de carácter general que prevé el artículo 4 de la Ley Federal del Procedimiento

Administrativo, pero se ha estimado que su naturaleza "general" abre la posibilidad hermenéutica de inscribir a los parámetros entre en las disposiciones "análogas" que deben publicarse en el Diario Oficial de la Federación y someterse como anteproyecto ante la Comisión Federal de Mejora Regulatoria junto con una manifestación de impacto regulatorio (MIR), o bien su dispensa.

Otro aspecto relevante a considerar es el concerniente al ámbito material de validez y aplicación de los parámetros, sobre todo si este estudio se ha concretado al entorno digital[277] o al ámbito de las TI como rezan los Términos de Referencia.

Considerando que existen puntos de conexión en el mundo físico y el entorno digital que los parámetros deben prever, se ha concebido proponer un anteproyecto que no se circunscriba a uno u otro entrono, sino que tenga un enfoque genérico y sin perjuicio de que paulatinamente se vayan sectorizando los parámetros.

El ámbito material de los parámetros es también muy importante que quede definido en los parámetros, es decir, que se genere la diferencia específica entre cada uno de los mecanismos de autorregulación que se prevén la LFPDPPP y su Reglamento (Códigos deontológicos; Código de buenas prácticas profesionales; Sellos de confianza; Políticas de privacidad; Reglas de privacidad corporativas; y otros mecanismos, que incluyan reglas o

[277] Reglamento de la LFPDPPP:

> **Artículo 2.** Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:
>
> **III. Entorno digital**: Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos;

estándares específicos),a fin de evitar confusiones entre los particulares y las autoridades.

La certificación de los responsables es otra cuestión que requiere definición como herramienta para garantizar el correcto desarrollo de las medidas o mecanismos de autorregulación y sobre todo, debe establecerse el debido consenso jurídico acerca de si los parámetros: 1) se van a remitir a la Ley de Metrología y Normalización en materia de acreditación/certificación; 2) se va a extender los previsto en esa Ley; o bien, 3) si se va a crear un marco *sui generis* o *ad hoc* para este tema.

Por lo que se refiere al registro de los esquemas de autorregulación, se ha considerado que es facultad exclusiva del IFAIPD proveer las reglas correspondientes, pues conforme al artículo 86 del Reglamento de la LFPDPPP al mismo le corresponde llevar su administración.

II.- SUGERENCIAS DE LA INDUSTRIA

Es importante señalar que en el terreno de las recomendaciones, en la realización de este estudio se consultó a la administración del Sello de Confianza de la Asociación Mexicana de Internet, A.C. (AMIPCI), que como reiteradamente se ha señalado en este estudio, es la única entidad nacional que viene realizando esfuerzos importantes en materia de autorregulación de datos personales en el entorno digital.

Sus consideraciones o expectativas sobre los parámetros de los esquemas de autorregulación vinculante arrojan importantes elementos que pueden enriquecer el trabajo de la Secretaría de Economía y el IFAIPD, las cuales –y con la debida autorización de la AMIPCI- se exponen a continuación:

Niveles del esquema

a) El esquema de autorregulación deberá contar con niveles de protección adecuados para cada tipo de información recolectada por el mismo (persona física o moral certificadora).

b) El esquema de autorregulación deberá contar con procesos o procedimientos formales de acuerdo a los niveles de protección requeridos por cada tipo de información recolectada.

Ámbito de aplicación

a) Deberán ser aplicables en todo el territorio nacional, dado que es una ley federal.

b) Asimismo deberán tener alcance y vinculación internacional, considerando el Cross Border Privacy Rules System de APEC, o cualquier otro esquema de cooperación transfronteriza vinculante o no, que las autoridades establezcan para tales fines, como por ejemplo un puerto seguro (safe harbor).

c) Ser candidatos para formar parte de alianzas o grupos de cooperación transfronteriza en la materia, tales como la ATA, la Red Iberoamericana de Protección de Datos o cualquier otro similar.

d) Los esquemas de autorregulación deberán enfocarse en dos ámbitos generales: el físico y el digital.

e) A partir de lo anterior y para una adecuada representatividad y experticia, sería conveniente que se vincularan preferentemente en sectores: salud, telecomunicaciones, educación, legal, economía, publicidad, mercadotecnia, etc.

Derechos del titular

a) El esquema establecerá mecanismos eficientes para facilitar al titular el ejercicio de sus derechos ARCO.

b) El esquema establecerá mecanismos de comunicación entre éste y el titular.

c) El esquema establecerá procesos que toman en consideración las limitaciones temporales propuestas en la ley para atender requerimientos del titular.

d) El esquema generará evidencia operativa suficiente para cumplir con los requerimientos de la LFPDPP en cuanto a la atención de peticiones de derechos ARCO de los titulares y el debido tratamiento de los datos.

e) El esquema delimitará algún mecanismo alternativo de mediación de controversias en materia de datos personales y privacidad, entre los titulares y los responsables.

Revisión del esquema

a) El esquema establecerá prácticas de revisión interna que garanticen su vigencia en relación al cumplimiento de las disposiciones de la LFPDPPP.

b) El esquema propondrá criterios de evaluación que permita homologar y normalizar los resultados obtenidos por las empresas que opten por su implementación respecto del tratamiento de datos que realicen.

c) El esquema establecerá criterios de revisión que permitan evaluar su viabilidad como mecanismo de autorregulación, de acuerdo al tipo de datos recolectados por la organización adherente.

d) El esquema establecerá prácticas de reporteo y seguimiento para brindar información suficiente a la autoridad en relación a los resultados obtenidos en temas de tratamiento, cuando la organización decide implementar el esquema.

e) El esquema propondrá ejercicios adecuados de revisión periódica por entidades externas que validen el buen funcionamiento de los

controles aplicados para proteger información de titulares, conforme la clasificación de la misma.

f) El esquema acordará reglas para trabajar con las entidades que auditen el cumplimiento de la LFPDPPP, a través del mismo esquema.

g) Podrá haber auditores de tercera parte dentro del propio esquema de autorregulación, para coadyuvar en el debido funcionamiento del mismo.

h) El esquema deberá contener un apartado de selección, evaluación, aprobación y revisión de auditores de tercera parte, incluida la periodicidad y vigencia de éstos.

i) El esquema propondrá criterios de selección de dichos auditores de revisión de tercera parte, para garantizar su competencia.

j) El esquema propone medios de evaluación de las entidades de revisión certificadas a manera de garantizar su objetividad.

Alcance del esquema

a) El esquema cubre la totalidad de los datos recolectados por éste.

b) El esquema cubre la totalidad de las operaciones del mismo, en relación al tratamiento de datos personales de sus adherentes.

c) El esquema establecerá claramente su alcance y lo pone a disposición de las autoridades, los posibles adherentes, los titulares y usuarios en general.

Control del esquema

a) El esquema establecerá controles físicos, tecnológicos o procesales adecuados conforme el tipo de datos recolectados por la organización adherente.

b) El esquema establecerá medios de comunicación efectivos y adecuados para garantizar que los titulares cuentan con información suficiente en relación al tipo de controles utilizados para resguardar sus datos.

c) El esquema definirá medios alternos de protección para la organización en caso de que los principales se vean comprometidos

Responsabilidad del esquema

a) El esquema establecerá roles y responsabilidades claros dentro de su organización.

b) El esquema identificará los roles y responsabilidades para que los titulares sepan a quién presentar sus requerimientos de ejercicio de derechos.

c) El esquema realizará campañas educativas y seminarios informativos en torno a la protección de datos personales y privacidad para sus adherentes.

Seguridad

a) El esquema establecerá medidas compensatorias y de rápida reacción al presentarse un incumplimiento en relación a sus requerimientos, incluidos preceptos de la propia LFPDPPP.

b) El esquema establecerá controles para garantizar que al presentarse un incumplimiento, se publiquen los comunicados necesarios ante autoridades y titulares.

c) El esquema establecerá controles de mantenimiento de las condiciones de seguridad posterior a la tipificación y entendimiento de una brecha de seguridad.

d) El esquema establecerá medios de comunicación bidireccional entre la organización y entidades externas (IFAI, SE, adherentes, titulares) para atender requerimientos en el inter de la investigación y reacción ante un incidente de seguridad.

e) El esquema establecerá procedimientos que permitan garantizar la eliminación de la causa de un incidente de seguridad en el hayan sido vulnerados datos personales.

III.- RECOMENDACIONES ESPECÍFICAS

A manera de recomendaciones concretas, en esta sección se hace una exposición general del contenido que deben tener los parámetros sobre los mecanismos de regulación *in genere*, con precisiones que garanticen la eficacia de los mismos y algunos elementos *ad cautelam* en materia de acreditación/certificación, conforme a lo siguiente:

A).- TIPO DE INSTRUMENTO JURÍDICO.

Se propone la elaboración de un ACUERDO por el que se den a conocer los parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

B).- CONTENIDO

CONSIDERANDOS

En esta sección se deben explicitar los fundamentos del acto administrativo consistente en el acuerdo que da conocer los parámetros, vinculándolo al Plan Nacional de Desarrollo y al Programa Sectorial de Economía 2007-2012.

CAPÍTULO I
DISPOSICIONES GENERALES

Debe definir el objetivo de los parámetros y su ámbito de aplicación, así como definiciones básicas para su debida comprensión. Igualmente se establecen las características de los esquemas de autorregulación vinculante.

CAPITULO II
DE LAS CLASES DE ESQUEMAS DE AUTORREGULACIÓN

En este apartado corresponde señalar los elementos primordiales de los distintos esquemas (medios o mecanismos) de autorregulación referidos en la LFPDPPP y su Reglamento: códigos deontológicos, códigos de buena práctica profesional, sellos de confianza, políticas de privacidad y otros mecanismos.

CAPITULO III
DEL CONTENIDO DE LOS ESQUEMAS DE AUTORREGULACIÓN

En este capítulo se requiere desarrollar los contenidos mínimos obligatorios de los distintos esquemas de autorregulación para que puedan ser registrados por el IFAIPD, así como el tema de su ámbito de aplicación.

Aquí se prevén reglas sobre la complementariedad[278], mecanismos para medir la eficacia del esquema adoptado, consecuencias y medidas correctivas en caso de incumplimiento, identificación de los responsables, sistemas de supervisión y vigilancia, capacitación, medidas concretas tomadas respecto a la protección a categorías especiales de titulares (*menores, con discapacidad y no hispano hablantes*), transferencias nacionales e internacionales de datos personales, administración del esquema, procedimientos para la protección de los datos[279] y mecanismos alternativos de solución de controversias

Los parámetros deben requerir a los solicitantes, la identificación clara y precisa del ámbito de aplicación de los esquemas de autorregulación. Para esto, se sugiere circunscribir la aplicación de los mecanismos a alguno de los siguientes supuestos:

a) Un tipo de información personal en específico.

b) Una actividad o clase de actividades específicas.

c) Un sector profesional o industrial específico.

278 En nuestra opinión, los esquemas de autorregulación deben garantizar un mínimo de flexibilidad a la hora de diseñar los mecanismos específicos de cumplimiento. En ese sentido, este apartado cubre los rubros de:

a) Reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos.

b) Mecanismos para facilitar el ejercicio de los derechos ARCO (incluyendo de manera detallada la forma de atención a las solicitudes que se formulen por los titulares afectados, así como modelos para el ejercicio de los mismos, en su caso).

c) Procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la Ley.

d) Procedimientos o mecanismos que se emplearán para hacer eficaz la protección de datos personales por parte de los adheridos.

279 Se estima conveniente que el tema de tratamiento de quejas y solución alternativa de Controversias sea un elemento voluntario y no obligatorio.

Asimismo, puede referirse a los tipos de soporte o medios en los que se contengan los datos personales, como son:

a) En soporte físico,

b) En soporte electrónico,

c) En el entorno digital, y/o

d) En soporte mixto.

Se recomienda que los parámetros señalen de manera expresa que los esquemas de autorregulación que se pretendan inscribir ante la autoridad correspondiente, siempre serán complementarios y coadyuvantes de la Ley. En ese sentido, en el tratamiento de los datos personales se deberán prever disposiciones específicas por las cuales los miembros observen los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad a que se refiere el artículo 6 de la LFPDPPP.

Asimismo, deberían prever mecanismos que garanticen a los titulares de los datos, el ejercicio de los derechos de acceso, rectificación, oposición y cancelación, de acuerdo con la Ley y su Reglamento.

Se recomienda que los parámetros requieran a los solicitantes indicar la manera en que se garantizará la adhesión a los esquemas de autorregulación de manera voluntaria.

Adicionalmente, se recomienda prestar especial atención en aquellos casos en que los esquemas de autorregulación sean presentados por asociaciones, colegios u otros que impliquen la asociación obligatoria para el ejercicio de una profesión, con el objetivo de que el mecanismo no violente sus derechos o intente desplazar a sus integrantes.

Se recomienda que los parámetros establezcan como requisito de inscripción, la designación de un órgano individual o colegiado encargado de la administración del mecanismo de autorregulación vinculante propuesto.

En el supuesto de los códigos deontológicos, sellos de confianza y otros equivalentes, el establecimiento de un administrador podría facilitar la comunicación entre la autoridad y la entidad autorregulada, así como la funcionalidad y supervisión del mecanismo. Asimismo, este órgano podrá tener a su cargo la función de incluir nuevos miembros, la elaboración de reportes de cumplimiento, así como presentar la información que en su caso le sea requerida por la autoridad para la supervisión y vigilancia del mecanismo.

Se recomienda que los parámetros requieran el establecimiento de procedimientos para la revisión sistemática de los esquemas de autorregulación a cargo de los propios solicitantes, los cuales evalúen al menos:

a) Cumplimiento de las obligaciones asumidas por los adheridos al mecanismo;

b) Funcionamiento de los procedimientos establecidos en el mecanismo;

c) Resumen de las evaluaciones de vigilancia realizadas durante el periodo revisado; y

d) Adecuación de las cláusulas a las actividades y circunstancias actuales de los sujetos obligados.

A fin de dotar de eficacia a este requisito, se recomienda especificar los intervalos en los cuales los responsables o administradores de los esquemas de autorregulación deban llevar a cabo dichos procedimientos, así como la pertinencia de presentar un reporte de los hallazgos en un informe periódico ante la autoridad.

Como complemento de lo anterior, se recomienda que los parámetros establezcan la forma en la cual los solicitantes acrediten el requisito de supervisión y vigilancia al que se refiere el artículo 82 del Reglamento.

De este modo pueden incluirse procedimientos adecuados que garanticen el cumplimiento del mecanismo de autorregulación y de la Ley.

Asimismo, se recomienda que estos procedimientos culminen con un reporte en el que se expresen los hallazgos y, en su caso, las no conformidades, las cuales podrían dar lugar a las sanciones a que nos referimos más adelante.

Para la eficacia de este requisito, se recomienda señalar el tipo de personas u órganos encargados de llevar a cabo las labores de supervisión y vigilancia.

Para el efectivo cumplimiento de los esquemas de autorregulación es indispensable que los mismos cuenten con medidas disuasorias. En este sentido, se recomienda que los parámetros incluyan el tipo de sanciones idóneas, así como el órgano encargado de administrarlas.

En el caso de los códigos deontológicos, sellos de confianza u otros análogos, dichas sanciones pueden consistir en:

a) Amonestaciones;

b) Sanciones económicas;

c) Suspensión temporal o definitiva de la adhesión al mecanismo.

Como es de esperarse, la suspensión de los derechos del miembro sancionado podrá implicar también la terminación de la licencia de uso del distintivo o marca que en su caso se otorgue a los adheridos.

A fin de garantizar los derechos de las partes, se sugiere que el establecimiento de las sanciones se realice de conformidad con los principios de contradicción, audiencia, accesibilidad y proporcionalidad

Vigencia y renovación. Para garantizar un seguimiento y actualización constante, se recomienda que los parámetros establezcan la vigencia que tendrán los esquemas de autorregulación vinculante, así como el procedimiento que se deberá seguir para su renovación.

Por ejemplo, se puede establecer que la inscripción de los esquemas de autorregulación vinculante tenga una vigencia de dos años, tras lo cual, sea necesario someter el mismo a un procedimiento de renovación.

En general, se considera recomendable solicitar para la renovación los mismos documentos que fueron requeridos por la autoridad para la primera inscripción, siempre que estos hayan sufrido modificaciones o actualizaciones.

Revocación. Se recomienda que los parámetros establezcan causas de revocación de la inscripción del mecanismo de autorregulación. En el caso de los códigos deontológicos, sellos de confianza u otros análogos, dicha revocación podría tener lugar en alguno de los siguientes casos:

a) Incumplimiento sistemático de sus disposiciones por parte de sus miembros;

b) Ineficacia del Código para el debido cumplimiento de la ley;

c) Exista falsedad de información en la solicitud de inscripción o en la presentación de los reportes de revisión, o renovación;

d) No se cumplan las recomendaciones que hayan sido conclusión de los reportes de revisión; y

e) Otras que a juicio de la autoridad así lo ameriten.

Capacitación. A fin de dar cumplimiento con lo dispuesto por el artículo 82 de la LFPDPPP, se recomienda que los esquemas de autorregulación establezcan los programas de capacitación en materia de protección de datos personales que estarán disponibles para los adheridos u obligados por el mecanismo correspondiente.

CAPITULO IV
DE LA CERTIFICACIÓN

Establecer el marco sobre el tema de la acreditación y la certificación, a fin de establecer su objeto, características, funciones de los acreditadores y certificadores, procedimientos y tipos de certificados. Asimismo este apartado debe establecer las obligaciones de las personas físicas o morales que sean reconocidas como certificadores en materia de protección de datos personales, bajo los principios de independencia, objetividad, confidencialidad y verificación.

Este capítulo aborda también los temas relativos a vigencia, renovación y revocación de la acreditación.

Requisitos de las personas físicas y morales. En primer lugar, se sugiere establecer en los parámetros las cualidades y características que deberán acreditar ante la autoridad, aquellas personas físicas y morales que deseen prestar el servicio de certificación.

En ese sentido, se recomienda tener en consideración lo siguiente:

a) Tener domicilio en México.

b) Especificar el tipo de persona jurídica que podrá solicitar la acreditación: Sociedad Civil, Sociedad Anónima, Sociedad de Responsabilidad Limitada, etc.

c) Documentación que acredite los conocimientos y experiencia suficiente en materia de datos personales, así como del área específica en la que desea prestar el servicio de certificación. La cual puede consistir en título que acredite una licenciatura o ingeniería afín, certificación de alguna entidad certificadora internacional o equivalente y cursos de capacitación, entre otros.

Solicitud. Se sugiere que en la solicitud de acreditación, las personas físicas o morales presenten:

a) Formato oficial emitido por la autoridad, debidamente requisitado en original y copia.

b) Documentación que acredite conocimientos y experiencia suficiente en materia de datos personales, así como en el área específica en la que desea prestar el servicio de certificación.

c) En el caso de las personas morales, se deberá presentar acta constitutiva original y copia para cotejo.

d) Manual de operaciones que contenga los procedimientos de evaluación, verificación y auditoría necesarios para otorgar y mantener un certificado.

e) Modelo de contrato de prestación de servicios de certificación en materia de protección de datos personales.

f) Modelo de certificado propuesto.

Ámbito de aplicación. Al igual que el resto de los esquemas de autorregulación vinculante, las personas que presten el servicio de certificación deberían circunscribir su actividad conforme a alguna de las siguientes categorías sugeridas:

a) Tipo de datos personales sobre los que se especializará el acreditado;

b) Tipo de productos o de servicios objeto de la certificación.

Independencia. Las personas que deseen ser acreditadas como certificadores en materia de protección de datos personales deben demostrar su independencia, y en su caso, garantizar que su función de certificación se mantenga libre de cualquier interés o influencia que pudiera comprometer su juicio profesional, objetividad e integridad.

A fin de garantizar lo anterior, el interesado podría incluir en sus procedimientos, mecanismos que permitan la inhibición del acreditado en un asunto particular que así lo requiera. Dicha inhibición sería requerida siempre que el acreditado se encuentre relacionado con el responsable que solicita la certificación, de forma que pudiera comprometerse la objetividad del acreditado.

Algunos criterios más específicos en este sentido podrían incluir:

a) Prohibir cualquier certificación de un responsable, cuando éste tenga alguna forma de asociación con el acreditado.

b) Prohibir el ofrecimiento de servicios que afecten su imparcialidad, como lo es el de consultoría.

Finalmente, debería establecerse que los procedimientos y políticas de certificación que implemente el acreditado no deberán ser discriminatorios.

Verificación de los datos. Dadas las características especiales que reviste el modelo de certificación, es necesario que la autoridad cuente con atribuciones que le permitan vigilar el debido cumplimiento de esta función.

En este sentido, la autoridad por sí o por medio de terceros podría practicar procedimientos de verificación *in situ* a fin de comprobar la documentación presentada por el solicitante.

En estos casos, las visitas deberán ser planeadas y notificadas previamente al solicitante, especificando la documentación, los procesos y demás información que vaya a ser verificada por la autoridad.

Las visitas se restringirán únicamente al lugar en donde el solicitante pretenda prestar el servicio de certificación.

Asimismo, la autoridad en cualquier momento podría requerir información y documentación sobre cualquier situación relacionada con los procesos de certificación que lleve a cabo el acreditado. De igual modo, la autoridad podrá realizar visitas *in situ* en cualquier momento para comprobar dicho funcionamiento.

Finalmente, se sugiere que en las revisiones que la autoridad realice, esta elabore un reporte que será comunicado al interesado al término de la visita en donde especificará los hallazgos encontrados, y en su caso, las recomendaciones que el acreditado deba realizar. Para ello, la autoridad debería indicar un tiempo límite en el cual el interesado deberá dar cumplimiento.

Revocación. En relación con la revocación de la acreditación, los parámetros deberán establecer de manera clara y precisa los supuestos en los que esta tendrá lugar.

Así, se sugiere que estos contemplen:

a) Falsedad de información presentada en la solicitud.

b) No haber dado cumplimiento en el término fijado, a las recomendaciones efectuadas por la autoridad en los procedimientos de revisión que esta efectúe.

c) Que el Instituto haya sancionado de forma sistemática a los responsables certificados por el acreditado, de manera que se demuestre la ineficacia del mecanismo de autorregulación.

Certificación. Para la prestación del servicio de certificación, se sugiere que el acreditado elabore un protocolo de evaluación de la conformidad de los responsables, el cual deberá establecer la forma en la que se evaluará el cumplimiento de cada uno de los principios de la ley y su reglamento, así como el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los titulares de los datos. En ese sentido, se sugiere que el procedimiento de certificación incluya:

a) Una evaluación inicial de la conformidad, que incluirá la verificación de los formatos de autoevaluación que al efecto sean completados por el solicitante, lo que podrá incluir entrevistas personales o telefónicas, inspecciones del sistema de datos personales, de las medidas de seguridad, evaluación de riesgos, y escaneos de los sitios webs y/o de las aplicaciones.

b) Elaboración de un reporte que destaque los hallazgos del acreditado en relación con el nivel de conformidad del solicitante, así como los cambios o adecuaciones que en su caso el solicitante deba realizar.

c) Verificación del cumplimiento de las recomendaciones expuestas en el reporte.

d) Certificación de las políticas de privacidad del solicitante de conformidad con la Ley, el Reglamento y los protocolos de actuación del acreditado.

Asimismo, el acreditado deberá contar con un protocolo que establezca los procedimientos de supervisión, vigilancia y auditoría, por los cuales efectúe una revisión periódica de los certificados que otorgue.

Finalmente, se sugiere que cuando el acreditado tenga conocimiento de que alguna práctica del responsable certificado pueda constituir un incumplimiento de la ley, del reglamento o del protocolo del acreditado, éste deba iniciar inmediatamente un proceso de revisión para verificar su conformidad. En caso de encontrar fallas o incumplimientos, el acreditado lo notificará al responsable a fin de hacer las correcciones necesarias en un tiempo determinado. La falta de cumplimiento del responsable deberá dar lugar a la revocación del certificado por el acreditado.

Revocación de la certificación. En cuanto a la revocación de la certificación, esta es una facultad que en principio corresponde al acreditado que otorgó la certificación. En ese sentido, al igual que la revocación de la acreditación, y a fin de dotar de certeza jurídica a los responsables certificados, se sugiere establecer las causas expresas y claras en los que esta procederá. Al respecto, se sugiere que esta tenga lugar cuando:

a) Exista falsedad de la información presentada por el responsable al acreditado para obtener la certificación.

b) El responsable no haya dado cumplimiento a las recomendaciones que el acreditado haya efectuado durante los procedimientos de verificación y auditoría.

c) Otros supuestos, como podría ser la falta de pago de las contraprestaciones que al efecto, y de acuerdo con los términos del contrato, hayan sido prefijados.

CAPITULO V
DE LA NOTIFICACIÓN DE LOS ESQUEMAS DE AUTORREGULACIÓN

En esta sección se establecen los requisitos generales para el trámite de notificación de los esquemas de autorregulación que convengan los particulares en términos del primer párrafo del artículo 44 de la LFPDPPP ante las autoridades sectoriales que correspondan y al Instituto, que podría ser por escrito o a través del sitio Web del IFAIPD.

CAPITULO VI
DEL REGISTRO

Solamente se establece que los esquemas de autorregulación notificados se inscribirán en el Registro de Esquemas de Autorregulación Vinculante de Protección de Datos Personales en Posesión de Particulares a cargo del Instituto, siempre que su reúnan los requisitos previstos en estos Parámetros y los que establezcan las Reglas para el Registro de Mecanismos y Medidas de Autorregulación en la materia. Corresponderá al IFAIPD emitir las reglas sobre su administración.

ARTÍCULOS TRANSITORIOS

Aquí se señala que los parámetros serán vigentes al día siguiente de su publicación en el Diario Oficial de la Federación y que, para efectos su implementación, se establecerá la coordinación con las distintas dependencias de la Administración Pública Federal a convocatoria del titular de la Secretaría.

Se considera fundamental un tipo de Comité, Comisión o Grupo de Trabajo que implemente sectorialmente este tema, toda vez que son varias las dependencias públicas que intervienen en el tema de la protección de datos personales y las cuales se deben notificar los esquemas de autorregulación que se adopten por los particulares, tomando en cuenta lo que la LFPDPPP establece en su artículo 40:

> **Artículo 40.-** La presente Ley constituirá el marco normativo que las **dependencias** deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto

Conforme a este numeral, las dependencias que intervienen son –además del IFAIPD- las que así se reconocen en la Ley Orgánica de la Administración Pública Federal:

> **Artículo 26.-** Para el despacho de los asuntos del orden administrativo, el Poder Ejecutivo de la Unión contará con las siguientes **dependencias**:
>
> Secretaría de Gobernación
> Secretaría de Relaciones Exteriores
> Secretaría de la Defensa Nacional
> Secretaría de Marina
> Secretaría de Seguridad Pública
> Secretaría de Hacienda y Crédito Público
> Secretaría de Desarrollo Social
> Secretaría de Medio Ambiente y Recursos Naturales
> Secretaría de Energía

Secretaría de Economía
Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación
Secretaría de Comunicaciones y Transportes
Secretaría de la Función Pública
Secretaría de Educación Pública
Secretaría de Salud
Secretaría del Trabajo y Previsión Social
Secretaría de la Reforma Agraria
Secretaría de Turismo
Consejería Jurídica del Ejecutivo Federal

FIRMA.

Este acuerdo lo suscribiría el Secretario de Economía, conforme a una interpretación estricta del artículo 43 fracción V de la LFPDPPP y relativos de su Reglamento.

IV.- PROPUESTA DE PARÁMETROS

Con los antecedentes indicados en los apartados precedentes, se ha considerado que el ACUERDO ADMINISTRATIVO es la vía idónea para dar a conocer los parámetros que elabore la Secretaría de Economía en coadyuvancia con el IFAIPD, conforme al siguiente anteproyecto.

Acuerdo mediante el cual se dan a conocer los Parámetros para el correcto desarrollo de los Esquemas de Autorregulación Vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Economía.

Con fundamento en los artículos 16, 89, 92 de la Constitución Política de los Estados Unidos Mexicanos; 11, 12, 13, 34 fracciones XXIII y XXXI de la Ley Orgánica de la Administración Pública Federal; 4 de la Ley Federal de Procedimiento Administrativo; 43 fracción V, 44 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares; 79, 80, 81, 82, 83, 84, 85 y 86 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares; 3, 5 fracción XVI y 24 del Reglamento Interior de la Secretaría de Economía; y

CONSIDERANDO

Que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, señala que “Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”.

Que el Plan Nacional de Desarrollo (PND) 2007-2012 tiene como finalidad establecer los objetivos nacionales, las estrategias y las prioridades que durante la presente Administración deberán regir la acción del gobierno;

Que el Eje 2 Economía competitiva y generadora de empleos del PND tiene como uno de sus objetivos fortalecer el Estado de Derecho y la seguridad pública, garantizando certidumbre legal y jurídica a las personas y a la propiedad;

Que el Programa Sectorial de Economía 2007-2012 establece como objetivo rector 2.5, elevar la competitividad de las empresas mediante el fomento del uso de las tecnologías de información, la innovación y el desarrollo tecnológico en sus productos y servicios, a su vez, como objetivo rector 3.2 incrementar la participación de México en los flujos de comercio mundial y en la atracción de Inversión Extranjera Directa (IED), en el cual se establece que se deberá posicionar a México como un oferente en el mercado de servicios de tecnologías de información;

Que el artículo 43 fracción V de la Ley Federal de Protección de Datos Personales en Posesión de Particulares establece que es competencia de la

Secretaría de Economía expedir los parámetros necesarios para el correcto desarrollo de los esquemas de autorregulación a que se refiere el artículo 44 de la propia Ley, en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos, por lo que ambos organismos desarrollaron trabajos coordinados de consulta y análisis institucional para emitir los presentes parámetros;

Que con el propósito de crear las bases necesarias para que los particulares, sean estas personas físicas o morales, desarrollen esquemas de autorregulación vinculante en materia de protección de datos personales y que complementen lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se expide el siguiente:

ACUERDO

Único.- Se dan a conocer los parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

PARÁMETROS PARA EL CORRECTO DESARROLLO DE LOS ESQUEMAS DE AUTORREGULACIÓN VINCULANTE A QUE SE REFIERE EL ARTÍCULO 44 DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.

CAPÍTULO I
DISPOSICIONES GENERALES

Objetivo

Artículo 1.- Los presentes parámetros tienen por objeto establecer reglas para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

Ámbito de aplicación

Artículo 2.- Los estándares previstos en estos parámetros son de carácter general y de aplicación en todo el territorio de los Estados Unidos Mexicanos, y han sido formulados por la Secretaría de Economía, en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos, como obligatorios para determinar o valorar la pertinencia y correcto desarrollo de los esquemas de autorregulación vinculante en materia de protección de datos personales en posesión de particulares adoptados por los responsables y encargados con el fin de complementar lo dispuesto por la Ley Federal de Protección de Datos personales en Posesión de los Particulares, su Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones.

Artículo 3.- La inobservancia de los presentes parámetros impedirá que los esquemas de autorregulación notificados conforme al artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,

sean inscritos en el Registro que al efecto administre el Instituto Federal de Acceso a la Información y Protección de Datos Personales.

Artículo 4. De conformidad con lo establecido en el Reglamento, los esquemas de autorregulación vinculante tienen los siguientes objetivos primordiales:

I. Coadyuvar al cumplimiento del principio de responsabilidad al que refiere la Ley y el Reglamento;
II. Establecer procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la Ley;
III. Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal que esté en su posesión;
IV. Promover que los responsables de manera voluntaria cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la Ley, y mostrar a los titulares su compromiso con la protección de datos personales;
V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;
VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;
VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;
VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de

privacidad, incluyendo herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación, y

IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Artículo 5.- Estos esquemas serán vinculantes para quienes se adhieran a los mismos; no obstante, la adhesión será de carácter voluntario. En el caso de asociaciones, cámaras u organismos empresariales o profesionales, de ningún modo se podrá condicionar la membresía a ésta a la suscripción de un esquema de autorregulación.

Definiciones

Artículo 6.- Para efectos de estos parámetros, se entenderá por:

I. Esquema de autorregulación vinculante: todo mecanismo o medida de autorregulación que cuente con los requisitos a que se refieren los artículos 82, 83 y 84 del Reglamento, y que hayan sido notificados conforme a estos parámetros y registrados ante el Instituto.

II. Instituto: el Instituto Federal de Acceso a la Información y Protección de Datos Personales.

III. Ley: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

IV. Parámetros: Los que se refiere el presente acuerdo, mismos que se encuentran dirigidos al correcto desarrollo de los Esquemas de Autorregulación Vinculante a que se refiere el artículo 44 de la Ley

Federal de Protección de Datos Personales en Posesión de los Particulares.

V. Reglamento: el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

VI. Secretaría: la Secretaría de Economía.

VII. Registro: el Registro de Esquemas de Autorregulación Vinculante de Protección de Datos Personales en Posesión de Particulares a cargo del Instituto

Características generales

Artículo 7.- Los esquemas de autorregulación serán obligatorios para los adheridos al mismo y contendrán las sanciones por su incumplimiento conforme a los presentes parámetros.

Artículo 8.- Todo esquema de autorregulación que se pretenda notificar a las autoridades sectoriales y registrar en el Instituto deberá contener en su diseño, mecanismos que garanticen los principios rectores de la protección de datos personales previstos en el artículo 6 de la Ley:

I. Licitud;
II. Consentimiento;
III. Información;
IV. Calidad;
V. Finalidad;
VI. Lealtad;
VII. Proporcionalidad, y

VIII. Responsabilidad.

Artículo 9.- Todo esquema de regulación que se notifique y pretenda registrar de conformidad con los presentes parámetros, deberá contener la información relativa a los precios estimados que tendrán para los suscriptores o adherentes, si los hubiere.

Artículo 10.- Los esquemas de autorregulación podrán reunir las características de dos o más mecanismos o medidas previstos en la Ley, su Reglamento y estos parámetros, lo cual deberá informarse al momento de su notificación.

CAPITULO II
DE LAS CLASES DE ESQUEMAS DE AUTORREGULACIÓN

Códigos deontológicos

Artículo 11- Se consideran códigos deontológicos, todo acuerdo, convenio, contrato o cualquier otro instrumento celebrado por escrito, en el que se establecen reglas y principios que tienen como finalidad regular la conducta de los integrantes de una empresa, grupo de empresas u organización, en relación con el tratamiento y la protección de datos personales, de conformidad con la Ley, su Reglamento y las disposiciones aplicables del sector correspondiente.

Artículo 12.- Los aspectos relacionados con la protección de datos personales, podrán formar parte de códigos de ética generales que comprendan otros aspectos distintos, siempre que estos se apeguen a la

Ley, su Reglamento, las disposiciones aplicables del sector correspondiente y a estos parámetros.

Códigos de buena práctica profesional

Artículo 13.- Son códigos de buena práctica profesional, todo acuerdo, convenio, contrato o cualquier otro instrumento similar celebrado por escrito, adoptado por una asociación profesional en el que se precisan los compromisos que asumen los responsables y encargados para garantizar un adecuado tratamiento y protección de datos personales, de acuerdo con la Ley, su Reglamento, las disposiciones aplicables del sector de que se trate y estos parámetros.

Sellos de confianza

Artículo 14.- Son sellos de confianza los mecanismos de autorregulación consistentes en distintivos, marcas u otros similares, cuyo uso es otorgado o licenciado a responsables y encargados de datos personales por un tercero, con el objeto de garantizar frente a los titulares el tratamiento y protección de sus datos personales de conformidad con la Ley, su Reglamento, las disposiciones aplicables del sector correspondiente y estos parámetros, mediantes servicios de verificación, auditoría, revisión o certificación.

Reglas de privacidad corporativas

Artículo 15.- Son reglas de privacidad corporativas, el conjunto de principios y reglas de carácter interno, adoptados por un grupo de empresas que pertenezcan a un mismo grupo económico, las cuales tienen como finalidad definir una política general y vinculante a todas sus filiales dentro y fuera del territorio nacional para garantizar un nivel adecuado de protección

de datos personales de acuerdo con la Ley, su Reglamento las disposiciones aplicables del sector correspondiente y estos parámetros.

Políticas de privacidad

Artículo 16.- Son políticas de privacidad, las declaraciones unilaterales hechas por un responsable en las que se explicitan los fines, usos, manejo y obligaciones que éste asume en relación con los datos personales de sus clientes o usuarios, siempre que estos se apeguen a la Ley, el Reglamento, las disposiciones aplicables del sector y estos parámetros.

Otros mecanismos

Artículo 17.- En el caso de la adopción de esquemas de autorregulación no previstos expresamente en la Ley, su Reglamento o en estos parámetros, la Secretaría en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos Personales resolverá sobre su procedencia, siempre y cuando reúnan los requisitos generales previstos en los presentes estos parámetros.

Artículo 18.- Los responsables podrán incluir como otros mecanismos de autorregulación vinculante, contratos o cláusulas que celebren con sus clientes, proveedores o empleados donde consten los elementos mínimos previstos en el Reglamento y estos parámetros.

CAPITULO III
DEL CONTENIDO DE LOS ESQUEMAS DE AUTORREGULACIÓN

Contenido obligatorio

Artículo 19.- Los esquemas de autorregulación vinculante, para ser inscritospor la autoridad competente, deberán contener los requisitos a que se refiere el presente capítulo, la Ley y el Reglamento.

Tipo de esquema

Artículo 20. Se deberá especificar el tipo de esquema de autorregulación vinculante convenido, pudiendo consistir en códigos deontológicos, códigos de buena práctica profesional, sellos de confianza, políticas de privacidad, reglas de privacidad corporativa u otros que posibiliten a los titulares identificar a los responsables comprometidos con la protección de sus datos personales.

Ámbito de aplicación

Artículo 21.- Los esquemas de autorregulación vinculante deberán establecer con claridad su ámbito material de aplicación, las actividades a que se refiere y los tratamientos sometidos al mismo.

Artículo 22.- Los esquemas de autorregulación deberán establecer el ámbito personal de los mismos, los cuales podrán referirse a empleados, clientes, proveedores, usuarios o demás personas con los que los sujetos al esquema de autorregulación tengan algún vínculo referido a sus datos.

Artículo 23.- Los esquemas de autorregulación deberán hacer mención de las disposiciones legales, reglamentarias o administrativas que rijan el sector de que se trate, a fin de garantizar el principio de licitud en el tratamiento de los datos.

Artículo 24.- Los esquemas de autorregulación podrán estar dirigidos al correcto tratamiento de datos personales en posesión de particulares, que se refieran a:

a) Un tipo de información personal en específico.
b) Una actividad o clase de actividades específicas.
c) Un sector profesional, comercial o industrial específico.
d) Un sector que participe en actividades que impliquen flujo transfronterizo de datos.

Artículo 25.- Los esquemas de autorregulación podrán referirse a los tipos de soporte o medios en los que se contengan los datos personales en posesión de particulares:

a) En soporte físico.
b) En soporte electrónico.
c) En el entorno digital.
d) En soporte mixto.

Artículo 26.- Los esquemas de autorregulación podrán ser temporales, debiéndose indicar expresamente en el acto de notificación de los mismos ante el Instituto y las autoridades sectoriales, cuándo o bajo qué circunstancias dicho esquema dejará de tener efectos. Asimismo, deberán señalar los mecanismos por los cuales se comunicará a los interesados de la terminación del mismo.

Complementariedad

Artículo 27.- Los esquemas de autorregulación son complementarios y coadyuvantes de la protección que brinda la Ley, su Reglamento y las disposiciones aplicables del sector correspondiente. En ese sentido, en el tratamiento de los datos personales deberán prever disposiciones específicas por las cuales los miembros observen los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad a que se refiere el artículo 6 de la Ley.

Artículo 28.- Los esquemas deberán prever mecanismos que garanticen a los titulares de los datos, el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición , de acuerdo con la Ley y su Reglamento.

Artículo 29.- Los esquemas de autorregulación no podrán limitar el alcance de la Ley y el reglamento, ni limitar su responsabilidad frente a los derechos de sus usuarios.

Artículo 30.- Todo esquema de autorregulación deberá contemplar las medidas de seguridad físicas, administrativas o técnicas aplicables al sector y tipo de datos sujetos al mismo a que se refieren la Ley y el Reglamento.

Mecanismos para medir la eficacia del esquema adoptado

Artículo 31.- Los esquemas de autorregulación vinculante deberán establecer mecanismos por los cuales sean revisados sistemáticamente, los cuales evaluarán al menos:

a) Cumplimiento de las obligaciones asumidas por los obligados;

b) Funcionamiento de los procedimientos establecidos en el esquema;

c) Resumen de las evaluaciones de vigilancia realizadas durante el periodo revisado; y

d) Adecuación de las cláusulas a las actividades y circunstancias actuales de los sujetos obligados.

Artículo 32.- La revisión del mecanismo será efectuada por el administrador del esquema, el órgano designado para tal efecto o un tercero, siempre que garantice su imparcialidad e independencia frente a los adheridos.

Artículo 33.- El mecanismo de revisión previsto en el esquema de autorregulación deberá tener lugar al menos cada dos años, y antes de cada renovación de inscripción.

Artículo 34.- Todo proceso de revisión debe culminar con un reporte, donde se expresarán los resultados de la revisión, así como las recomendaciones necesarias a fin de hacer más eficiente y efectivo el cumplimiento del esquema.

Artículo 35.- La autoridad podrá efectuar verificaciones a fin de comprobar los resultados obtenidos en los reportes así como el cumplimiento de las recomendaciones efectuadas. El cumplimiento de las recomendaciones podrá ser tomado en consideración por la autoridad para la revocación de la inscripción del esquema de autorregulación.

Consecuencias y medidas correctivas en caso de incumplimiento

Artículo 36.- Para la debida observancia de sus disposiciones, los esquemas de autorregulación establecerán las sanciones que corresponda aplicar a los miembros que incumplan con los mismos.

Los órganos responsables de aplicar las sanciones deberán observar los principios de contradicción, audiencia, sencillez, accesibilidad, celeridad y gratuidad.

Artículo 37.- Las sanciones podrán consistir en amonestaciones, sanciones económicas, suspensión temporal o definitiva de adhesión al mecanismo.

La suspensión de derechos del miembro podrá incluir también la terminación de la licencia de uso de distintivo o marca que en su caso se otorgue a los adheridos.

Artículo 38.- Los esquemas de autorregulación vinculante podrán prever que las sanciones efectuadas se hagan públicas.

Artículo 39.- En todo caso, se establecerá una graduación de sanciones que permita su individualización de manera proporcional a la gravedad de la infracción.

Artículo 40.- Todas las sanciones deberán ser notificadas al afectado.

Identificación de los responsables

Artículo 41.- Los esquemas de autorregulación deberán expresar de manera clara el perfil de las personas que podrán adherirse a ellos, así como el procedimiento de adhesión.

Artículo 42.-. Los esquemas deberán prever mecanismos por los cuales se pueda identificar a sus miembros. Esto podrá realizarse a través de sellos, distintivos, certificados u otras marcas de carácter exclusivo. La pertenencia

a un esquema de autorregulación deberá publicarse en algún lugar de fácil acceso al público.

Artículo 43.- El administrador del esquema de autorregulación deberá mantener una lista actualizada de miembros a disposición de la autoridad.

Artículo 44.-. Tratándose de empresas que tengan diferentes filiales, el esquema deberá precisar las entidades de las mismas que estarán o no sujetas al mismo.

Sistemas de supervisión y vigilancia

Artículo 45.- Los esquemas de autorregulación vinculante deberán establecer procedimientos para llevar a cabo evaluaciones periódicas de supervisión y vigilancia, en intervalos que permitan llevar un seguimiento continuo del nivel de cumplimiento de las disposiciones del mismo.

Artículo 46.- Cuando se identifiquen no conformidades durante los procedimientos de supervisión y vigilancia, el administrador deberá requerir el cumplimiento en un tiempo límite, en cuyo defecto, impondrá la sanción que corresponda.

Artículo 47.- Los procedimientos de supervisión y vigilancia podrán estar a cargo del órgano de administración del esquema o de un tercero imparcial designado para tal efecto; sin perjuicio de que se opte por la certificación en los términos del artículo 83 del Reglamento y los artículos ___ de los presentes Parámetros.

Artículo 48.- En el caso de que los sistemas de supervisión y vigilancia sean llevados a cabo por segunda o tercera persona, el interesado deberá

presentar el contrato o convenio respectivo, al momento de la notificación del esquema.

Artículo 49.-. Los esquemas de autorregulación deberán contener criterios que permitan homologar y normalizar los resultados obtenidos por las personas físicas o morales que opten por su implementación respecto del tratamiento de datos personales que realicen, así como criterios de revisión que permitan evaluar su viabilidad o pertinencia como medida autorregulatoria.

Capacitación

Artículo 50.- Los esquemas de autorregulación deberán establecer programas de capacitación en materia de protección de datos personales que estarán disponibles para los adheridos u obligados por el mecanismo correspondiente.

Artículo 51.- Con la notificación del esquema de notificación de que se trate, se informará a las autoridades sectoriales competentes y al Instituto, el tipo de capacitación y si la misma se proveerá por terceros.

Medidas concretas tomadas respecto a la protección a categorías especiales de titulares (*menores, personas con discapacidad y personas que no hablen el idioma español*).

Artículo 52.- Los modelos de autorregulación vinculante deberán incluir medidas de protección reforzada si los datos fueren sensibles o los titulares de los datos se encuentran en una especial situación de vulnerabilidad. Dichas medidas deberán especificarse cuando exista la posibilidad de que los obligados al esquema de autorregulación traten con dichos datos.

Artículo 53.- En el caso de que los titulares de los datos sean menores de edad, deberá garantizarse que el responsable cuente con el consentimiento de quien ejerza la patria potestad o la representación legal del menor, siempre que se trate de la obtención, uso, modificación o transferencia de datos.

Artículo 54.- En caso de que los titulares no hablen el idioma español, deberá garantizarse que los responsables adopten las providencias necesarias para que aquellos conozcan sus derechos contenidos en la Ley, el Reglamento y el esquema de autorregulación.

Artículo 55.- Respecto a personas con discapacidad, deberán adoptarse las medidas necesarias para garantizar a estas el acceso y ejercicio de sus derechos. Ningún dato de personas con discapacidad podrá constituir alguna forma de discriminación.

Artículo 56.- El Instituto evaluará si el modelo requiere de medidas adicionales para otorgar una mayor protección a titulares de datos personales que se encuentren en una situación especial.

Transferencias nacionales e internacionales de datos personales

Artículo 57.- Los esquemas de autorregulación vinculante contendrán disposiciones dirigidas a garantizar el cumplimiento de las obligaciones a que se refieren los artículos 36 de la Ley, y 67 a 76 del Reglamento en relación con la transferencia de datos personales a terceros dentro y fuera del territorio nacional.

Artículo 58.- Las normas internas de protección a que se refiere el artículo 70 del Reglamento, así como las cláusulas contractuales del artículo 75, podrán constar en los esquemas de autorregulación vinculante a que se refieren estos parámetros.

Artículo 59.- Para su inscripción por parte del Instituto, los interesados deberán indicar en la notificación, además de lo previsto en el artículo _ de estos parámetros:

a) La forma en la que el receptor de los datos personales asume las mismas obligaciones que corresponden al responsable que transfirió los datos personales;

b) Mecanismo y condiciones en las que los titulares de los datos consienten el tratamiento de sus datos.

Artículo 60.- Para los efectos del artículo 37, fracción III, y 70 del Reglamento, si la transferencia internacional de datos personales tiene lugar entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, pero con establecimiento fuera del territorio nacional, deberá presentarse la documentación que acredite dicha relación.

Administración del esquema

Artículo 61. En el caso de los códigos deontológicos, códigos de buenas prácticas profesionales, sellos de confianza u otros análogos, los esquemas de autorregulación deberán contar con un administrador, cargo que podrá

recaer en un órgano individual o colegiado que garantice su imparcialidad y evite el conflicto de intereses.

Artículo 62.- La forma de designación del administrador deberá establecerse en el documento a que se refiere el artículo __ de estos parámetros.

Artículo 63.- El administrador tendrá la función de tramitar la admisión de nuevos miembros, elaborar los reportes a que se refieren estos parámetros, así como proporcionar la información y demás documentación que le sea requerida por la autoridad competente.

Procedimientos para la protección de los datos

Artículo 64.- Los esquemas de autorregulación podrán contar con procedimientos para atender las quejas que les sean sometidas en relación con el incumplimiento de sus obligados en el trato de los datos personales y en el respeto de los derechos de acceso, rectificación, oposición y cancelación de los titulares de los datos.

Para ello, deberán elaborar un procedimiento especial de tratamiento de quejas. Asimismo, deberá señalarse en la solicitud, al agente encargado para recibir las quejas y el tratamiento que se le dará a estas.

Artículo 65.- La presentación de una queja podrá dar lugar al inicio de un procedimiento de verificación, la cual, de ser necesario, podrá concluir con la sanción que corresponda de acuerdo con los principios a que se refieren los estos parámetros.

Artículo 66.- La resolución recaída a este procedimiento, se entenderá como la última respuesta del responsable, para efectos de lo dispuesto en el artículo 45 de la Ley.

Mecanismos alternativos de solución de controversias

Artículo 67.- Sin perjuicio de los artículos anteriores, el agente encargado del esquema de autorregulación podrá sugerir a las partes involucradas remitir el asunto a un mecanismo alternativo de solución de controversias, siempre que el titular de los datos y el responsable involucrado lo consientan.

Para los efectos del párrafo anterior, los esquemas de autorregulación vinculante podrán contar con mecanismos de solución de controversias como la conciliación o mediación; servicios que podrán prestar por sí o mediante la contratación de expertos independientes.

Artículo 68.- Los mecanismos alternativos de solución de controversias se regirán por acuerdo entre las partes, o en su defecto, por las leyes federales o locales aplicables en la materia. En todo caso, deberán establecer procedimientos que cumplan con los siguientes principios:

a) Accesibilidad: El mecanismo deberá ser accesible a los titulares de los datos, promoviendo el conocimiento sobre su existencia, su funcionamiento y reduciendo al máximo los costos.

b) Independencia: El mecanismo deberá garantizar la independencia del conciliador o mediador.

c) Imparcialidad: La decisión del conciliador o mediador, deberá fundarse en criterios objetivos, y ser debidamente fundada y motivada.

Artículo 69.- En todo caso, los procedimientos llevados a cabo bajo los mecanismos alternativos de solución de controversias, deberán observar los principios de contradicción y audiencia, a fin de garantizar los derechos de todas las partes de manera imparcial.

Las decisiones adoptadas en el mecanismo deberán ser notificadas a las partes.

Artículo 70.- En caso de no encontrar una solución al caso, independientemente de la sanción que conforme al mecanismo corresponda aplicar, el conciliador o mediador deberá remitir el asunto ante la autoridad competente para los efectos legales que correspondan.

En ningún caso, la presentación de una queja o sometimiento a un mecanismo alternativo de solución de controversias, impedirá al titular del ejercicio del derecho de iniciar las acciones legales que correspondan, incluyendo los procedimientos a que se refiere la Ley y su Reglamento.

CAPITULO IV
DE LA CERTIFICACIÓN

Objeto

Artículo 71.- Mediante la certificación en materia de protección de datos personales, las personas físicas y morales acreditadas como certificadores, evalúan la conformidad de las políticas, programas y procedimientos de privacidad, así como las medidas de seguridad adoptadas por los responsables y encargados que voluntariamente se sometan a su actuación, para el debido cumplimiento de la Ley, su Reglamento, y las disposiciones aplicables del sector que corresponda.

Características y funciones del organismo de acreditación.

Artículo 72.- Para operar como un organismo de acreditación en materia de protección de datos personales, el interesado deberá cumplir con los requisitos y seguir el procedimiento a que se refiere el Título Cuarto, Capítulo I de la Ley Federal sobre Metrología y Normalización y las disposiciones aplicables de su Reglamento, así como demostrar calidad técnica, honorabilidad y experiencia en el tratamiento de datos personales

Artículo 73.- Los organismos de acreditación tendrán las siguientes funciones:

I. Resolver las solicitudes de acreditación que le sean presentadas, emitir las acreditaciones y notificarlo al Instituto, a la Secretaría y a las dependencias del ramo que corresponda;
II. Realizar verificación de los datos que se refiere el artículo __ de estos parámetros;
III. Revisar periódicamente el cumplimiento de los acreditados de las condiciones y requisitos bajo los cuales les fue otorgada la acreditación;
IV. Renovar las acreditaciones cuando los interesados cumplan con lo dispuesto por estos parámetros;
V. Revocar las acreditaciones en los términos y condiciones a que se refieren estos parámetros; y
VI. Las demás que le otorguen las leyes y sus reglamentos.

Artículo 74.- Podrán solicitar la acreditación como certificadores, las personas físicas y morales que cuenten con domicilio en México.

En el caso de las personas morales, se requerirá además ser una sociedad debidamente constituida conforme a las leyes mexicanas, en cuyo objeto social se encuentre la prestación del servicio de certificación de acuerdo con la Ley y el Reglamento.

Solicitud

Artículo 75.- La solicitud de acreditación se realizará por escrito ante el organismo de acreditación, a la cual se deberá adjuntar lo siguiente:

a) Formato debidamente llenado en original y copia.

b) Documentación que acredite conocimientos y experiencia suficiente en materia de datos personales, así como en el área específica en la que desea prestar el servicio de certificación.

c) En el caso de las personas morales, se deberá presentar acta constitutiva original y copia para cotejo.

d) Manual de operaciones que contenga los procedimientos de evaluación, verificación y auditoría necesarios para otorgar y mantener un certificado.

e) Modelo de contrato de prestación de servicios de certificación en materia de protección de datos personales.

f) Modelo de certificado propuesto.

Ámbito de aplicación

Artículo 76.- El solicitante deberá especificar las actividades, áreas, productos o servicios, y tratamiento de datos personales sobre las que efectuarán certificaciones.

Independencia, objetividad y confidencialidad

Artículo 77.- Las personas que deseen ser acreditadas como certificadores en materia de protección de datos personales deberán demostrar su independencia, y en su caso, garantizar que su función de certificación se mantenga libre de cualquier interés o influencia que pudiera comprometer su juicio profesional, objetividad e integridad.

Artículo 78.- Para ello, el interesado podrá incluir en sus procedimientos mecanismos que permitan la inhibición del acreditado en un asunto particular que así lo requiera. Dicha inhibición será requerida siempre que el acreditado se encuentre relacionado con el responsable que solicita la certificación, de forma que pudiera comprometerse la objetividad del acreditado.

Artículo 79.- En todo caso, el acreditado deberá abstenerse de participar en un proceso de certificación, cuando éste tenga alguna forma de asociación con el interesado.

Artículo 80.- Los procedimientos y las políticas del acreditado no deben ser discriminatorios y deben ser administrados de una manera no discriminatoria.

Verificación de los datos

Artículo 81.- El organismo de acreditación, por sí o por medio de terceros, podrá practicar procedimientos de verificación a fin de comprobar la documentación presentada por el solicitante.

En este caso, las visitas deberán ser planeadas y notificadas previamente al solicitante, especificando la documentación, los procesos y demás información que vaya a ser verificada. Las visitas se restringirán únicamente al lugar en donde el solicitante pretenda prestar el servicio de certificación.

Artículo 82.- El organismo de acreditación podrá requerir información y documentación sobre cualquier situación relacionada con los procesos de certificación que lleve a cabo el acreditado.

Asimismo, el organismo podrá practicar procedimientos de verificación en cualquier momento para comprobar el funcionamiento a que se refiere el párrafo anterior.

Artículo 83.- En las revisiones que el organismo realice, elaborará un reporte que será comunicado al interesado al término de la visita en donde especificará los hallazgos encontrados, y en su caso, las recomendaciones que el acreditado deba realizar. Para ello, el organismo dará un tiempo límite en el cual el interesado deberá dar cumplimiento.

Vigencia y Renovación de la acreditación

Artículo 84.- Las acreditaciones otorgadas a una persona física o moral para prestar el servicio de certificación en materia de protección de datos personales, tendrá una vigencia de dos años.

Al término de la vigencia, el interesado deberá presentar la solicitud de renovación correspondiente ante el organismo de acreditación, el cuál evaluará la pertinencia de concederla de acuerdo con los procedimientos de verificación y auditoría que al efecto realice.

Revocación de la acreditación

Artículo 85.- Además de las causas señaladas en el artículo 76 del Reglamento de la Ley Federal sobre Metrología y Normalización, serán causas de revocación o cancelación de la acreditación las siguientes:

a) Exista falsedad en la información presentada en la solicitud o en los reportes posteriores;

b) No dar cumplimiento a las recomendaciones realizadas durante los procedimientos de verificación;

c) El Instituto haya sancionado de forma sistemática a los certificados por el acreditado; y

d) Otras causas graves señaladas por el Instituto y la Secretaría.

Procedimiento de Certificación

Artículo 86.- Para la prestación del servicio de certificación, el acreditado deberá elaborar un protocolo de evaluación de la conformidad de los responsables, el cual establecerá la forma en la que se evaluará el cumplimiento de cada uno de los principios de la ley y su reglamento, así

como el ejercicio de los derechos de acceso, rectificación, oposición y cancelación de los titulares de los datos.

Artículo 87.- El proceso de certificación incluirá:

a) Una evaluación inicial de la conformidad, que incluirá la verificación de los formatos de autoevaluación que al efecto sean completados por el solicitante, lo que podrá comprender entrevistas personales o telefónicas, inspecciones del sistema de datos personales, de las medidas de seguridad, evaluación de riesgos, y escaneos de los sitios webs y/o de las aplicaciones.

b) Elaboración de un reporte que destaque los hallazgos del acreditado en relación con el nivel de conformidad del solicitante, así como los cambios o adecuaciones que en su caso el solicitante deba realizar.

c) Verificación del cumplimiento de las recomendaciones expuestas en el reporte.

d) Certificación de las políticas de privacidad del solicitante de conformidad con la Ley, el Reglamento y los protocolos de actuación del acreditado.

Artículo 88.- El acreditado deberá contar con un protocolo que establezca los procedimientos de supervisión, vigilancia y auditoría, por los cuales efectué una revisión periódica de los certificados que otorgue.

Artículo 89.- Cuando el acreditado tenga conocimiento de que alguna práctica del responsable certificado pueda constituir un incumplimiento de la

ley o su reglamento, así como de su protocolo, éste deberá iniciar inmediatamente un proceso de revisión para verificar su conformidad. En caso de encontrar fallas o incumplimientos, el acreditado lo notificará al interesado a fin de que este haga las correcciones necesarias en un tiempo determinado. La falta de cumplimiento del responsable deberá dar lugar a la revocación del certificado por el acreditado.

Revocación de la certificación

Artículo 90.- El acreditado revocará los certificados en los siguientes casos:

a) Se encuentre que la documentación presentada por el interesado es falsa o ha cambiado sin haberlo notificado al acreditado.

b) Omita hacer las modificaciones que el acreditado haya recomendado para el debido tratamiento de los datos personales objeto de la certificación, siempre que estos ocasionen una violación grave a lo dispuesto por la Ley y su Reglamento.

CAPITULO V
DE LA NOTIFICACIÓN DE LOS ESQUEMAS DE AUTORREGULACIÓN

Artículo 91.- Los esquemas de autorregulación que convengan los particulares en términos del primer párrafo del artículo 44 de la Ley, serán notificados simultáneamente ante las autoridades sectoriales que correspondan y al Instituto.

Artículo 92.- La notificación de un esquema de autorregulación se hará por escrito, la cual deberá incluir:

I. Identificación de la o las personas, físicas o morales, de las organizaciones civiles o gubernamentales, nacionales o extranjeras, que hayan convenido el esquema de autorregulación;
II. El convenio o instrumento legal donde conste la adaptación del esquema de autorregulación;
III. Explicación del esquema de autorregulación y los alcances del mismo;
IV. Los ámbitos territorial, material, sectorial y personal de los esquemas de autorregulación a que se refieren los presentes Parámetros;
V. El alcance y vinculación internacional, considerando otros esquema de cooperación transfronteriza vinculante o no, que las autoridades establezcan para tales fines;
VI. En el caso de códigos deontológicos o políticas privacidad, deberán estar formulados en español con un lenguaje entendible y claro, evitando utilizar léxicos especializados o ambiguos;
VII. En el caso de sellos o marcas de confianza, se adjuntará las características técnicas de los mismos y los derechos de propiedad intelectual de los mismos;
VIII. Identificación de las personas o sectores que puedan verse afectados o tengan interés en el esquema propuesto, incluyendo consumidores, usuarios, empleados, proveedores o demás interesados;
IX. Identificación del o los administradores del esquema de autorregulación, así como de las personas o entidades que intervengan en el tratamiento de datos personales como encargados o terceros;
X. Información sobre las entidades de auditoría, verificación, certificación o acreditación que intervendrán en los procesos de evaluación de segunda o tercera parte en su caso;
XI. La medidas de seguridad administrativas, físicas o técnicas , así como los tipos de controles físicos, tecnológicos o procesales adecuados conforme el tipo de datos recolectados por la organización adherente;

XII. Si el esquema incluye la contratación de un tercero para el tratamiento de datos personales, el documento por el cual conste dicho acuerdo;

XIII. El esquema establecerá medios de comunicación efectivos y adecuados para garantizar que los titulares de los datos personales cuentan con información suficiente en relación al tipo de controles utilizados para resguardar sus datos; y

XIV. Los demás requisitos previstos en el artículo 82 del Reglamento y en los presentes Parámetros.

Artículo 93.- En casos de que el modelo de autorregulación sea representativo de una industria o sector, o que por su grado de especialización así lo requiera, a criterio de la Secretaría podrá ser sometido a consulta pública para hacer observaciones sobre la viabilidad del modelo.

CAPITULO VI
DEL REGISTRO

Artículo 94.-. Los esquemas de autorregulación notificados se inscribirán en el Registro de Esquemas de Autorregulación Vinculante de Protección de Datos Personales en Posesión de Particulares a cargo del Instituto, siempre que su reúnan los requisitos previstos en estos Parámetros y los que establezcan las Reglas para el Registro de Mecanismos y Medidas de Autorregulación en la materia.

Para los efectos de la notificación, se aplicará lo dispuesto en el artículo 17 de la Ley Federal del Procedimiento Administrativo.

TRANSITORIOS

PRIMERO.- El presente Acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. Para efectos de la implementación del presente Acuerdo, con base en el artículo 77 del Reglamento se establecerá la coordinación con las distintas dependencias de la Administración Pública Federal a convocatoria del titular de la Secretaría.

México, D.F., a ____ de Junio de 2012.- El Secretario de Economía, **Bruno Ferrari García de Alba**.- Rúbrica.

RESUMEN EJECUTIVO

Conclusiones y Propuestas

Como corolario del **ESTUDIO DE AUTORREGULACIÓN EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO DE LAS TI** que se relaciona con las facultades de la Secretaría de Economía (SE) de México de acuerdo con el artículo 43 fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) para emitir parámetros -en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos (IFAIPD)- para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 del propio ordenamiento, este resumen ejecutivo contiene lo más relevante del estudio, así como conclusiones y propuestas que respetuosamente se permite formular la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (**CANIETI**).

1). Conceptos generales. Un primer apartado sustancial que la "coadyuvancia" SE-IFAIPD debe comprender en la elaboración de uno (o varios parámetros) sobre autorregulación en el ámbito de la protección de datos personales, es el consenso sobre la definición de la variada gama de conceptos que se involucran en el mundo digital universal y, en particular, para las Tecnologías de la Información en México.

En una era en la que el concepto de gobernanza regulatoria tiene un amplio sentido, "reglar la autorregulación" amerita que la terminología sea considerada un elemento indispensable de los parámetros y para ello se ensayan algunas definiciones de orden general sobre autorregulación, parámetros, y sobre lo que se debe entender por cada esquema, toda vez la LFPDPPP los menciona como alternativas (código deontológico, código de buenas prácticas profesionales, sellos de confianza, políticas de privacidad,

reglas de privacidad corporativas,; y otros mecanismos, que incluyan reglas o estándares específicos, así como el tema de la certificación de los responsables), que en nuestra propuesta de parámetros se definen.

2). Concepto de parámetro. En este estudio se ha ensayado una noción de parámetro. Para tal fin se le entiende como el conjunto de normas, estándares o factores de carácter general determinados por la Secretaría de Economía, en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos, que sirven de referencia para determinar o valorar la pertinencia y correcto desarrollo de los mecanismos y medidas de autorregulación vinculante en materia de protección de datos personales en posesión de particulares adoptados por los responsables y encargados con el fin de complementar lo dispuesto por la Ley Federal de Protección de Datos personales en Posesión de los Particulares, su Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones.

Dichas normas deberán establecer requisitos, reglas o estándares específicos para el correcto desarrollo de códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas, certificación de los responsables en materia de protección de datos personales u otros mecanismos.

Toda vez que un parámetro expedido por SE-IFAIPD será general, la Ley Federal del Procedimiento Administrativo abre la posibilidad de inscribirlo en las disposiciones “análogas”. Por tanto, deberán publicarse en el Diario Oficial de la Federación y someterse a procesos de validación ante la Comisión Federal de Mejora Regulatoria (COFEMER).

3). Concepto de Tecnologías de la Información. Como Sector de las TI, se propone concebir como el conjunto de industrias y/o empresas cuya actividad económica principal consiste en el diseño, desarrollo, producción, explotación, mantenimiento y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos, custodia y administración de información, así como aquellas unidades económicas vinculadas al desarrollo del software y hardware, los servicios de TI, Business Process Outsourcing (BPO), los medios creativos digitales, redes, aplicaciones o cualquier otra tecnología de la información que permiten el intercambio, almacenamiento y/o procesamiento informatizado o por medios físicos de datos.

4). Clases de Autorregulación. En el derecho comparado existen cuatro clases de autorregulación: 1. Autorregulación vinculante: en la que una organización o grupo de sujetos privados es designado para dictar y aplicar normas dentro de un grupo generalmente establecido directamente por los poderes públicos (*mandated self - regulation*); 2. Autorregulación aprobada: en la que los estándares son elaborados por sus destinatarios, y adoptados finalmente por los poderes públicos (*sancionated self - regulation*); 3. Autorregulación compelida: se caracteriza porque los estándares son adoptados de manera autónoma ante la amenaza de una eventual intervención normativa pública (*coerced self - regulation*); y 4. Autorregulación voluntaria: no hay intervención pública dirigida a imponer o fomentar, directa o indirectamente, la autorregulación (*voluntary self - regulation*).

En relación con el tratamiento de datos personales y los mecanismos o esquemas de autorregulación, de lo investigado se observa que existen -al menos- tres modelos normativos que los diferentes países han adoptado:

sistemas de heterorregulación, autorregulación pura y autorregulación integrada o mixta.

5). Experiencias de los Modelos de Autorregulación. Aunque hay países, como Estados Unidos, donde opera la autorregulación pura (no vinculante), es decir, sin intervención de la autoridad, existe heterorregulación de protección de datos personales en posesión de particulares en materia de telecomunicaciones e información genética en el ámbito laboral. Además por su carácter federal existen diversas leyes locales que eventualmente abordan la temática.

La tendencia de la autorregulación pura tiende a ser reemplazada por una mayor injerencia de la autoridad, ya que no cubre las expectativas de la autoridad ni de los consumidores. Por ello, la Casa Blanca emitió recientemente un estudio llamado “Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy”. Éste incluye el Consumer Privacy Bill of Rights, que son principios para proteger los datos personales y tienen por objetivo pasar al Congreso para ser ley, o bien servir de base para crear códigos de conducta consolidados por medio de consultas públicas acorde con el Consumer Privacy Bill of Rights.

En Estados Unidos se ha puesto énfasis en la educación de los usuarios con la difusión de diversos materiales en los que se den a conocer sus derechos de privacidad.

Los análisis coinciden respecto a ampliar las facultades de la FTC para aprobar Códigos de Conducta, otorgar sellos de confianza (safe harbor) y promover modelos de autorregulación en los que haya consulta pública.

Los avisos de privacidad han tenido poca efectividad para los consumidores, ya que son complejos y poco prácticos, por lo que la tendencia es homogeneizar prácticas en materia de protección de datos personales.

El uso de las nuevas tecnologías ha obligado a ampliar los conceptos para otorgar mayor protección a los consumidores, por lo que un modelo flexible como el norteamericano ha sorteado con rapidez los problemas no contemplados.

Es de destacar el esfuerzo de la FTC en proteger a más grupos de consumidores como a la comunidad de habla hispana en Estados Unidos con la emisión de informes y prestar ayuda en español. El modelo de protección de datos de menores de edad es insuficiente por solo contemplar a niños menores de 13 años, sin embargo, para el rango de 13 a 17 es necesario crear un marco *ad hoc* que no interfiera con su libertad de expresión y su desarrollo personal. Tener muchos requisitos para ser una empresa certificadora para protección de menores ha llevado a que solo 5 empresas tengan la autorización de la autoridad.

El sello de confianza otorgado por el Departamento de Comercio ha sido un éxito por el número de empresas que lo tienen, sin embargo solo tiene vigencia de un año, por lo que ha habido casos de varias empresas que no renuevan el sello.

El Código Modelo para la Protección de Datos Personales de Canadá, propuesto conforme a los principios establecidos por los estándares nacionales, podrá ser tomado como referencia por las organizaciones para crear y operar sus propios Códigos de Protección de Datos Personales

(*Code for the Protection of Personal Information*), con los mínimos señalados en el código modelo.

La primera problemática que enfrentaron las autoridades canadienses en la implementación del Personal Information and Electronic Documents Act (PIPEDA), fue la de limitar el ámbito de aplicación de la ley, surgiendo la interrogante sobre cuáles serían los datos personales que estarían en el ámbito de protección de la ley, diferenciando la información personal de la actividad comercial. A tal efecto se ha expandido la protección a las fotografías, la dirección de correo electrónico para negocios, el número de identificación ligado a un empleado, y la dirección IP (computer Internet Protocol).

Por lo que hace a México, se debe resaltar que el 22 de Febrero del presente año 2012, la Misión Permanente de México ante la Organización de los Estados Americanos (OEA) envió a la OEA las respuestas a un cuestionario sobre legislación y prácticas de privacidad y protección de datos “para recabar insumos que contribuyan al cumplimiento de los mandatos contemplados en la Resolución AG/RES. 2661 (XLI-O11) del 6 de Octubre de 2011”, y reconoció que solamente existen los modelos de autorregulación en materia de datos personales, el sello de confianza AMIPCI, el Código de Ética de BBVA Bancomer y el Código de Conducta del grupo farmacéutico NOVARTIS.

Es aconsejable tomar en consideración que en México existen modelos de autorregulación vinculante en el mundo financiero, bancario y de valores, cuyas leyes especiales reconocen el establecimiento de “organismos autorregulatorios” que pueden servir de ejemplo en materia de protección de datos personales.

6). El Modelo Mixto o Integrado de la Autorregulación en Materia de Datos Personales. Dentro de un tercer grupo de esquemas de autorregulación, se observa una clara tendencia de los países hacia un modelo, el cual comprende una legislación sobre protección de datos personales que incluye modelos de autorregulación (*modelo mixto o integrado*). México se encuentra dentro de esta categoría y con un enfoque similar se encuentra en Alemania, Argentina, Australia, Chipre, España, Grecia, Irlanda, Italia, Japón, Luxemburgo, Perú, Uruguay y la UE.

7). Los Códigos Deontológicos. El derecho comparado muestra que los códigos de privacidad son el mecanismo de autorregulación más usual previsto hasta ahora en las legislaciones. Reciben diferentes denominaciones (códigos de buenas prácticas, códigos de conducta, códigos deontológicos, códigos tipo, etc.) y prácticamente todos hacen referencia a normas de comportamiento adoptadas por los propios destinatarios de sus previsiones, ya sea sectores empresariales, asociaciones gremiales o profesionales. Los hay señalados en la Ley y los elaborados por las propias empresas, las asociaciones representativas o la industria.

Como se anotó en este trabajo, en muchos casos no son claros los efectos jurídicos que las legislaciones otorgan a estos códigos, o cuáles son los incentivos para adoptarlos, ya que la mayoría de las legislaciones se limita a señalar que estos serán “inscritos” o “registrados” ante la autoridad correspondiente. La reducción de multas en México o los incentivos reputacionales, deben ser promovidos para motivar su práctica.

En este documento se destacan las principales características de los códigos: representatividad, complementariedad, publicidad y registro, revisión, revocación, contenido, evaluación, temporalidad y alcance, y costos

de formulación y adopción, con la idea de integrarse a un futuro parámetro institucional en la materia.

En el ámbito europeo (UE, España y Reino Unido), los sistemas de autorregulación analizados presentan bajos niveles de participación. No se percibe que la autorregulación constituya un medio atractivo para impulsar la protección de datos personales. En general, se advierte que el cumplimiento de las disposiciones legales vigentes es suficiente y que medidas adicionales como la autorregulación no brindan un valor añadido a los responsables.

Esta percepción, sin duda, tiene origen en la inexistencia de medidas impulsadas por las autoridades nacionales que fomenten la autorregulación como una práctica con valor añadido.

Ninguna de las legislaciones analizadas contempla ni promueve la adopción, uso y divulgación de un sello o distintivo de confianza, en materia de protección de datos personales.

Del mismo modo, no se detectaron acciones o medidas tendentes a dotar de valor a la adopción de códigos de conducta, ni de información que distinguiera positivamente a las empresas que los adopten de otras que no lo hubieren hecho.

En España, a pesar de mostrar una participación baja, existe un aspecto favorable que debe tomarse en consideración: la adopción de códigos de conducta por parte de asociaciones o grupos de empresa que aglomeran a responsables de tamaño pequeño o mediano. Por lo tanto, la participación se realiza a través de representantes colectivos.

Otro aspecto positivo que puede rescatarse del caso español es el (relativamente) alto grado de participación de responsables que tratan datos personales considerados sensibles. Se trata de agrupaciones que han demostrado interés para dejar constancia que llevan a cabo un tratamiento adecuado de este tipo de datos.

El único código de conducta relevante que promueve el uso de un sello de confianza entre sus miembros los constituye “Confianza Online”. Este distintivo está dirigido a los prestadores de servicios de la sociedad de la información, y abarca aspectos adicionales a la mera protección de datos personales: protección el consumidor, publicidad online y protección de menores de edad.

En cuanto a los códigos de conducta institucionales, es decir, aquellos diseñados y promovidos por una autoridad nacional, los que han sido emitidos por la ICO inglesa representan ejemplos notables en cuanto a los segmentos o principios que abordan. No obstante, se reitera que estos códigos no abordan todos los aspectos regulados por la normativa de protección de datos personales, ni están dirigidos a todos los sectores que en su actividad cotidiana tratan datos personales.

El caso del Reino Unido es significativo en cuanto a su nivel de participación, pues a pesar de que su sistema permite tanto la adopción de oficio como la elaboración de códigos por parte de la autoridad, únicamente se identifica un código de conducta adoptado de oficio; el resto está constituido por los códigos que han sido analizados e identificados en el estudio.

La situación del Reino Unido se repite a nivel de la Unión Europea, en donde al día de hoy solo puede darse cuenta de un código de conducta en materia

de protección de datos personales que tenga un ámbito de validez comunitario.

El caso de los códigos comunitarios debe ser valorado con cuidado, pues se trata de códigos que deben cumplir con los principios establecidos en la Directiva de Protección de Datos Personales y, además, estar conformes con la normativa nacional de los 27 países que integran en Mercado Común. Por consiguiente, el código de conducta de la FEDMA merece un análisis particular al tratarse del único código que ha conseguido la aprobación del Grupo de Trabajo del Artículo 29 en la Unión Europea.

8). Sellos, Marcas o Distintivos de Confianza. De la revisión hecha hasta ahora, se observa que actualmente existen pocos mecanismos de certificación que se asemejen al enfoque que pretende adoptarse en México. Si bien existen los denominados "Sellos de Confianza" (en realidad uno solo, el de la AMIPCI) estos han sido, en su mayoría, elaborados por entidades (empresas, asociaciones, etc.) privadas de acuerdo con estándares propios.

Sobre el tema es recomendable el estudio que realizó el Proyecto i+Confianza en el año 2002[280] para comparar 19 marcas o sellos de confianza: L@belsite (Francia), Trusted Shops (Alemania), Comercio Certificado (Argentina), e-com-quality mark (Italia), DIN Tested Website (Alemania), Qweb (Italia), Trust-e (Estados Unidos), Squaretrade (Estados Unidos), Webassured (Estados Unidos), Consumer Trust (Singapur), Health On the Net (Suiza), BBBOnline Reliability (Estados Unidos), BBBOnline Privacy (Estados Unidos), Confiar-e (Chile), [G] Garantía de Protección de

[280] i+Confianza es un proyecto promovido por: Asociación Española de Normalización y Certificación (AENOR), Asociación Española para el Derecho y la Economía Digital (AEDED). Real e Ilustre Colegio de Abogados de Zaragoza (REICAZ) Fundació Catalana per a la Recerca (FCR) El documento producido por ese proyecto se denomina "Libro Blanco sobre los Sistemas de Autorregulación, los Sellos de Confianza en Mercados Digitales y Códigos de Buenas Prácticas". AENOR, España, Diciembre 2002.

Datos (España), AGACE (España), Bureau Veritas Web Value (Francia), IQA (España); y Marca AENOR de Buenas Prácticas Comerciales (España)

De estos sellos, subsiste la mitad: Trusted Shop, Qweb, Trust-e, Web Assured, Hon Code, Confiar-e, [G] ahora como Confianza Online, AGACE y AENOR. BBBOnline Reliability y BBBOnline Privacy se fusionaron en Better Business Bureau, que tiene el "Business Seal for the Web"[281].

En otro orden de ideas, en países de modelos de autorregulación pura, como es el caso de Estados Unidos, cobran especial relevancia sellos de confianza, muchos de ellos con efectos multinacionales, como Trust-e, Business Seal for the Web (del Better Business Bureau), VeriSign, Mc Afee, Webassured, ESRB Privacy Online Children's Certification Seal, Privo's Seal of Approval, etc. los cuales contienen especificaciones especiales.

Debido a que entre estas marcas existe competencia, sus propuestas comerciales para colocar los sellos de confianza ha implicado la exposición de las ventajas y desventajas que tiene cada uno de ellos. Así es que Trust-e se autocalifica como el sello de privacidad por excelencia, y afirma que VeriSign Trust Seal, McAfee Secure Trustmark, Comodo HackerProof Seal o el GeoTrust SSL Certificates son sellos para garantizar seguridad; y que los otros son sellos que solo garantizan buenas prácticas comerciales, tales como BBB Accredited Business Seal, buySAFE Seal, Bizrate Customer Certified Seal o el Shopping.com's Trusted Store Seal. Lo importante de ellos es que participan como agentes certificadores del Safe Harbor Privacy Principle y pueden ser considerados como relevantes en la construcción de los modelos mexicanos.

[281] Wwww.bbb.org/us/bbb.online-business/

Para el Departamento de Comercio de Estados Unidos el sello de confianza otorgado para el flujo transfronterizo de datos entre Estados Unidos y la Unión Europea ha sido efectivo, ya que las personas que cuentan con esta certificación suelen cumplirlo, lo que no impide a la autoridad de iniciar un proceso en contra por violentar el modelo. Sin embargo, una problemática a la que se ha enfrentado la autoridad de Estados Unidos es el engaño de las empresas, ya que sólo dura un año la vigencia del sello y éstas siguen utilizándolo luego de que expira. Quizás por eso la UE y la APEC inclusive estén considerando que la tendencia de la autorregulación pura sea reemplazada por una mayor injerencia de la autoridad, ya que no cubre las expectativas de la autoridad ni de los consumidores.

En la línea de espera sigue el proyecto del 2008 del "Proyecto Piloto de Sello de Confianza Regional, así como las propuestas de la Red Iberoamericana de Protección de Datos.

Es importante señalar que los Sellos o Marcas de Confianza generalmente son distintivos que se otorgan cuando los responsables han pasado por un proceso de adhesión a un código deontológico o de buenas prácticas y/o a esquemas de certificación (verificación, auditoría, etc.) previos. Si se toman como referencia los sellos European Privacy Seal (EuroPriSe) y el Privacy Mark (Japón), no queda duda que la certificación es esencial para emitir un sello. Asimismo si se revisan las nuevas propuestas de APEC y la Comisión Europea comentadas anteriormente, la tendencia es hacia un esquema de autorregulación basado en la certificación.

Aunque en Europa existen importantes sellos o marcas de confianza, o bien, códigos de buenas prácticas, tales como los reconocidos en Alemania (Trusted Shops), Francia (Bureau Veritas Web Value), Italia (e-com-quality mark) o Suiza (Hon Code) en este proyecto se han considerado

preliminarmente los basados en las directivas de la Unión Europea, ATA o APEC.

9). Certificación. Como se comenta en este trabajo, el tema de la certificación se fundamenta actualmente en la Ley Federal sobre Metrología y Normalización, y la entiende como el procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacionales o internacionales.

Dentro de los esquemas de la Evaluación de la Conformidad, la certificación sirve para determinar el grado de cumplimiento con las normas oficiales mexicanas o la conformidad con las normas mexicanas, las normas internacionales u otras especificaciones, prescripciones o características. Un primer análisis de estas disposiciones indica que la aplicabilidad de las nociones de certificación (y de acreditación inclusive) se enfoca en procedimientos y métodos establecidos en las NOM y/o en su defecto a las normas internacionales; por lo que se podría deducir apriorísticamente que no son aplicables al ámbito de los parámetros.

Una primera interpretación indica que los Parámetros no pueden exceder los alcances de la Ley de Metrología y Normalización, ni mucho menos de su Reglamento, donde su artículo 71 contempla los requisitos para operar una entidad de acreditación. Es decir, con un espíritu crítico o un juicio muy estricto, un parámetro –de rango inferior a un Reglamento- no podría crear nuevas reglas de acreditación/certificación, salvo que se “convenga” que esos conceptos tienen otro sentido en materia de protección de datos personales.

Con un espíritu propositivo, la acreditación a que se refiere el Reglamento de la LFPDPPP podría definirse con un sentido práctico para estimular la adopción de esquemas de autorregulación, sobre todo si se toma en cuenta que finalmente la autorregulación es voluntaria y que el IFAIPD no pierde –en ningún momento- sus facultades para verificar que los responsables cumplen con la ley y sus principios en materia de protección de datos personales.

Un parámetro sobre autorregulación que incluya la acreditación/certificación debe ponderar los impactos que tendría desde un punto de vista "motivacional" si se crean nuevas obligaciones; se hacen más estrictas las obligaciones existentes; si crea o modifica trámites; si afecta derechos o prestaciones para los particulares; y si establece definiciones, clasificaciones, que conjuntamente con otra disposición afecten o puedan afectar los derechos, obligaciones, prestaciones o trámites de los particulares.

No obstante el valor comercial, reputacional y de fomento a la calidad de estos esquemas, se debe atender de manera muy seria lo relativo al costo-beneficio para los organismos mexicanos que pretendan ser acreditados como certificadores en materia de protección de datos personales, pues los documentos revisados hasta ahora (internacionales o nacionales) exigen una amplia cantidad de requisitos cuantitativos y cualitativos.

Se debe estar atento al hecho de que la Comisión Europea recientemente dijo que examinará la posibilidad de crear regímenes europeos de certificación para los procesos, tecnologías, productos y servicios que sean conformes a las normas de protección de la intimidad.

Para este trabajo han resultado relevantes los sistemas de certificación en materia de privacidad con los que cuentan el European Privacy Seal y el Privacy Mark en Japón, así como el de APEC, cuyas normatividades se explican en su integridad.

10).- Ventajas de la Autorregulación en Materia de Datos Personales. Con la idea de exponer las ventajas que tienen los modelos de autorregulación en el campo de la protección de datos personales, en este estudio se analizaron las más relevantes, tanto para la industria, la autoridad y sobre todo, los titulares de los datos personales:

Prevención:

- El establecimiento de esquemas o modelos de autorregulación tienen una función eminentemente preventiva, ya que permitirá mitigar o en su caso establecer mecanismos para mediar entre las partes y que los daños o perjuicios que determinadas acciones puedan causar sean resueltas en un ambiente de particulares.

Solución de controversias:

- Permite el establecimiento de formas de mediación o resolución de controversias a través de procedimientos *ad hoc* para cada sector y atendiendo las necesidades propias de una industria o iniciativa privada.

- A través de mecanismos de solución de controversias que son propuestos por la autorregulación se pueden prever procedimientos que resulten eficaces, pero sobre todo que el tiempo de atención y resolución sea corto.

- Los procedimientos que se establecen en los mecanismos de autorregulación para la solución de controversias podrían resultar de

menor costo, que de aquellos procedimientos en los que tiene intervención la autoridad.

- Los modelos de autorregulación permitirán que la intervención de la autoridad en la solución de conflictos sea menos frecuente, lo que permitirá que las cargas de trabajo de las autoridades no se dispare.

- La autorregulación tiene más ventajas cuando contiene soluciones alternativas de conflictos, que no limitan ni excluyen el derecho de los titulares de datos personales para acudir a las vías legalmente establecidas para resolver cualquier inconformidad derivada del tratamiento de sus datos personales o de la atención a sus solicitudes de ejercicio de los derechos ARCO.

- Los esquemas de mediación y resolución de controversias que aportan la mayoría de las organizaciones promotoras de la autorregulación, podrían ser consideradas como parte del servicio que presten los agentes responsables y las organizaciones certificadoras.

Consideraciones reputacionales:

- Se considera que la adopción de un mecanismo de autorregulación contribuye en buena medida al capital de imagen, ya que los usuarios, adherentes, etcétera, proyectarán una imagen de responsabilidad y respeto a la protección de los datos personales.

- Con la proyección de compromiso y responsabilidad en la protección de datos personales, las personas físicas o morales que adopten algún modelo de autorregulación lograrán en cierta medida establecer una relación de confianza con sus clientes o usuarios.

Beneficios económicos y competitivos:

- La adopción de mecanismos de autorregulación no solo representará beneficios a los usuarios, clientes o adherentes; ya que para las personas físicas o morales que los adopten representará beneficios económicos pues tendrán más posibilidades de establecer relaciones comerciales a nivel internacional.

- Uno de los requerimientos para que la autorregulación sea efectiva redundará en beneficios para las partes, por un lado promoverá la sana competencia y por otro, requerirá de brindar más información al consumidor.

- Uno de los insumos de la economía digital son los datos personales de usuarios, clientes o adherentes, por lo que la adopción de mejores prácticas en temas de privacidad, permitirá el sano desarrollo de la economía nacional en su conjunto.

- Es muy útil para el desarrollo económico integrar al régimen jurídico aquellas normas que de facto son necesarias para organizar y pactar buenas prácticas a través de códigos deontológicos, sin tener que pasar por todo el proceso legislativo, en tanto se da la coexistencia y complementariedad de los marcos normativos.

- Los mecanismos de autorregulación deben servir para auxiliar a las autoridades competentes para llevar a cabo su función de protección de la privacidad, así como acercar mecanismos internacionales para promover y hacer cumplir la protección de la privacidad, así como para mantener el flujo continuo de la información entre las Economías y con sus socios comerciales.

- Los sellos de confianza han logrado que un amplio conjunto de usuarios hayan creado confianza y aumentado la participación a través de todos sus canales en línea, incluyendo sitios web, aplicaciones móviles, publicidad, servicios de nube, análisis de negocio y marketing por correo electrónico.

- Para incrementar la interoperabilidad (jurídica) global entre países a través del desarrollo de modelos de privacidad con un proceso de consulta, y reforzando la cooperación para eliminar las barreras para el intercambio de datos. Las empresas que realizan flujo transfronterizo de datos deben enfrentarse al cumplimiento de múltiples jurisdicciones, ya que existe poca armonía entre las leyes extranjeras.

- La adopción de códigos de conducta puede constituir un elemento distintivo para aumentar la competitividad del sector TI frente a otras opciones del mercado, ya que actores de este sector que prestan servicios como alojamiento (hosting) o atención al cliente (call centers) son altamente requeridos por empresas europeas.

Privacidad a la medida:

- Una ventaja importante de los modelos de autorregulación es que, para su adecuación a la realidad o necesidades de un sector, industria o empresas no es necesario seguir un procedimiento complejo (como es el caso del ámbito normativo), resultando procesos ágiles.

- La autorregulación permitirá la aplicación de exigencias legales de forma sencilla y atendiendo necesidades y realidades de los diferentes modelos de negocios existentes en el ámbito digital.

- Es de gran ventaja la flexibilidad con la que se pueden adaptar los mecanismos de autorregulación a los cambios tecnológicos que son adoptados por los distintos sectores.

- A través de la autorregulación se permite regular “temas” muy específicos y complejos, como es el caso de la protección de datos personales de menores.

- Entre las ventajas de la autorregulación se encuentra que se promueve la autonomía privada de la voluntad; entendiéndose este concepto como el principio jurídico-filosófico que les atribuye a los individuos un ámbito de libertad, dentro del cual pueden regular sus propios intereses; permitiéndoles crear relaciones obligatorias entre ellos, que deberán ser reconocidas y sancionadas en las normas de derecho.

- Diversos investigadores mencionan las ventajas de la autorregulación sobre la regulación estatal para Internet, enunciando que estas son su mayor prontitud, flexibilidad y eficacia; el aprovechamiento de la experiencia acumulada de la industria; y que los recursos gubernamentales son limitados. La autorregulación permite que – si existe voluntad-, se implemente regulación más eficaz, provista de mecanismos de sanción dentro del ámbito privado.

- Los mecanismos de certificación en materia de protección de datos contribuyen a la correcta aplicación de las leyes o reglamentos sobre protección de datos personales, teniendo en cuenta las características específicas de los distintos sectores y las diferentes operaciones de tratamiento.

- Los códigos de ética tienen como consecuencia, por lo general, una mínima carga jurídica en comparación a la ley. Se inclinan a ser solo simples recomendaciones y no contienen mecanismos limitantes.

- Para que sean ventajosos los esquemas de autorregulación se requiere que dispongan de herramientas que los hagan eficaces. Dentro de estos mecanismos se han sugerido:

  (1) Establecer medios ágiles, efectivos y gratuitos en caso de inobservancia del código para que la persona no solo exija el respeto de sus derechos y libertades sino que se convierta en un "fiscalizador" de la gestión del administrador de sus datos personales,
  (2) Consagrar mecanismos de control interno y externo de verificación del cumplimiento de los códigos, y
  (3) Prever sanciones por el incumplimiento de los códigos.

Complementariedad:

- Los mecanismos de autorregulación tienen por objeto complementar y hacer efectiva la aplicación de la ley. En algunos casos como se ha visto en el estudio, tienden a sustituir la normatividad.

- La autorregulación es una manera de promover las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

- Los códigos de conducta elaborados por organizaciones sectoriales comerciales y profesionales han sido definidos como "un puente" entre las reglas sustantivas de las leyes de protección de datos y su instrumentación a nivel operativo.

- El éxito del modelo de corregulación depende en gran medida de la oportunidad que se brinde al público y a los principales interesados, de comentar y examinar la propuesta de Código de Privacidad, máxime cuando éstos tienen por objeto sustituir la protección que brinda la ley.

- Para los Estados miembros de la Unión Europea es importante alentar 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 sus directivas.

- Para la legislación mexicana, la autorregulación en materia de protección de datos personales tiene como finalidad complementar la legalidad, con lo que se quiere decir que los esquemas que se adopten servirán para organizar y pactar buenas prácticas a través de códigos deontológicos, sin tener que pasar por todo el proceso legislativo, en tanto se da la coexistencia y complementariedad de los marcos normativos.

- Para la sociedad mexicana representa una oportunidad valiosa de ahondar en el uso de buenas prácticas en acatamiento del principio de responsabilidad, uno de los ocho ejes de observancia ineludible en materia de privacidad.

- Aunque no ha demostrado ser un modelo con alta participación, la autorregulación debe seguir considerándose una alternativa para promover mejores prácticas en materia de protección de datos personales.

Confianza:

- Los modelos de autorregulación pueden ser la vía que permita el desarrollo del comercio electrónico, permitiendo crear una ambiente de confianza entre los usuarios y los responsables, pues con la adopción de los mecanismos se mostrará el compromiso y responsabilidad en la protección de datos personales.

- Para los usuarios tiene como ventaja observar cuáles empresas se encuentran adheridas al mecanismo de autorregulación que mejor atienda a sus necesidades.

- Con la autorregulación se alientan mecanismos que eliminan el mayor número posible de obstáculos al desarrollo del comercio electrónico, tales como la desconfianza de los consumidores en las páginas web que ofrecen productos o servicios.

- En el ciberespacio, el objetivo central de la autorregulación es generar confianza en la interacción de los usuarios de Internet; y en este sentido se busca equiparar las acciones y las gestiones en un marco ético para mejorar la calidad de un servicio en el mundo del Internet.

- Con el marco de trabajo adecuado, las verificaciones, los balances, la vigilancia y los controles, la autorregulación es -con mucho- una ruta más atractiva que la promulgación de leyes por el gobierno central.

- Los códigos de privacidad otorgan cierta flexibilidad a las organizaciones en el cumplimiento de sus obligaciones. Fue ideado como un mecanismo para favorecer la seguridad y la confianza de los consumidores y usuarios ya que permite a la industria y a sus clientes elaborar un marco de protección que se ajuste a sus necesidades.

- En un gran número de países es importante el establecimiento de parámetros, prácticas y sellos de confianza para los negocios por Internet, a fin de ampliar la confianza del público en las empresas que realicen comercio electrónico y cuenten con alguno o todos los sellos adheridos a su Programa que posee tres sellos de confianza para los sitios en Internet.

- La representatividad de los mecanismos de autorregulación es un elemento que puede resultar fundamental para la certeza y operatividad de los códigos, toda vez que ayuda a reducir el grado de confusión en que puede caer un consumidor o usuario frente a un sector o industria fragmentada.

Beneficios sociales:

- Los medios de comunicación masiva como la radio, la televisión, la prensa escrita, la publicidad e Internet, ya cuentan con mecanismos de autorregulación, muchas veces relacionados con la metodología y la selección de determinados contenidos que puedan afectar severamente a la sociedad, o bien, con prácticas comerciales.

- Siguiendo a Frank Kuitenbrouwer señala que la autorregulación puede servir para varios fines en relación con el proceso legislativo: La autorregulación puede tener la intención de evitar la legislación; la autorregulación puede ser usada para anticipar la legislación; la autorregulación puede servir para instrumentar la legislación; y la autorregulación también puede complementar la legislación.

- La autorregulación permite compensar insuficiencias y limitaciones, favoreciendo así que las actividades objeto de la misma se ajusten a sus propios valores y normas: De ahí que se considere un complemento adecuado de la regulación, principalmente en sectores de especial conflictividad respecto de derechos fundamentales.

- Cada ámbito del ciberespacio es factible de regularse con el propósito de otorgar confianza a los usuarios. Los esfuerzos para regular el Internet, principalmente en el campo del comercio electrónico son, en primer lugar, justificables como una alternativa ante la sociedad de la información que

carece de límites territoriales y por lo tanto jurídicos, pero la autorregulación es un instrumento idóneo para contribuir a que las estructuras de gobierno puedan atender y resolver las problemáticas derivadas del Internet.

- Para la APEC cualquier esquema de protección que se adopte, ya sea legislativo, autorregulación, o de cualquier otra índole, debería prevenir el mal uso de la información personal y el daño que con ello se pueda ocasionar a los particulares, siempre de manera proporcional tomando en cuenta la probabilidad y severidad del daño que pueda representar la obtención de información.

- En materia laboral, los códigos de buenas prácticas son útiles pues logran un equilibrio entre las legítimas expectativas de los trabajadores acerca del correcto tratamiento de su información personal y los intereses legítimos de los empleadores para llevar sus propios negocios, en el marco de la ley.

- Un adecuado procedimiento de otorgamiento de sellos de confianza se construye sobre una sólida base de transparencia y la rendición de cuentas respecto a la recopilación y uso de información personal.

- Por lo que respecta a los principios sustantivos, hay grandes ventajas en las prácticas sugeridas, como son: asignar a una persona para proteger los datos personales, capacitar personal en materia de privacidad y cuidar sus transferencias de datos con terceros; pero también en la capacitación de los consumidores en materia de privacidad sobre las herramientas disponibles para ejercer sus derechos.

- La consulta pública de los mecanismos de autorregulación es valiosa porque implica que las compañías, grupos de industrias, defensores

privados, grupos de consumidores, víctimas, académicos, empresas internacionales, autoridades locales, y en general cualquier otro grupo relevante interesado en el proceso de desarrollar códigos de conducta den soluciones creativas a diversos problemas.

- Los mecanismos de autorregulación exitosos prevén fórmulas para evaluar periódicamente la eficacia de los instrumentos de autorregulación, midiendo el grado de satisfacción de los afectados y, en caso necesario, actualizando el contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

- Quienes adoptan un modelo de autorregulación promueven en su organización o en la de sus afiliados una intensa reorganización de sus sistemas de seguridad de la información y un cambio de cultura en el personal que trata datos personales, indispensables para alcanzar los niveles de protección que la mayoría de las legislaciones exigen para el tratamiento de este tipo de datos.

11).- Principios Generales y Específicos para la Autorregulación en el campo de la protección de datos personales. Como parte de este estudio, se propusieron principios que deben tomarse en cuenta en las etapas iniciales o de maduración de un sistema de autorregulación vinculante en materia de protección de datos personales en posesión de los particulares.

Como Principios Generales, se proponen los siguientes:

a) Toda industria y/o empresa del sector de las TI deberá conocer y respetar los principios que rigen el tratamiento de datos personales. A tales efectos, los agentes económicos deberán garantizar la realización de

cursos de capacitación a todos los niveles, para aquellas personas que traten datos personales con motivo de sus funciones o responsabilidades.

b) Deberá fomentarse el deber de confidencialidad como principio ineludible de cualquier persona que por razón de sus funciones o responsabilidades trata datos personales.

c) Se deberá garantizar el respeto de los derechos de los titulares de datos personales, entre otras medidas, a través de la debida implementación de procedimientos para la atención de solicitudes de derechos ARCO y la designación de la persona o departamento a que se refiere el artículo 30 de la LFPDPPP.

d) Se deberán identificar todos los sistemas de información que traten datos personales para determinar si los mismos cumplen con los niveles de seguridad exigibles para el tipo de datos que tratan.

e) Deberán adoptarse las medidas internas de cada organización que permitan programar, en el menor tiempo posible, la ejecución del análisis de brecha a que se refiere el artículo 61, fracción V del Reglamento de la LFPDPPP. Lo anterior, sin perjuicio de la necesidad de tomar en consideración cualesquiera otras de las acciones a que se refiere dicho artículo 61.

f) En su caso, deberán llevarse a cabo todas las acciones correctoras necesarias para que los sistemas de información que traten datos personales cumplan con las medidas necesarias para garantizar la seguridad de los datos personales.

g) Debe eliminarse la práctica consistente en la “conservación indefinida” de los soportes manuales en que se tratan datos personales y fomentarse la eliminación periódica de los datos personales tratados mediante dispositivos electrónicos, cuando en ambos casos se hubiere cumplido la

finalidad para la cual fueron recabados y no exista disposición legal que disponga su conservación por un tiempo mayor.

h) Siempre que su actividad lo permita, el sector de la TI deberá procurar la implantación de la "oficina sin papeles" en sus propias actividades.

i) Toda organización es responsable de las transferencias de datos (nacionales e internacionales) que deban realizarse con motivo de su actividad. En su caso, deberá asegurarse la legalidad de la transferencia, si esta se realiza para finalidades distintas de aquéllas que originaron la obtención de los datos.

j) Ninguna página web, propiedad de las empresas que participan en el sector de las TI, podrá carecer de una Política de Privacidad y, en su caso, de los Avisos de Privacidad legalmente exigibles si a través de las mismas se recaban datos personales.

Como principios particulares, también se anotaron los específicos para el ámbito de las TI, acentuadas a algunos subsectores particularmente relevantes en el tratamiento de datos personales en el entorno digital.

Empresas dedicadas al diseño, desarrollo, producción, explotación, mantenimiento y/o comercialización de productos, tecnologías y servicios asociados al procesamiento de datos, custodia y administración de información:

a) Toda empresa que procese, custodie o administre datos personales por cuenta de terceros es un **encargado** en los términos a que se refieren los artículos 3, fracción IX de la LFPDPPP y 49 de su Reglamento. Dichas empresas deberán regular este tratamiento mediante la adopción de las

disposiciones contractuales (u otro instrumento jurídico) a las que se refiere el artículo 51 del Reglamento de la LFPDPPP.

b) Los encargados deberán cumplir con todas las medidas de seguridad exigibles conforme al tipo de datos personales tratados o en virtud de la finalidad del tratamiento. Ningún encargado debe tratar datos personales si sus productos, tecnologías o servicios asociados no cumplen con dichas medidas de seguridad.

c) Los empleados de los encargados deben ser consientes del deber de confidencialidad que asumen si tratan datos personales.

Empresas dedicadas al desarrollo de software y hardware:

a) Las empresas que desarrollen software que será destinado al tratamiento de datos personales deberán asegurarse de que sus productos permitirán a los usuarios el cumplimiento de las medidas de seguridad exigibles en virtud del tipo de datos personales que serían tratados o en relación con la finalidad del tratamiento.

b) Los fabricantes de hardware deberán asegurarse de que sus productos garantizan la disponibilidad, accesibilidad e integridad de la información en ellos tratada.

Empresas dedicadas a la prestación de servicios de TI o Business Process Outsourcing (BPO):

a) Si la prestación de los servicios conlleva el tratamiento de datos personales, estas empresas estarán actuando como encargados y, por lo tanto, deberán cumplir las disposiciones de la LFPDPPP y de su Reglamento aplicables.

b) En concreto, deberán regular la relación con sus clientes mediante la adopción de las disposiciones contractuales (u otro instrumento jurídico) a las que se refiere el artículo 51 del Reglamento de la LFPDPPP.

c) Los empleados de este tipo de empresas deben ser consientes del deber de confidencialidad que asumen si tratan datos personales.

Medios creativos digitales, redes, aplicaciones o cualquier otra tecnología de la información que permiten el intercambio, almacenamiento y/o procesamiento informatizado o por medios físicos de datos:

a) Las empresas dedicadas a estas actividades deben asegurar que las tecnologías empleadas aseguran la integridad de los datos personales intercambiados.

b) También deben garantizar que, durante su transferencia, no pueda tener acceso a la información ninguna persona que no se encuentre debidamente autorizada.

c) En el caso de llevar a cabo el registro de comunicaciones electrónicas, estas empresas deberán asegurarse que cuentan con el consentimiento de los titulares para ello o, en su caso, que existe legislación que autorice a realizar dicho registro.

Niños y Adolescentes. Siguiendo con las políticas de Estados Unidos, en 1998 fue promulgada la Children's Online Privacy Protection Act (COPPA) y el 21 de abril de 2000 entró en vigor la Children's Online Privacy Protection Rule, ambas con el propósito de proteger la información personal de los niños menores de 13 años que fueran obtenidos vía Internet.

Para ello el prestador del servicio debe ser parte de un modelo de autorregulación aprobado por la FTC. Las páginas de Internet obtienen un sello de confianza con el cual pueden obtener los datos personales de los menores con un permiso autentificado de los padres.

En su informe del 2010 de la FTC, se sugirió al Congreso otorgar protección a los adolescentes entre 13 y 18 años, ya fuera con la ampliación del rango de protección de la COPPA, o con una legislación especial. Ampliar la cobertura de la ley sería complejo, ya que existe una gran diferencia de comportamiento en línea y uso del Internet, incluso limitar el uso a este sector de la población podría ser contrario a la constitución por restringir su libertad de expresión y el derecho a recibir información.

Flujo Transfronterizo de Datos. Un principio en este rubro deriva de la Directiva 95/46/EC de la Unión Europea, conforme a la cual sólo pueden realizarse intercambios de datos con países que tengan una legislación similar que garantice una protección adecuada de datos personales. Para tal propósito fueron acordados los Safe Harbor Privacy Principles entre la Unión Europea y el Departamento de Comercio de los Estados Unidos, por lo que las empresas que cumplieran con estos requerimientos podían pedir un sello de confianza a dicho departamento con el objetivo de realizar intercambio transfronterizo de datos con la vigencia de un año. En la actualidad más de 2,700 empresas son parte del programa de flujo transfronterizo de datos con la Unión Europea282.

Educación. No se quiere omitir que el caso del nuevo marco norteamericano también llama a la industria a incrementar sus esfuerzos para educar a los

282 Véase White House, nota 1 *supra*, pág. 33.

consumidores en materia de privacidad y las herramientas disponibles para ejercer sus derechos, por lo que hay principios adicionales que debemos considerar, tales como:

La **opción simplificada** es un principio que permea en Estados Unidos, a fin de que las compañías simplifiquen las opciones del consumidor, conforme a los siguientes conceptos:

a) No es necesario otorgar una opción antes de recabar y usar datos personales para prácticas consistentes en una transacción o en la relación entre la compañía y el consumidor, o las requeridas o autorizadas por la ley.
b) Para prácticas que requieren una opción por parte del consumidor, las compañías deben ofrecer la elección al momento y en el contexto en el cual el consumidor realiza la decisión acerca de sus datos. Las compañías deben obtener el consentimiento expreso de los consumidores antes de usar sus datos de manera diferente a los propósitos con que fueron obtenidos; o para obtener información sensible para ciertos propósitos.

Igualmente se está exigiendo mayor **transparencia**, y al efecto se pide a las empresas que:

a) Los avisos de privacidad sean más claros, cortos y estandarizados para una mejor comprensión y comparación de sus prácticas de privacidad.
b) Las compañías provean a los consumidores acceso razonable a su propia información, dicho acceso debe depender de la sensibilidad de los datos o la naturaleza del uso.
c) Todos los interesados incrementen sus esfuerzos para educar a los consumidores sobre las prácticas comerciales en materia de privacidad.

Otros principios derivados del *habeas data*:

a) Estimular una política dirigida a las empresas consistente en "No realizar seguimiento" (**Do not track**).
b) Mejorar las **políticas de privacidad en dispositivos móviles**, debido a que en los últimos años ha aumentado su uso y capacidades.
c) Llamar a los consultores (Data Brokers) a **cumplir con estándares de privacidad** para incrementar la transparencia de sus servicios.
d) Extender su trabajo a los **grandes proveedores de plataformas**, tales como proveedores de servicios de Internet, desarrolladores de sistemas operativos, buscadores y redes sociales, con el objetivo de incrementar sus niveles de privacidad a favor de los consumidores.
e) **Promover la autorregulación con la creación de códigos vinculantes (enforceable).** Acerca de este último punto, el Departamento de Comercio de Estados Unidos, con el apoyo de los principales actores de cada industria han comenzado un proyecto para facilitar el desarrollo de **códigos de conducta para sectores específicos**. La Comisión ha visto este esfuerzo de manera favorable y llama a las compañías, asociaciones y empresas de autorregulación a adoptar los principios contenidos en el marco normativo.

12).- Propuesta de Parámetros (estructura). Una manera de resumir o condensar los hallazgos de los trabajos de comparación de los modelos de autorregulación en materia de privacidad y protección de datos personales en el ámbito específico de las TI, así como para generar recomendaciones concretas en la materia, es formular un primer borrador que sirva de base o guide line para que se emitan los denominados "*parámetros para el correcto desarrollo de los mecanismos y medidas de autorregulación*".

Es importante señalar que con ese objetivo ha sido necesario determinar primeramente la metodología de redacción de los *parámetros,* es decir, su "formato", ya que estos modelos normativos no figuran en ningún tipo de texto conocido formalmente hasta la fecha, al menos desde el punto de vista de una norma que tenga efectos generales con ese nombre. De ahí que se hayan explorado distintos esquemas, resultando el más pertinente el que se asemeja a un reglamento administrativo.

Las consideraciones al respecto han sido necesarias para evitar que se confundan los parámetros con otras normas de la pirámide jurídica, tales como lineamientos, decretos, acuerdos, directivas, criterios, manuales, metodologías, NOM, NMX, reglas de operación, patrones, resoluciones, u otro tipo de normas que derivan de los sistemas de normalización o estandarización.

Otro aspecto relevante a considerar es el concerniente al ámbito material de validez y aplicación de los parámetros, sobre todo si este estudio se ha concretado al entorno digital o al ámbito de las TI como rezan los Términos de Referencia.

Considerando que existen puntos de conexión en el mundo físico y el entorno digital que los parámetros podrían recoger, se ha concebido respetuosamente proponer un anteproyecto que no se circunscriba a uno u otro entrono, sino que tenga un enfoque genérico y sin perjuicio de que paulatinamente se vayan sectorizando los parámetros.

El ámbito material de los parámetros es también muy importante que quede definido en los parámetros, es decir, que se genere la diferencia específica entre cada uno de los mecanismos de autorregulación que se prevén la LFPDPPP y su Reglamento (Códigos deontológicos; Código de buenas

prácticas profesionales; Sellos de confianza; Políticas de privacidad; Reglas de privacidad corporativas; y otros mecanismos, que incluyan reglas o estándares específicos),a fin de evitar confusiones entre los particulares y las autoridades.

La certificación de los responsables es una cuestión que requiere definición como herramienta para garantizar el correcto desarrollo de las medidas o mecanismos de autorregulación y sobre todo, debe establecerse el debido consenso jurídico acerca de si los parámetros: 1) se van a remitir a la Ley de Metrología y Normalización en materia de acreditación/certificación; 2) se va a extender los previsto en esa Ley; o bien, 3) si se va a crear un marco *sui generis* o *ad hoc* para este tema.

Por lo que se refiere al registro de los esquemas de autorregulación, se ha considerado que es facultad exclusiva del IFAIPD proveer las reglas correspondientes, pues conforme al artículo 86 del Reglamento de la LFPDPPP al mismo le corresponde llevar su administración.

A manera de recomendaciones, esta sección se abre un apartado general sobre los mecanismos de regulación *in genere*, con sub-apartados para esquemas particulares y algunos elementos *ad cautelam* en materia de acreditación/certificación, que comprende lo siguiente:

A).- TIPO DE INSTRUMENTO JURÍDICO.

Se propone la elaboración de un ACUERDO por el que se den a conocer los parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley

Federal de Protección de Datos Personales en Posesión de los Particulares.

B).- CONTENIDO

CONSIDERANDOS

En esta sección se deben explicitar los fundamentos del acto administrativo consistente en el acuerdo que da conocer los parámetros, vinculándolo al Plan Nacional de Desarrollo y al Programa Sectorial de Economía 2007-2012.

CAPÍTULO I
DISPOSICIONES GENERALES

En este primer apartado se debe definir el objetivo de los parámetros y su ámbito de aplicación, así como definiciones básicas para su debida comprensión. Igualmente se establecen las características de los esquemas de autorregulación vinculante.

CAPITULO II
DE LAS CLASES DE ESQUEMAS DE AUTORREGULACIÓN

Aquí corresponde señalar los elementos primordiales de los distintos esquemas (medios o mecanismos) de autorregulación referidos en la LFPDPPP y su Reglamento: códigos deontológicos, códigos de buena práctica profesional, sellos de confianza, políticas de privacidad y otros mecanismos.

CAPITULO III
DEL CONTENIDO DE LOS ESQUEMAS DE AUTORREGULACIÓN

Esta sección es muy importante para desarrollar los contenidos mínimos obligatorios de los distintos esquemas de autorregulación para que puedan ser registrados por el IFAIPD, así como el tema de su ámbito de aplicación. Aquí se prevén reglas sobre la complementariedad, mecanismos para medir la eficacia del esquema adoptado, consecuencias y medidas correctivas en caso de incumplimiento, identificación de los responsables, sistemas de supervisión y vigilancia, capacitación, medidas concretas tomadas respecto a la protección a categorías especiales de titulares (*menores, con discapacidad y no hispano hablantes*), transferencias nacionales e internacionales de datos personales, administración del esquema, procedimientos para la protección de los datos[283] y mecanismos alternativos de solución de controversias

CAPITULO IV
DE LA CERTIFICACIÓN

Establecer el marco sobre el tema de la acreditación y la certificación, a fin de establecer su objeto, características, funciones de los acreditadores y certificadores, procedimientos y tipos de certificados. Asimismo este apartado debe establecer las obligaciones de las personas físicas o morales que sean reconocidas como certificadores en materia de protección de datos personales, bajo los principios de independencia, objetividad, confidencialidad y verificación. Este

283 Se estima conveniente que el tema de tratamiento de quejas y solución alternativa de Controversias sea un elemento voluntario y no obligatorio.

capítulo aborda también los temas relativos a vigencia, renovación y revocación de la acreditación.

CAPITULO V
DE LA NOTIFICACIÓN DE LOS ESQUEMAS DE AUTORREGULACIÓN

En esta sección se establecen los requisitos generales para el trámite de notificación de los esquemas de autorregulación que convengan los particulares en términos del primer párrafo del artículo 44 de la LFPDPPP ante las autoridades sectoriales que correspondan y al Instituto, que podría ser por escrito o a través del sitio Web del IFAIPD.

CAPITULO VI
DEL REGISTRO[284]

Solamente se establece que los esquemas de autorregulación notificados se inscribirán en el Registro de Esquemas de Autorregulación Vinculante de Protección de Datos Personales en Posesión de Particulares a cargo del Instituto, siempre que su reúnan los requisitos previstos en estos Parámetros y los que establezcan las Reglas para el Registro de Mecanismos y Medidas de Autorregulación en la materia.

ARTÍCULOS TRANSITORIOS

284 Nuestra propuesta se limita únicamente a señalar aspectos generales del Registro.

Aquí se señala que los parámetros serán vigentes al día siguiente de su publicación en el Diario Oficial de la Federación y que, para efectos su implementación, se establecerá la coordinación con las distintas dependencias de la Administración Pública Federal a convocatoria del titular de la Secretaría.

13).- Consideraciones Finales. Aunque no ha demostrado ser un modelo con alta participación, la autorregulación debe seguir considerándose una alternativa para promover mejores prácticas en materia de protección de datos personales.

Quienes adoptan un modelo de autorregulación promueven en su organización o en la de sus afiliados una intensa reorganización de sus sistemas de seguridad de la información y un cambio de cultura en el personal que trata datos personales, indispensables para alcanzar los niveles de protección que la mayoría de las legislaciones exigen para el tratamiento de este tipo de datos.

Por otro lado, y tomando como punto de referencia las exigencias establecidas en la Unión Europea, resulta indispensable tomar en consideración que en esta región se exige que las transferencias de datos fuera del Espacio Económico Europeo se realice hacia países o responsables que garanticen un nivel de protección a los datos personales, equiparable al que se brinda en esta región.

En este sentido, la adopción de esquemas de autorregulación puede constituir un elemento distintivo para aumentar la competitividad del sector TI frente a otras opciones del mercado, ya que actores de este sector que prestan servicios como alojamiento (*hosting*) o atención al cliente (*call centers*) son altamente requeridos por empresas europeas.

Es importante señalar que la adopción de mecanismos o medidas de autorregulación con valor añadido (con respaldo gubernamental o certificación) puede aumentar la confianza en el comercio electrónico, en un entorno que aún no explota toda la capacidad de este medio de comercialización.

Se percibe que el grado de participación de las autoridades competentes es un factor importante en el éxito de los esquemas de autorregulación, en la medida en que son éstas quienes pueden fomentar su adopción mediante acciones de difusión y de distinción positiva a favor de aquellos responsables que sí los han adoptado.

Conforme a lo anterior, es recomendable analizar la posibilidad de generar una estrategia dirigida a la implementación de un sistema de autorregulación con alta participación por parte de las autoridades encargadas de impulsar el desarrollo productivo de sectores específicos de la economía, con apoyo institucional por parte del Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAIPD).

La estrategia de referencia debería definir también si se impulsa e implementa un esquema que promueva la adopción de códigos de conducta puros y simples o uno que otorgue valor añadido a su adopción, mediante el otorgamiento de sellos o distintivos de confianza debidamente difundidos y respaldados.

La estrategia de difusión y respaldo a los esquemas de autorregulación no debe ser ajena a la utilización de campañas publicitarias realizadas por firmas acreditadas que consigan “posicionar” los sellos como marcas reconocidas.

Proyecto Ejecutado para la:

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI)

Por:

CGMPS Consultores Especializados, S.C.

www.cgmps.com.mx