Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Capítulo cuarto

SEGURIDAD Y PRIVACIDAD EN LA NUBE

Dentro del contexto de la era digital, las características de *Internet*, el tratamiento de la información, el dinamismo de las TIC y la economía digital, es importante destacar los elementos fundamentales que constituyen retos específicos para la adopción del cómputo en la nube en las labores de gobierno electrónico o en general del sector público.

En los retos que se mencionan en el párrafo anterior confluyen los aspectos tecnológico, cultural y jurídico.

En este apartado daremos cuenta de retos jurídicos relevantes para el éxito de la adopción y el desarrollo del cómputo en la nube, en particular la privacidad y la seguridad en la nube.

Debemos darnos cuenta de que los servicios de cómputo en la nube presentan retos al sistema jurídico nacional e internacional y por ello proponemos partir de un marco claro y transparente en el ámbito contractual, donde el gobierno y las empresas se comprometan a lograr los mejores resultados y cumplir con los derechos que están en juego respecto de la información del Estado mismo y de los habitantes y/o ciudadanos.

Como ya hemos mencionado en el estudio, las variantes en la modalidad de cómputo en la nube y los diferentes actores requieren certeza jurídica.

El uso del cómputo en la nube en las distintas áreas del gobierno mexicano debe respetar los derechos de los usuarios, como la libertad de expresión, además de establecer reglas, compromisos y obligaciones claros a los usuarios, titulares, responsables de la información y proveedores de cómputo en la nube. También debe haber certeza de las obligaciones y responsabilidades de los requisitos técnicos y de los comprobantes de la calidad de sus servicios, así como contar con los programas de atención de emergencias, entre otros.

En suma, la confianza en el cómputo en la nube y en el gobierno digital requiere de certeza jurídica, seguridad tecnológica, privacidad de la información y el compromiso y responsabilidad de todos los agentes participantes.

Los aspectos de privacidad y seguridad son correlativos, inseparables e interdependientes en todo el entorno de la nube y su regulación jurídica.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

I. Seguridad

En materia de informática no se puede hablar de seguridad al cien por ciento. En el caso de las TIC y del cómputo en la nube propiamente, un elemento fundamental para su utilización y máximo aprovechamiento es el estándar aplicado de seguridad.

En sentido estricto, y al menos a nivel federal, el Esquema de Interoperabilidad y Datos Abiertos de la Administración Pública Federal, documento al que ya hemos aludido en este estudio, define el término de "ciberseguridad" desde el punto de vista jurídico, como "la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada".

La consultora Gartner[113] en el documento "Evaluación de riesgos de seguridad del cómputo en la nube", señala siete puntos en materia de seguridad y privacidad que se deben considerar antes de suscribirse y establecer una relación contractual con el proveedor de cómputo en la nube:

> 1. Acceso privilegiado del usuario. Los datos confidenciales generados fuera de la empresa traen consigo un nivel de riesgo inherente, ya que los servicios externalizados pueden pasar por alto los "controles físicos, lógicos y de personal". Obtenga la mayor información posible acerca de las personas que manejan sus datos. "Pedir a los proveedores que suministren información específica sobre la contratación y la supervisión de los privilegios de los administradores y los controles sobre el acceso".
>
> 2. Cumplimiento de la normativa. Los clientes son, en última instancia, responsables de la seguridad y la integridad de sus propios datos, incluso cuando está en manos de un proveedor de servicios. Los proveedores tradicionales de servicios están sujetos a auditorías externas y la seguridad de las certificaciones. Los proveedores de cómputo en la nube que se niegan a someterse a estos controles son las "señales de que los clientes sólo pueden utilizar esto para las funciones más triviales".
>
> 3. Ubicación de los datos. Cuando se utiliza la nube, es probable que no se sepa exactamente dónde están alojados sus datos. De hecho, usted ni siquiera sabe en qué país se almacenarán; hay que pedir a los proveedores que se comprometan contractualmente a obedecer los requisitos locales de privacidad en nombre de sus clientes.

[113] *Gartner: Seven cloud-computing security risks.* Bajo el título *Assessing the Security Risks of Cloud Computing*, publicado el 3 de junio de 2008, en la página de Gartner: *http://www.gartner.com/DisplayDocument?id=685308* o disponible en *http://www.networkworld.com/news/2008/070208-cloud.html*

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

4. Segregación de los datos. Los datos en la nube están típicamente en un entorno compartido junto con los datos de otros clientes. La encriptación es eficaz, pero no es una panacea. "Hay que saber lo que se hace para separar los datos en reposo". El proveedor de la nube debe proporcionar evidencia de que los sistemas de cifrado se han diseñado y probado por especialistas experimentados. "Los accidentes de cifrado puede hacer que los datos inutilizables, e incluso el cifrado normal pueda complicar la disponibilidad".

5. Recuperación. Incluso si usted no sabe dónde están sus datos, un proveedor de cómputo en la nube debe decirle lo que ocurrirá con sus datos y el servicio en caso de un desastre. "Cualquier oferta que no se replica en la infraestructura de datos y aplicaciones a través de múltiples sitios es vulnerable a un fracaso total". Pregunte a su profesional si tiene "la capacidad de hacer una restauración completa y cuánto tiempo tomará."

6. El apoyo a la investigación. La investigación de la actividad inapropiada o ilegal puede ser muy difícil en la computación en la nube. "Los servicios de cómputo en la nube son especialmente difíciles de investigar, porque el registro y los datos de varios clientes pueden ser co-ubicados y también pueden propagarse a través de un siempre cambiante conjunto de máquinas y centros de datos. Si usted no puede conseguir un compromiso contractual para apoyar a las formas específicas de investigación, junto con la evidencia de que el vendedor ya ha apoyado con éxito estas actividades, entonces su única suposición segura es que las solicitudes de investigación y descubrimiento serán imposibles.

7. Viabilidad a largo plazo. Idealmente, su proveedor de cómputo en la nube nunca irá a la quiebra, puede ser adquirida por otra empresa. Pero usted debe estar seguro que sus datos deberán estar disponibles incluso después de tal evento. "Pedir a los proveedores potenciales cómo se recuperan los datos y si sería en un formato que pueda importar a una aplicación de remplazo.

Ante el panorama que nos presenta Gartner, se debe considerar que la mitigación de esos riesgos implica un esfuerzo y compromisos de todas las partes. Se trata de preocupaciones que en general se atienden principalmente por el sector empresarial, pues de ello depende en gran medida su crecimiento y/o sostenibilidad. Ninguna empresa con ánimo de seguir creciendo y mantener a sus clientes satisfechos dejaría de atender las mejores prácticas y las normas que garanticen la mayor seguridad de la información en el entorno de la nube.

Ante todo eso, es de vital importancia analizar el perfil del proveedor de la nube, su capacidad, su prestigio y en particular, sus antecedentes en materia de la privacidad que ofrece respecto de la información que trata.

A nivel internacional, se pueden señalar varias normas o instrumentos que brindan un alto grado de seguridad, para hacer frente a los retos comentados.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

A continuación señalamos los más importantes:

— El SAS 70 es un estándar internacional que provee una guía para que un auditor independiente emita una opinión de la descripción de controles de la organización a través del Reporte de Servicio del Auditor. Este reporte puede ser de dos tipos:
  a) El reporte de tipo I, que detalla la descripción de controles de la organización en un punto específico de tiempo (por ejemplo 30 de junio de 2003).
  b) El reporte de tipo II, que no solo incluye la descripción de controles de la organización, sino que también incluye un *testing* detallado de los controles de la organización durante un período mínimo de seis meses (por ejemplo, 1 de enero de 2003 a 30 de junio de 2003).
— Una auditoría bajo los principios de *SysTrust* permite obtener un informe sobre la fiabilidad del sistema con base en la disponibilidad, seguridad, integridad y confidencialidad de la información. A diferencia de SAS 70, no da información sobre los controles y procedimientos internos del proveedor de servicios, y no es un estándar internacional.
— La ISO/IEC 27001, estándar para la seguridad de la información (*Information technology - Security techniques - Information security management systems - Requirements*). Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido "Ciclo de *Deming* (planificar, hacer, verificar, actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002).[114]

En los estándares ISO/IEC, a la seguridad de la información se le asignó la familia 27000, la cual contempla los siguientes:

— ISO 27000: Publicada en mayo de 2009. Contiene la descripción general y el vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.
— UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la versión española, 29 noviembre de 2007. Es la norma principal de requisitos de un

[114] Estas y otras pertenecientes a temas de seguridad, gestión y almacenamiento de información. Además de cuestiones de seguridad de la información en las telecomunicaciones, de aplicaciones y de su administración pública, investigación forense o evidencia digital, pueden verse en *http://www.iso27000.es*

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

sistema de gestión de seguridad de la información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su anexo A contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO17799).
— ISO 27002 (anteriormente denominada ISO17799). Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.
— ISO 27003. En fase de desarrollo; probable publicación: 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
— ISO 27004. Publicada en diciembre de 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.
— ISO 27005. Publicada en junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.
— ISO 27006. Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Como se puede observar, estas normas internacionales son un abanico de posibilidades respecto de la seguridad de la información y el tratamiento de información, que tiene relación con el cómputo en la nube y es el fundamento técnico normativo que utilizan los proveedores de cómputo en la nube.

Ahora bien, hay que mencionar que dentro de nuestro sistema jurídico nacional las normas ISO no son obligatorias, pero sí muy tomadas en cuenta de manera voluntaria por las empresas. Además, se recurre a las normas oficiales mexicanas (NOM), que sí son vinculantes y en muchos casos se basan para su adecuación, en las normas internacionales. En razón de lo anterior, existen varias NOM que ya guardan relación y son utilizadas y exigidas en materia de tratamiento y seguridad de la información.

A continuación presentamos un cuadro que expone algunas de esas equivalencias entre normas técnicas nacionales con su similar internacional.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

DIARIO OFICIAL DE LA FEDERACIÓN 13 de abril de 2006 Declaratoria de Vigencia las Normas Mexicanas (Extracto)	
NMX-I-041/02-NYCE-2006 Tecnologías de la Información-Seguridad de la Información Parte 02: Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).	Campo de aplicación Esta Norma Mexicana tiene por objeto especificar los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo con la Norma Mexicana NMX-I-041/01-NYCE dentro del contexto de los riesgos identificados por la Organización. Concordancia con normas internacionales Esta Norma Mexicana es parcialmente equivalente a la Norma Internacional ISO/IEC 27001:2005.
NMX-I-086/01-NY-CE-2006 Tecnología de la Información (Ti)-Guía para la Gestión de la Seguridad de TI. Parte 01: Conceptos y Modelos para la Seguridad de TI.	Campo de aplicación Esta Norma Mexicana constituye una guía para la gestión de la seguridad de TI. Esta Norma Mexicana (NMX-I-086/01-NYCE) presenta los modelos y conceptos de gestión básicos, esenciales para una introducción a la gestión de la seguridad de TI. Estos conceptos y modelos se discuten y desarrollan en mayor profundidad en las restantes partes de la norma para proporcionar una orientación más detallada. El global de todas estas partes ayuda a identificar y gestionar todos los aspectos de la seguridad de TI. Concordancia con normas internacionales: Esta Norma Mexicana no es equivalente a ninguna norma internacional por no existir referencia alguna al momento de la elaboración de la misma. NOTA: Esta Norma Mexicana es idéntica al Reporte Técnico ISO/IEC TR 13335-1:1996.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

NMX-I-086/02-NYCE-2006 Tecnología de la información (Ti)-Guía para la Gestión de la seguridad de TI. Parte 02: Gestión y Planificación de la Seguridad de TI.	Campo de aplicación: esta Norma Mexicana tiene por objeto presentar las diferentes actividades relacionadas con la gestión y la planificación de la seguridad de TI, así como las funciones y las responsabilidades asociadas dentro de una organización. Es de interés para los gestores de TI con responsabilidades en la adquisición, diseño, implantación y explotación de sistemas de TI. Es también de interés para los gestores responsables de actividades que hacen un uso substancial de sistemas de TI. En general, esta parte es útil para quien tenga responsabilidades de gestión relacionadas con los sistemas de TI de la organización. Concordancia con normas internacionales: esta Norma Mexicana no es equivalente a ninguna norma internacional por no existir referencia alguna al momento de la elaboración de la misma. NOTA: Esta Norma Mexicana es idéntica al Reporte Técnico ISO/IEC TR 13335-2:1997.
NMX-I-086/03-NYCE-2006 Tecnología de la Información (Ti)-Guía para la Gestión de la Seguridad de TI. Parte 03: Técnicas para la Gestión de la Seguridad de TI.	Campo de aplicación: esta Norma Mexicana proporciona técnicas para la gestión de la Seguridad de TI, basadas en las pautas generales descritas en las partes 1 y 2. Dichas técnicas están diseñadas para facilitar la implantación de la seguridad de TI. Para una comprensión completa de esta parte 3 es conveniente estar familiarizado con los conceptos y modelos introducidos en la NMX-I-086/01-NYCE y el material relativo a la gestión y planificación desarrollada en la NMX-I-086/02-NYCE. Concordancia con normas internacionales: esta Norma Mexicana no es equivalente a ninguna norma internacional por no existir referencia alguna al momento de la elaboración de la misma.

Es importante mencionar que los aspectos de seguridad deben abarcar medidas administrativas, físicas, tecnológicas y todas estas contempladas en un ordenamiento jurídico.

Un ambiente de nube que cumpla con medidas de seguridad confiables debe cubrir por lo menos tres áreas:

1. Primero, contar con un programa de seguridad de la información, cuya prioridad radique en prevenir y corregir, en su caso, amenazas

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

a la seguridad de la información y sobre todo, a la operación del usuario.
2. Segundo, mantener actualizada y permanentemente un conjunto de controles que permitan minimizar el riesgo de una eventual vulneración.
3. Y tercero, operar un marco de cumplimiento que cuente con los controles adecuados y que efectivamente se mantengan en correcta operación.

En cuanto a las características del plan de seguridad, por lo menos si atendemos los principios comunes de la familia de estándares ISO/IEC 2700, este debe asegurar medidas y acciones concretas en cuatro rubros:

1) Planear. Las acciones y medidas de seguridad deben constar documentadas, con definición de mecanismos de toma de decisiones basadas en riesgos.
2) Hacer. Contar con los controles de seguridad apropiados y, sobre todo, que estén en efectiva operación.
3) Verificar. El programa debe tener una mecánica de auditoría y verificación, así como de mejoras continuas.
4) Actuar. Es decir, validar la efectividad del plan de seguridad, y mantenerlo actualizado conforme al desarrollo tecnológico o los nuevos retos de seguridad que se vayan planteando con el tiempo.

Un componente importante de seguridad en la nube, como debe serlo en consecuencia también de los documentos de seguridad del proveedor, lo constituye la reacción ante eventuales incidentes o vulneraciones de seguridad.

A este respecto, es básico que el proceso de respuesta se componga al menos de elementos como los siguientes:

a) Preparación. Debe existir un proceso cierto y claro para responder ante eventuales vulneraciones de seguridad.
b) Identificación. El plan de seguridad debe permitir contar con un proceso que pueda identificar ágilmente la naturaleza y las causas de la vulneración.
c) Contención. El plan debe contener elementos claros de contención de los posibles efectos derivados de la eventual vulneración.
d) Mitigación. Consiste en reducir los riesgos de la vulneración producida y evitar consecuencias relacionadas con aquella.
e) Corrección. De forma importante, todo programa de seguridad debe tener la flexibilidad de ajustarse o mejorar con base en una eventual experiencia de vulneración.

Idealmente, es conveniente que el citado programa de seguridad del proveedor de servicios de cómputo en la nube se encuentre certificado por

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

alguna organización independiente de prestigio, o alternativamente por sellos de confianza otorgados por organismos gremiales o similares.

En los temas de seguridad y privacidad, es fundamental que las normas aplicables, independientemente de cuáles sean estas o bajo qué marco legal se circunscriban, reconozcan las buenas prácticas de la industria, así como mecanismos de autorregulación, en particular aquellos que pueden ser susceptibles de ser reconocidos globalmente.

A este respecto, el Instituto Mexicano para la Competitividad publicó "*Cloud Computing*: nuevo detonador para la competitividad de México",[115] que discute los aspectos de seguridad en la nube (entre otros), y concluye con la "desmitificación" en el sentido de que la nube pueda proveer un ambiente "menos seguro" que un ambiente físico.

En este sentido, el estudio del IMCO coincide con nuestra opinión en el sentido de que la información no se encuentra más o menos protegida o segura por "dónde" se encuentre, sino en función de bajo qué estándar (legal y/o contractual) se encuentra protegida, de donde concebimos la importancia del prestigio de quién ofrece la nube.

Además de la coincidencia de la recomendación de no establecer regímenes de protección basados en consideraciones territoriales o de supuesta residencia física de la información, también son mencionables las siguientes sugerencias de acción gubernamental:

1. Adoptar estándares internacionales, así como colaborar en su formación (incluyendo la mención a la posible ampliación del ISO 27000 para incluir temas de privacidad).
2. Suscribir y ajustarse a obligaciones derivadas de convenios internacionales (con una sugerencia específica a suscribir el llamado Convenio de Budapest en materia de ciberdelitos).
3. Aprovechar mecanismos de coordinación regionales (como el Parlamento Latinoamericano o la Cumbre Latinoamericana de Innovación).
4. Establecer preferentemente el adoptar los mecanismos procesales de cooperación internacional o armonización legislativa.

---

[115] Gallegos, Rodrigo y Reyes-Retana Cecilia, *Cloud Computing*: *nuevo detonador para la competitividad de México*, Política Digital. *http://www.politicadigital.com.mx/?P=leernoticia&Article=21198*. También véase Centro de la OCDE en México para América Latina, *Diálogos sobre cómputo en la nube como detonador de competitividad en México*, en *http://www.oecd.org/document/52/0,3746,es_36288966_36287974_44993332_1_1_1_1,00.html* (consultada en diciembre de 2012).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

II. Privacidad

1. *Principios de protección*

La confianza es el principal y más importante elemento para la adopción de las TIC en las empresas y el gobierno. Para ello, es importante que, aunado a la seguridad de la información, haya políticas de privacidad y reglas claras para garantizar la confidencialidad y la adecuada protección de la información.

Al mismo tiempo, debe atenderse el ámbito cultural, lo cual implica generar los valores respecto de la responsabilidad de los usuarios y la estricta selección de funcionarios públicos en el manejo de la información, así como definir los perfiles de los responsables del tratamiento de la información.

La privacidad y el adecuado tratamiento de la información son fundamentales para abonar a la confianza, ya sea que se encuentre tratada desde el interior de las instituciones o a través de los recursos del cómputo en la nube.

Esta confianza debe generarse con la participación y el compromiso de todos los involucrados (sectores público, privado y sociedad) en el ciclo de la información. Se requiere que los proveedores de cómputo en la nube adopten medidas y políticas de seguridad y privacidad que provean un alto estándar de transparencia ante los usuarios. Así, el prestigio de los proveedores y sus antecedentes en el estándar de privacidad y seguridad sobre la información que obtienen de sus clientes (su tecnología y sus políticas internas) debe ser un elemento de consideración indispensable en su contratación.

Por otro lado, es recomendable contar con marcos jurídicos claros a nivel nacional, que sean coherentes con el marco internacional, así como adoptar normas que sean producto del reconocimiento ubicuo, no territorial y multijurisdiccional del cómputo en la nube, teniendo en cuenta que el flujo trasfronterizo de datos es un elemento indispensable en el cómputo en la nube y en la economía digital.

La seguridad y la privacidad en el ámbito técnico son la piedra angular en la confianza a generar sobre el tratamiento de la información, y, por ende, deben contar con una regulación adecuada y competitiva para propiciar un ambiente de confianza, que fomente el uso de las nuevas tecnologías y de los modelos de negocios.

Es así como la privacidad se vuelve día con día un gran reto para el gobierno, para las empresas y para los usuarios de *Internet*, y en especial para el cómputo en la nube.

La seguridad y la privacidad de la información deben formar parte de las políticas públicas del gobierno, de la cultura del respeto a los derechos humanos, de los acuerdos entre empresas y de sus políticas internas. Ello

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

ayudaría a incrementar considerablemente la confianza y contribuir al fomento y al estímulo de la adopción del cómputo en la nube y de cualquier otro entorno de negocios dentro de la economía digital.

En razón de lo anterior, se debe buscar un equilibrio razonable entre el flujo de información (materia prima del desarrollo comercial y de negocios) y la protección de los datos.

En el caso del cómputo en la nube, existe el reto de generar "confianza" en su entorno, para lo cual se requiere de un compromiso de lo regional o internacional a lo local, y la participación activa de todos los agentes interesados en temas inherentes a la nube, según los hemos abordado en el presente estudio.

Dentro del marco jurídico en el tema de la privacidad en el cómputo en la nube, se debe considerar la naturaleza del desarrollo tecnológico, la naturaleza de *Internet* y el flujo de los datos y de los diferentes tipos de contenidos. Además, se debe contemplar la dificultad de la aplicación del derecho nacional a temas que escapan de su jurisdicción, buscando generar acuerdos contractuales de los diferentes agentes que participan o tienen interés en aprovechar las tecnologías y el cómputo en la nube en especial.

Este tema de privacidad conlleva también la profesionalización de los funcionarios responsables del tratamiento de la información. Se deben establecer perfiles adecuados para los funcionarios, definir sus atribuciones y privilegios (de acceso, autorización, etcétera), establecer con claridad las obligaciones y responsabilidades del proveedor de nube, del encargado de la administración de los recursos y de los terceros que participan en alguna etapa, así como de los usuarios y/o titulares de los datos.

En suma, el cómputo en la nube requiere que la confianza jurídica descanse sobre el compromiso y los acuerdos que los proveedores de la nube tengan entre ellos y que cumplan con respecto a los datos de los usuarios. Además, se debe fortalecer un marco de armonización en materia de privacidad y protección de datos personales, como ya se está haciendo en diversas regiones del mundo y a lo que nos referiremos en un apartado especial del presente estudio.

Se necesita un modelo que genere pautas legislativas, administrativas y jurisdiccionales, que establezca también un mecanismo de concentración de buenas prácticas en materia de privacidad y un grupo de asesores o mediadores para toda la región. Por ejemplo, un convenio en materia de privacidad y seguridad de la información para la región de OCDE, TLCAN o Latinoamérica, que incluya pautas a seguir por los proveedores de la nube, los usuarios y la cooperación interinstitucional de las diferentes entidades públicas de los Estados partes.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Algunas empresas que tienen la finalidad de contribuir de manera conjunta a vencer el reto de la desconfianza e incrementar el desarrollo del sector TIC han generado pautas que brindan la certeza de las condiciones y requisitos de los servicios y/o bienes que proveen, en razón de la confianza que otorga el contar con normas vinculantes sobre la privacidad y la protección de sus datos personales.

Cabe destacar que hay consenso de las principales empresas y gobiernos del mundo para procurar un entorno de confianza para los usuarios y clientes de los servicios en la nube. Es por ello que se han realizado foros de líderes de gobierno, empresariales, de asociaciones no gubernamentales, defensores de derechos humanos y expertos en tecnologías, donde se discuten las problemáticas, se generan soluciones, se promueven y adoptan compromisos y normas o estándares internacionales creados por los principales organismos internacionales encargados del tema.

En la medida en que se adopte el compromiso de parte de los proveedores de servicios en la nube, de las empresas de seguridad, de los usuarios y de los gobiernos, se podrá contar con seguridad y privacidad en la nube a un buen nivel de protección y así se logrará generar confianza para su adopción y crecimiento, lo cual traerá beneficios sociales y económicos.

Recientemente, a finales de julio de 2011, la Asociación para la Industria del Software y la Información (en inglés *Software and Information Industry Association*- SIIA), a través de su División de Políticas Públicas, señaló en su Guía de Cómputo en la Nube para Desarrolladores de Normas, que a fin de obtener por completo los beneficios del cómputo en nube, quienes formulan políticas públicas deben: [116]

1. Evitar reglas y políticas de cómputo en nube que sean específicas; favorecer aquellas de carácter general que sean aplicables a una amplia gama de tecnologías y servicios, y a aquellas que mantengan la igualdad de condiciones para el cómputo en la nube y todos los alcances de computación remota y almacenamiento de datos.
2. Promover estándares abiertos para la interoperabilidad del *software* y datos, y evitar políticas que pudieran favorecer un particular modelo de negocio o una tecnología sobre otra.
3. Promover políticas que permitan, en la medida de lo posible, la transferencia irrestricta de datos a través de las fronteras.

[116] Guía de Cómputo en la Nube, (SIIA) 2011, en *http://www.siia.net/aatc/2011/* (consultada en enero de 2011) Esta Guía señala también algunos mitos recurrentes sobre la nube. Traducción propia del autor.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

4. Fortalecer reglas de "gobernabilidad" en el tránsito de información para reconocer adecuadamente los requerimientos de las distintas jurisdicciones y proteger a los interesados respecto al almacenamiento y procesamiento de sus datos en la nube, o en cualquier entorno informático a distancia.
5. Evitar regulación, estatutos o cualquier política que pudiera dar preferencia a quienes procesen información usando instalaciones locales o que operen localmente.
6. Buscar regímenes de privacidad interoperables, sobre los cuales los países reconozcan entre sí sus propias reglas de privacidad en la mayor medida posible.
7. Adoptar un alcance global respecto a ciberseguridad, que reconozca la naturaleza global de los sistemas interconectados y provea de protección al suministro de información, independientemente de dónde se localice y que busque estándares de consenso internacional que impidan reglas de carácter nacional, parciales o impredecibles, entre los distintos países

Por otra parte, la llamada Commission Cloud 2[117], para un adecuado desarrollo del cómputo en la nube a nivel internacional, ha sugerido adoptar los siguientes pasos:

1. Modernización de la legislación (en este caso la Electronic Communications Privacy Act), que rige la ley de acceso a la información digital, a la luz de los avances en materia de tecnologías de la información.
2. Estudiar el impacto de la llamada Patriot Act, así como de leyes similares de seguridad nacional en otros países, en lo que concierne a la posibilidad de las empresas para desplegar la nube en un mercado global.
3. Que los Estados Unidos asuman un liderazgo propiciando un diálogo activo con otras naciones a fin de legitimar el acceso gubernamental a los datos almacenados en la nube y resolver conflictos legales en materia de datos.

Por otra parte, la 33a. Conferencia Internacional de Comisionados de Privacidad y Protección de Datos, que tuvo lugar en la ciudad de México, también dio lugar a conclusiones muy interesantes en materia de privacidad en la nube.

[117] Resumen del Reporte Cloud 2, publicado en 2011, por *Tech American Foundation* en *http://www.techamericafoundation.org/content/wp-content/uploads/2011/07/CLOUD2_Summary.pdf* (consultada en enero 2012). Véase anexo 15.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Específicamente, la llamada "Declaración de la Ciudad de México", que derivó de la Conferencia, señala a la globalización, los "big data", la innovación de los servicios en la red y a los servicios de cómputo en la nube, como los factores que constituyen actualmente los retos más importantes para una protección efectiva de los datos personales.[118]

En ese sentido, uno de los acuerdos más importantes de las autoridades de protección de datos es "impulsar el compartir información con las nuevas autoridades sobre la forma en la cual las organizaciones que emplean datos utilizan las herramientas disponibles para fomentar y promover buenas prácticas en materia de privacidad; así como también la forma en la cual la legislación protectora puede ser aplicada en forma más efectiva…".

Como puede apreciarse, el binomio de las buenas prácticas industriales y una buena legislación es indisoluble e indispensable para que el cómputo en la nube opere bajo altos estándares de confianza y privacidad de la información que los usuarios tratan a través de esos servicios.

La privacidad en el cómputo en la nube implica tomar medidas de prevención hacia el interior y hacia el exterior del entorno de la nube, sobre todo ante posibles violaciones a sistemas de información. Se requiere también la gestión adecuada por parte de los responsables y un marco jurídico acorde y congruente con las circunstancias globales y el flujo transfronterizo, que debe incluir sanciones y estrategias de investigación y cooperación internacional conjunta. Esto se resume en que hace falta certeza jurídica como punto de partida para la generación de la confianza necesaria que permita la adopción del cómputo en la nube en el sector público y privado.

2. *Experiencias internacionales*

Un sector de información relevante, que en muchas partes del mundo goza de una regulación especial, es el compuesto por los datos personales; es decir, la información a través de la cual es posible identificar a una persona física. En materia de privacidad y protección de datos personales, se han generado en el mundo occidental por lo menos tres áreas o modelos de regulación.

---

[118] El texto completo de la Declaración de la Ciudad de México puede consultarse en *http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/Declaracion_Mexico_ESP.pdf.* Cuestionamientos similares a los temas que abordó la Conferencia Internacional de Comisionados de Privacidad y Protección de Datos pueden encontrarse en los "´Términos de Referencia para la Revisión de los Lineamientos de Privacidad de la OCDE", del 31 de octubre de 2011. El texto de los citados Términos de Referencia puede consultarse en *http://www.oecd.org/dataoecd/63/29/48975226.pdf*

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

A. *Modelo europeo*

Regulado bajo principios de calidad y responsabilidad de los encargados de datos personales y garantizando derechos de los titulares de los mismos. Se busca armonizar principalmente entre miembros de la Comunidad Europea a través de la Directiva de Protección de Datos Personales. El Consejo de Europa ha encargado desarrollar estudios específicos sobre el cómputo en la nube, como se ha mencionado en apartados anteriores.

B. *Modelo anglosajón*

Reúne la tradición jurídica del derecho anglosajón respecto al *privacy law*. Principalmente veremos el caso de Estados Unidos, en el cual no se considera derecho fundamental. Da mayor apertura en la comunicación por medios electrónicos y la libertad de expresión.

C. *Modelo latinoamericano*

Modelo híbrido entre los otros dos. Muchos de los países de esta región han establecido tal derecho como fundamental. En México se cuenta con la disposición constitucional, su ley reglamentaria y el reglamento de dicha ley.[119]

Existen diferencias y similitudes que pueden analizarse con mucho detalle, pero para efectos de este estudio lo más relevante es que los sectores público y privado buscan generar pautas o principios generales mediante acuerdos a favor de generar confianza al usuario de *Internet*, el respeto a sus derechos sobre la información (privacidad, confidencialidad y protección de sus datos personales), con la finalidad de encontrar un punto de equilibrio entre la protección de derechos y el flujo necesario y responsable de la información.

Como parte del tema de la regulación o normas obligatorias con relación a la privacidad y la protección de datos personales, señalaremos de manera enunciativa el marco con que cuenta la legislación europea básica en materia de protección de datos:

— La Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995 (la Directiva de Protección de Datos) armoniza las legislaciones nacionales que exigen unas prácticas de gestión de datos de alta calidad a los "responsables del tratamiento de datos" y la garantía de una serie de derechos a las personas físicas.

[119] Se trata del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *DOF* el 23 de diciembre de 2011.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

— La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, del 12 de julio de 2002, garantiza el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.
— El Reglamento 45/2001, del 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y a la libre circulación de estos datos, regula el tratamiento de datos personales de las personas físicas realizado por las instituciones y organismos comunitarios.
— Decisión Marco 2008/977/JAI del Consejo, del 27 de noviembre de 2008 relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

La Directiva de Protección de Datos pretendía ser el paraguas para que se diera el punto de arranque a las directrices de armonización de las leyes de cada país miembro sin invadir sus principios nacionales. Sin embargo, la Directiva ha quedado desfasada respecto de la realidad de los modelos de negocios, del desarrollo tecnológico y de la necesidad del flujo de datos transfronterizo, en esa búsqueda de equilibrio entre la privacidad y la seguridad de la información y el desarrollo de la economía global de la información.

Es evidente que desde la fecha de su publicación, hace casi dieciséis años, han sucedido cambios muy significativos que exigen la adecuación del marco jurídico con todo el contexto económico y tecnológico. Ejemplo de ello es el reto que significa el cómputo en la nube.

Una de las principales restricciones del uso e implementación del cómputo en la nube es lo relativo al flujo, sobre todo en la importación o exportación de éstos. La Directiva que rige en Europa no contempla en su contenido una redacción que otorgue certeza jurídica y que estimule el aprovechamiento del cómputo en la nube y los beneficios que esperan obtener los distintos gobiernos europeos en distintos ámbitos.

La necesidad de la modificación del marco de protección de datos personales en Europa es evidente y ya se está trabajando en ello. En la Asamblea sobre Agenda Digita para Europa, que se llevó a cabo en junio de 2011 se destacó la urgencia de adecuar la Directiva de Protección de Datos y los demás ordenamientos relativos, para brindar confianza en la cesión y en el flujo de datos que den certeza jurídica al cómputo en la nube. Todo ello con el claro objetivo de alcanzar el éxito que ofrece este modelo de negocio basado en el ahorro y en el aprovechamiento compartido de recursos.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Hasta ahora, con la disposición actual en la materia, existen acuerdos para los países o empresas del exterior que buscan la equivalencia en el nivel de seguridad y privacidad de la información. Para la relación de los gobiernos y las empresas de Estados Unidos y Europa se han establecido acuerdos especiales que cumplan con los requisitos legales y técnicos que establece la regulación jurídica europea. Tal es el caso del *Safe Harbor*,[120] que cuenta con equivalencia y aceptación para empresas de los Estados Unidos, principalmente con la Comunidad Europea.

El tema del flujo de datos para los países miembros de la UE se encuentra insuficientemente regulado. Los datos pueden fluir libremente cumpliendo los requisitos dentro de la Unión Europea. Adicionalmente, se reconoce un grado equivalente en la privacidad. La Comisión Europea ha reconocido otros países que tienen un nivel de protección adecuado, entre ellos Suiza, Canadá, Argentina, Jersey y la Isla de Man y Uruguay, entre otros.

Y gracias a los principios sobre privacidad del *Safe Harbor* y el *AirPassenger Name* se establecen relaciones comerciales y turísticas con Estados Unidos.

Por su parte, Estados Unidos está trabajando en la adecuación de la "Ley de Privacidad en las Comunicaciones Electrónicas" (ECPA, por sus siglas en ingles). Además, cuenta con las legislaciones de cada uno de los estados, lo cual hace difícil lograr la certeza jurídica que requiere el constante desarrollo de las TIC y los nuevos modelos de negocio. Esta ley no ofrece los suficientes elementos para que el cómputo en la nube tenga el éxito deseado por las empresas y el gobierno. Cabe señalar que la ECPA se promulgó a mediados de la década de 1980. Es evidente que en aquellos días la nube se encontraba en sus primeros años y la regulación en materia de privacidad se refería básicamente a la conservación y a la privacidad de las comunicaciones electrónicas, como el *e-mail*. Claramente se observa que la regulación en Estados Unidos también se encuentra desfasada del fenómeno del cómputo en la nube y por ser éste el país donde residen varias de las más importantes empresas que proveen servicios de cómputo en la nube debe actualizar su legislación y coordinar el compromiso de las proveedoras, con el fin de alcanzar la transparencia, que abone en favor de la confianza.

En el caso de Latinoamérica, existen legislaciones recientes que consolidan un modelo de combinación de los dos sistemas mencionados y aun entre los principales países (Argentina, Colombia, Chile, México y Uruguay) hay, como era de esperarse, algunas diferencias. Sin embargo, se ha venido trabajando en la homologación del marco jurídico a nivel de las autoridades encargadas de velar por la protección de los datos personales en estos países.

[120] Programa Puerto Seguro, *http://export.gov/safeharbor/* (consultada en diciembre de 2011).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Ejemplo de lo anterior es el trabajo realizado por la Red Iberoamericana de Protección de Datos Personales.[121]

En suma, se puede ver cómo los sistemas jurídicos de las diferentes países y regiones del mundo se encuentran en medio del reto jurídico, que es la necesidad de brindar certeza jurídica a las operaciones electrónicas y sobre todo, a los modelos de negocios basados en el flujo de datos y su tratamiento a través de *Internet*, como es el caso del cómputo en la nube.

Se reitera que es necesaria y urgente la participación de todos los sectores, pero el liderazgo del gobierno es fundamental. En especial, el sector de TIC debe contribuir al forjamiento de ese liderazgo del gobierno y buscar que la Directiva Europea publicada en 1995 y la Ley de Privacidad en las Comunicaciones Electrónicas de los Estados Unidos de América que data de la época de los ochenta, sean actualizadas y sirvan de fomento al uso, adopción y éxito del cómputo en la nube.

Como sabemos, las leyes deben ser tales que logren impulsar el desarrollo y la adopción de las TIC, la nube en este caso, sin que obstaculicen o puedan quedar obsoletas con facilidad en el corto plazo; es preferible que tanto las leyes locales como las regionales establezcan las mejores prácticas a nivel internacional respecto de la seguridad y la privacidad en el flujo de la información.

Ante lo anterior, se sugiere adoptar normas técnicas que se generan mediante el consenso y la participación en órganos incluyentes y democráticos.

3. *Regímenes especiales de protección de datos*

De la misma manera que ocurre en el caso de la seguridad, el reconocimiento de las buenas prácticas de la industria y de los esquemas de autorregulación es fundamental para conseguir un marco eficaz y operativo de privacidad.

Un ejemplo significativo son las Reglas Corporativas Vinculantes, generalmente aplicables a empresas de la Unión Europea o con operación en

[121] Red Iberoamericana de Protección de Datos, cuyas reuniones proponen caminar hacia la homologación en pro de la practicidad y la adopción de las mejores prácticas en la protección de los derechos de los usuarios y los titulares de datos personales. Señalamos, por ejemplo, el seminario "El impacto de las trasferencias internacionales de datos en América Latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos" realizado del 14 al 16 de junio del 2011 en el Centro de Formación de Cartagena de Indias, Colombia. En el evento se propuso que se realizara una compilación de sentencias emitidas por los órganos de justicia de cada país o en el plano regional, con independencia de que exista o no una ley sobre el tema. Véase la página de la Red en *http://www.redipd.org/* (consultada en diciembre de 2011).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

ella, usualmente conocidas por su acrónimo "BCR", por su denominación en inglés *Binding Corporate Rules*.[122]

Las BCR son normas internas (tales como un código de conducta) adoptadas por un grupo multinacional de empresas que definen su política global respecto a las transferencias internacionales de datos de carácter personal dentro del mismo grupo empresarial, a las filiales situadas en países que no proporcionen un nivel adecuado de protección, a fin de ofrecer garantías suficientes para la protección de la privacidad, derechos fundamentales y las libertades de los individuos, en cumplimiento del apartado 2 del artículo 26 de la Directiva 95/46/CE.

Estas reglas tienen su origen en la aprobación del documento de trabajo WP74 (del 3 de junio de 2003) por el grupo de trabajo del artículo 29, establecido en virtud del artículo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo (del 24 de octubre), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Este sistema de Reglas Corporativas Vinculantes se encuentra desarrollado en los siguientes documentos de trabajo del Grupo de Autoridades Europeas de Protección de Datos (grupo de trabajo del artículo 29):[123]

— WP107, del 14 de abril de 2005, por el que se expone un procedimiento de cooperación para la emisión de dictámenes comunes sobre las salvaguardas adecuadas que resultan de las normas corporativas vinculantes *Binding Corporate Rules*.
— WP108, del 14 de abril de 2005, por el que se establece un modelo en forma de lista de control para solicitar la aprobación de normas corporativas vinculantes o *Binding Corporate Rules*.
— WP 74, del 3 de junio de 2003, sobre transferencias internacionales de datos personales a terceros países: aplicación del artículo 26.2 de la Directiva 95/46/CE, a las *Binding Corporate Rules* para las transferencias internacionales de datos.

---

[122] Reglas Corporativas Vinculantes (*Binding Corporate Rules* BCR), en *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf* (consultada en diciembre de 2011). Véase anexo 16.

[123] El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, tiene carácter de órgano consultivo independiente, y está integrado por las autoridades de protección de datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea —que realiza funciones de secretariado—. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en calidad de observadores.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Las BCR no buscan sustituir a las cláusulas contractuales o los contratos-tipo aprobados por la Comisión Europea, sino que constituyen una alternativa que puede suscribirse entre exportador e importador para la regulación de una transferencia internacional que suponga una cesión de datos, cuando el destinatario de los datos está ubicado en un país fuera de la Unión Europea y que no goza de un nivel de protección adecuado. Por ejemplo, sería el caso de una empresa europea que contrata a una empresa de *hosting* ubicada en China, sobre la premisa de un carácter verdaderamente vinculante tanto en el interior como en el exterior.

Algunos de los criterios previos a la elaboración de unas BCR deben ser: a) facilidad para el flujo de datos; b) implicación de la cultura de protección de datos en la multinacional; c) existencia de un valor añadido de la multinacional; d) colaboración con las autoridades de control; e) publicidad del tratamiento de los datos de cara a los ciudadanos; f) procedimientos ágiles para el ejercicio de los derechos; g) mejora del cumplimiento de la normativa de protección de datos; h) posibilidad de configurar las BCR como un mínimo si la legislación local es más rigurosa.

En cuanto a las fases para su creación, tenemos:

1. Fase de decisiones iniciales:
   - Seleccionar el equipo y la gestión.
   - Campo de aplicación.
   - Designación del punto de entrada: implicación de terceras entidades, estructura en capas.
2. Fase de análisis interno:
   - Recopilar información.
   - Comparar con la legislación aplicable.
   - Elaborar el mapa de contenidos y procedimientos: redactar normas e implantarlas.
3. Fase de proceso de solicitud:
   - Acercamiento inicial entre la multinacional y la autoridad competente.
   - Labor de equipo entre la multinacional y la autoridad competente.
   - Realizar solicitudes en borrador para que así la autoridad guíe a la multinacional.

En cuanto al contenido de las BCR, si bien éstas deben elaborarse a la medida de cada multinacional, el contenido de ellas deberá ser al menos el siguiente:

- Delimitar los flujos de información en el grupo y su sometimiento a los principios de protección de datos.
- Establecer los procedimientos para su ejecución interna.
- Auditorías.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

— Transparencia.
— Publicidad frente a terceros.

Estos acuerdos surgen de la necesidad de acelerar el crecimiento y favorecer los intereses de las empresas involucradas, propiciando un equilibrio entre los intereses y el respeto a los derechos de los usuarios. Para efectos de referencia, en seguida se incluye un ejemplo de ciertas cláusulas tipo[124] que se utilizan en la Unión Europea para transferencias de datos en el contexto de los citados BCRs.

Para el caso de México y otras economías del APEC, un mecanismo similar a las BCR de la Unión Europea son las Reglas Transfronterizas de Privacidad de la APEC (usualmente conocidas por su acrónimo CBPR, de su denominación en inglés *Cross-Border Privacy Rules*). Al igual que las BCR, se trata de normas que son desarrolladas por organizaciones usuarias, que documentan el tratamiento de datos personales dentro de las entidades de la misma organización o del mismo grupo de interés y que son susceptibles de obtener reconocimiento global o multi-jurisdiccional, con base en el cumplimiento de las normas de privacidad del APEC y las normas de privacidad correspondientes a la jurisdicción donde cada unidad de negocio tiene operación.

A este respecto, las economías que conforma el APEC reconocen la importancia de proteger la privacidad de la información y mantener los flujos de información entre las economías de la región Asia Pacífico y entre sus socios comerciales. Y señalan que "para desarrollar e implementar tecnologías y políticas que establezcan confianza en cuanto a comunicación, información y sistemas de entrega seguros, protegidos y fidedignos, y que traten asuntos que incluyan la privacidad...". La falta de confianza del consumidor hacia la privacidad y la seguridad de transacciones en línea y redes de información es un elemento que puede impedir a las economías miembro, obtener todos los beneficios del comercio electrónico. Las economías del APEC deben equilibrar y promover la protección de la privacidad de la información y el libre flujo de información en la región. Ante ello, se crea el Marco de Privacidad del Foro de Cooperación Económicas Asia-Pacífico (APEC).[125]

---

[124] Cláusulas Tipo, en relación al uso de BCR, en *https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/decision_comm_clausulas_contractuales_2010.pdf* (consultada en diciembre 2012).

[125] "Un marco que permita la transferencia de datos regionales beneficiará a los consumidores, a las empresas y a los gobiernos. Ministros han aprobado el Marco de Privacidad de APEC, reconociendo la importancia de desarrollar protecciones efectivas para la privacidad que eviten barreras a los flujos de información, asegurar en intercambio continuo…". Véase

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

El APEC ha realizado el Marco mencionado en concordancia con las Directrices de la OCDE[126] sobre la Protección de la Privacidad y flujos transfronterizos de datos personales, que "…aplican a datos personales del sector público o privado que, debido a la forma en que se procesan, a su naturaleza o al contexto en que se usan, suponen un peligro para la privacidad y las libertades individuales".

Estas directrices no se deberían interpretar como medio para evitar:

1. La aplicación de diferentes medidas protectoras a diferentes categorías de datos personales dependiendo de su naturaleza y del contexto en el que se recogen, almacenan, procesan o divulgan;
2. La exclusión de la aplicación de las directrices de datos personales que obviamente no entrañan riesgo alguno para la privacidad ni las libertades individuales; o bien
3. La aplicación de las directrices solo al procesamiento automático de datos personales.

Las excepciones a los principios de los capítulos dos y tres de estas directrices, como las relacionadas con la soberanía y la seguridad nacionales y el orden público, deberían ser:

— La menor cantidad posible y
— De conocimiento público.

En el caso concreto de países federales, la observancia de estas directrices se podría ver afectada por la distribución de competencias.

Estas directrices se deberán considerar como estándares mínimos que se puedan complementar con otras medidas de protección de la privacidad y de las libertades individuales.

Por su parte, la Organización de Estados Americanos generó un Proyecto de Principios en materia de Protección de Datos Personales, los cuales enunciamos enseguida:[127]

1. Legitimidad y justicia.
2. Propósito específico.
3. Limitados y necesarios.
4. Transparencia.

el Marco de Privacidad APEC en *http://publications.apec.org/publication-detail.php?pub_id=390* (consultada en junio de 2013). Véase anexo 18.

[126] Resumen de Directrices OCDE, en *http://www.oecd.org/dataoecd/16/51/15590267.pdf* (consultada en junio de 2013). Véase anexo 19.

[127] Documento OEA/Ser. G. de 2010, en *http://www.oas.org/dil/esp/CP-CAJP-2921-10_esp.pdf* (cconsultada en junio de 2013). Véase anexo 20.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

5. Rendición de cuentas.
6. Condiciones para el procesamiento de datos.
7. Revelación de información a los procesadores de datos.
8. Transferencias internacionales.
9. Derecho de la persona al acceso a la información.
10. Derecho de la persona a corregir y suprimir sus datos personales.
11. Derecho a objetar el procesamiento de datos personales.
12. Legitimación para ejercer los derechos sobre el procesamiento de datos personales.
13. Medidas de seguridad para proteger los datos personales.
14. Deber de confidencialidad y
15. Control, cumplimiento y responsabilidad.

Todos estos principios son de manera general los que han servido de base para el desarrollo de los ordenamientos de protección de datos en Latinoamérica y que sirven de referencia para el caso concreto del uso de la nube en el sector público en México.

Cómo podemos observar, los principios en privacidad son aplicables en gran parte al cómputo en la nube y ante ello se tiene un reto interesante atendiendo a que el principal obstáculo es la desconfianza.

Así, en la medida en que nuestro país es una de las principales economías de APEC, es muy posible que los CBPR de la APEC adquieran una enorme relevancia como una herramienta de cumplimiento de las disposiciones legales en materia de privacidad y protección de datos personales en México.

4. *Protección de datos personales en México*

En el caso de México, haremos una mención breve del marco jurídico que se refiere al derecho de protección de datos y la relación que guarda respecto del cómputo en la nube.

En primer lugar, este derecho ya está contemplado a nivel constitucional. Nuestra carta magna, en sus artículos 6o., 16, segundo párrafo, y 73, establecen el marco constitucional del derecho a la privacidad y de los datos personales como derecho fundamental, y expresan lo siguiente:

> Artículo 6o. …
>
> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reser-

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

vada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la *vida privada* y los *datos personales* será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Artículo 16. …

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.

Artículo 73. El Congreso tiene facultad: …

XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares. Las cursivas son nuestras

Ahora bien, debemos señalar que en nuestro país los datos personales han sido divididos según quien los posee, es decir, en posesión de:

a) Particulares.

b) Sector público.

Desde nuestro punto de vista, es uno de los varios cambios por hacer en nuestra legislación, pero sigamos la unificación de éstos, perfilando hacia la adopción del cómputo en la nube y su regulación jurídica en México y especialmente a la adopción del sector público.

En el caso de los datos personales en posesión de los particulares, tenemos principalmente:

1. Instrumentos internacionales (convenciones, tratado, pactos, declaraciones; derecho a la intimidad, a la vida privada o a la privacidad);
2. TLCAN (protección de datos poco exigente y con lagunas);
3. Acuerdo Global de Asociación Económica, Concertación Política y Cooperación México-Europa (exige protección elevada);[128]

[128] El 8 de diciembre de 1997, México y la Unión Europea firmaron el Acuerdo de Asociación Económica, Concertación Política y Cooperación. Este acuerdo, comúnmente llamado Acuerdo Global, está conformado por tres capítulos: dialogo político, cooperación y comercio. En lo comercial, el Acuerdo fija el objetivo de establecer una Zona de Libre Comercio (ZLC) en bienes y servicios, la apertura mutua de los mercados de compras públicas, la liberalización de los movimientos de capital y pagos, así como la adopción de normas en áreas de competencia y propiedad intelectual, donde incluye la cooperación para generar un marco jurídico para los servicios en línea y la protección de la privacidad y el adecuado

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares;[129]
5. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;[130]
6. Ley Federal de Protección del Consumidor, y
7. Criterios de cortes internacionales y de la Suprema Corte de Justicia de la Nación (SCJN).

En el caso de los datos personales en el ámbito público, los ordenamientos jurídicos que le dan fundamento al cómputo en la nube son:

— Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y Lineamientos de Protección de Datos Personales;[131]

Capítulo III "De los datos reservados y confidenciales"

…

Capítulo IV "De la protección de datos personales"

…

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

…

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI, Las demás que dispongan las leyes.

— Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;[132]

En su artículo 47, señala que los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades garantizarán la protección de los derechos de los individuos, en particular, a la vida privada y a la intimidad, así como al acceso y corrección de sus datos personales, de conformidad con los lineamientos que expida el Instituto y demás disposiciones aplicables para el manejo, mantenimiento, seguridad y protección de los datos personales.

---

tratamiento de los datos personales. Véanse de manera más precisa los artículos 12, 20 y 51 en *http://eeas.europa.eu/delegations/mexico/documents/eu_mexico/acuerdo97.es.pdf*

[129] Véase Anexo 21

[130] Véase Anexo 22

[131] Véase (extracto de) anexo 23.

[132] Véase (extracto de) anexo 24.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

— Lineamientos de Protección de Datos Personales;[133]

Tratamiento de datos por terceros

…

Vigésimo primero. Cuando se contrate a terceros para que realicen el tratamiento de datos personales deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

— Recomendaciones sobre medidas de seguridad aplicables a los sistemas de Datos Personales emitidos por el IFAI;

Instrumento técnico de apoyo en materia de medidas de seguridad aplicables a los sistemas de datos personales tanto físicos como automatizados, en posesión de las dependencias y entidades de la administración pública federal.

— Lineamientos Generales para la Organización y Conservación de los Archivos y las Dependencias de las Entidades de la Administración Pública Federal

…

Capítulo IV de "Documentos electrónicos"

Vigesimotercero. Las dependencias y entidades tomarán las medidas necesarias para administrar y conservar los documentos electrónicos, generados o recibidos, cuyo contenido y estructura permitan identificarlos como documentos de archivo que aseguren la identidad e integridad de su información.

Vigesimocuarto. Las dependencias y entidades aplicarán las medidas técnicas de administración y conservación que aseguren la validez, autenticidad, confidencialidad, integridad y disponibilidad de los documentos electrónicos de acuerdo con las especificaciones de soportes, medios y aplicaciones de conformidad con las normas nacionales e internacionales.

Vigesimoquinto. Las dependencias y entidades realizarán programas de respaldo y migración de los documentos electrónicos, de acuerdo con sus recursos.

— Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.[134]

---

[133] *DOF* 30/09/2005, disponible en: *http://www.fifonafe.gob.mx/m_legal/28.pdf* (consultado en enero 2012). Véase anexo 25.

[134] Esquema de Interoperabilidad y Datos Abiertos de la Administración Pública Federal, publicado en el *Diario Oficial de la Federación* del 6 de septiembre de 2011. Disponible en *http://www.normateca.gob.mx/Archivos/42_D_2803_06-09-2011.pdf* consultada en octubre de 2011. Véase anexo 6.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Tiene por objeto determinar las bases, principios y políticas que deberán observar las dependencias, las entidades y la Procuraduría General de la República, para la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar plataformas y sistemas de información, a fin de incrementar la eficiencia operativa de la Administración Pública Federal y su relación con la sociedad.

…

ARTÍCULO DECIMO PRIMERO. Las dependencias y entidades, en el ámbito de sus respectivas competencias, llevarán a cabo acciones tendientes a propiciar que en la prestación de servicios digitales, los particulares puedan:

I. Elegir libremente el canal y tipo de tecnología que les permita comunicarse de forma digital con las dependencias y entidades;

II. Interactuar con aplicaciones o sistemas basados en estándares abiertos;

III. Recibir atención simplificada a través de puntos únicos de contacto "ventanillas únicas", preferentemente digitales;

IV. Conocer vía remota, por medios digitales, el estado de sus trámites;

V. Obtener copias electrónicas de los documentos relacionados con el servicio digital de que se trate que la institución esté obligada a proporcionarle por ese medio;

VI. Contar con mecanismos digitales de participación ciudadana;

VII. Ser identificados por medios digitales por una sola vez, salvo que se advierta que los documentos presentados para acreditar su identidad son falsos, omitan dar aviso a la dependencia o entidad respectiva de cualquier modificación de los datos que haya proporcionado para su identificación personal o en términos de las disposiciones aplicables a la prestación del servicio digital de que se trate se requiera la confirmación de su identidad, y

VIII. Tener acceso a datos abiertos.

ARTÍCULO DÉCIMO SEGUNDO. Las dependencias y entidades en la prestación de servicios digitales deberán:

I. Asegurarse de que los servicios y sistemas digitales a su cargo mantengan la capacidad de interoperar, como una cualidad integral desde su diseño y a lo largo de su ciclo de vida;

II. Observar los documentos técnicos que en materia de interoperabilidad emita la Secretaría;

III. Favorecer, durante la búsqueda de soluciones tecnológicas, el enfoque de soluciones multilaterales;

IV. Identificar, clasificar y documentar, con el apoyo de la Subcomisión, la infoestructura que le corresponde y comunicarla a la Secretaría, a través de la Unidad de Gobierno Digital, y

V. Tener en cuenta que la información contenida en los medios digitales a su cargo es un recurso estratégico del Gobierno Federal que se debe:

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

a) Utilizar con sujeción a las disposiciones legales aplicables, para el cumplimiento de la función pública con independencia de quien la administre;
b) Poner a disposición de la sociedad, cuando la información digital sea pública y en términos de las disposiciones aplicables no tenga naturaleza reservada o confidencial, como datos abiertos, de modo tal que sea técnicamente posible localizarla, recuperarla, indizarla y reutilizarla a través de aplicaciones Web;
c) Administrar, desde que se obtenga o genere y hasta su eliminación, y con independencia del medio o formato en que se encuentre contenida, en términos de las disposiciones aplicables, y
d) Solicitar, en la medida de lo posible, una sola vez a los particulares y reutilizarla cuantas veces resulte necesario, en términos de las disposiciones aplicables.

Cuando una dependencia o entidad requiera comprobar la existencia de información establecida como requisito para la prestación de un servicio digital a su cargo, y ésta se encuentre bajo la responsabilidad de alguna otra, la deberá solicitar en primera instancia a la dependencia o entidad respectiva a través de un medio de transmisión electrónica, y sólo que no sea factible obtenerla de ésta, podrá solicitar su entrega al particular.

— Ley Federal de Firma Electrónica[135]

Establece la regulación de la firma electrónica avanzada, el certificado electrónico y los servicios a su alrededor.

…

Artículo 8. Para efectos del artículo 7 de esta Ley, la firma electrónica avanzada deberá cumplir con los principios rectores siguientes:
I. Equivalencia Funcional: Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;
II. Autenticidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;
III. Integridad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
IV. Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacio-

[135] Véase Ley Federal de Firma Electrónica, publicada en el *DOF*, 11 enero 2012, Disponible en *http://www.diputados.gob.mx/LeyesBiblio/ref/lfea/LFEA_orig_11ene12.pdf*, consultada en enero de 2012. Véase anexo 26.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

> nados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;
> V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y;
> VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

— Ley Federal de Archivos[136]

El objeto de esta Ley es establecer las disposiciones que permitan la organización y conservación de los archivos en posesión de los Poderes de la Unión, los organismos constitucionales autónomos y los organismos con autonomía legal, así como establecer los mecanismos de coordinación y de concertación entre la Federación, las entidades federativas, el Distrito Federal y los municipios, para la conservación del patrimonio documental de la nación, así como para fomentar el resguardo, difusión y acceso de archivos privados de relevancia histórica, social, técnica, científica o cultural.

A continuación, abonaremos en la conceptualización jurídica de la nube, a lo que podemos señalar específicamente dos ordenamientos federales.

En el ámbito privado, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,[137] que hace referencia expresa al tratamiento de datos personales en el "cómputo en la nube" y a la letra dice:

> Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:
> I. Cumpla, al menos, con lo siguiente:
> a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;
> b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

[136] Véase el Decreto publicado el *DOF*, el 23 de enero de 2012, en *http://www.diputados.gob.mx/LeyesBiblio/ref/lfa/LFA_orig_23ene12.pdf* (consultada en febrero de 2012). Véase anexo 27.

[137] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares Publicado en el *DOF*, el 21 de febrero de 2011. Véase anexo 20.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio y
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio y
II. Cuente con mecanismos, al menos, para:
a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para fines del presente Reglamento por cómputo en la nube se entenderá al *modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente* [Las negritas y cursivas son nuestras].

Las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube."

También debe referirse a los siguientes:

* CRITERIOS Generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos.

*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.

Ambos emitidos por el IFAI y disponibles en su sitio web.

En el ámbito público, encontramos que el artículo primero del Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal,[138] a la letra dice:

[138] Publicado en el *DOF* el 6 de septiembre de 2011, Véase anexo 6.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

> ARTÍCULO PRIMERO. Se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, el cual tiene por objeto determinar las bases, principios y políticas que deberán observar las dependencias, las entidades y la Procuraduría General de la República, para la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar plataformas y sistemas de información, a fin de incrementar la eficiencia operativa de la Administración Pública Federal y su relación con la sociedad.
>
> … V. Cómputo en la nube: al modelo de prestación de servicios digitales que permite a las instituciones públicas acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios.

Al respecto, vale la pena señalar que son los primeros en contemplar una definición legal y a pesar de la diferencia en la redacción de la definición de cómputo en la nube, se deja ver en esencia que se basan en la definición del NIST, que, como dijimos, es aceptada y referenciada a nivel internacional.

Lo anterior nos merece el comentario en el sentido de que el cómputo en la nube está legalmente permitido y que las definiciones se complementan de manera que cubre con lo que establece la definición que tomamos como base, y que ha sido la más utilizada por distintas organizaciones internacionales.

Como se puede observar, actualmente nuestro marco jurídico contempla expresamente el tratamiento de datos mediante la nube, y en ningún momento prohíbe que un tercero pueda llevar a cabo la administración o el tratamiento de la información pública.

De lo anterior se desprende algo claro: que el marco jurídico mexicano permite la contratación del cómputo en la nube y contempla que las dependencias permitan la tercerización de los servicios previa comprobación de que los proveedores cuenten con mecanismos que ofrezcan seguridad, privacidad y protección de datos personales.

Hay que decir que en el caso del cómputo en la nube, se debe atender a los antecedentes y a las características de los proveedores y exigir el cumplimiento de los más altos estándares internacionales. Si el proveedor cumple con las normas internacionales mencionadas en otros apartados, y, por ende, rebasa lo dispuesto por la ley y el reglamento, podemos pensar que se trata de un proveedor confiable.

En cuanto al tratamiento de los datos personales en el ámbito privado, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares tiene preponderantemente las siguientes características: I) está basada en un modelo legislativo de aviso de privacidad previo y II) se funda principalmente

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

en un régimen de *opt-out* para datos no sensibles y de *opt-in* para datos sensibles y datos financieros y patrimoniales.

Se trata de una ley cuyo principal objetivo es proteger la privacidad de los datos personales de los individuos (personas físicas), que están en posesión o conocimiento de empresas privadas. El objetivo último de la Ley es que las bases de datos compuestas de "datos personales" sean debidamente protegidas y no sean objeto de acceso o aprovechamiento ilícito.

En el contexto de la citada Ley, "datos personales" significa "cualquier información concerniente a una persona física identificada o identificable". Esto significa que puede tratarse de información numérica, alfabética, gráfica, fotográfica, acústica (voz) o de cualquier otro tipo, en la medida en que concierna a una persona física identificada o identificable.

Los "datos personales sensibles" son "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular." La Ley dispone que "en particular, se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual". Para obtener y tratar este tipo de datos es necesario contar con el consentimiento expreso de su titular, además de poner a disposición el aviso de privacidad correspondiente.

Como puede apreciarse, la definición de datos personales sensibles, al margen de que pueda estar alineada a documentos internacionales, es jurídicamente desafortunada, pues contiene términos no jurídicos, equívocos y subjetivos, en particular "la esfera más íntima" y el "riesgo grave". Queda para las regulaciones posteriores el reto de conducir estos términos a criterios objetivos y jurídicamente más sólidos.

Por exclusión, desde luego, cualesquiera datos personales que no se consideren sensibles conforme a la definición citada anteriormente se entienden como no sensibles. Para obtener y tratar este tipo de datos no es necesario contar con el consentimiento expreso de su titular, sin perjuicio de la obligación de poner a disposición el aviso de privacidad correspondiente.

En cuanto a la definición de "datos financieros y patrimoniales", la Ley no los define específicament, y tampoco lo hace su Reglamento; simplemente los contempla dentro de los datos que ameritan el consentimiento expreso, y por escrito, si lo pide la ley respectiva, del titular al responsable del tratamiento. En todo caso, podemos decir que se trata de datos que, como su nombre lo indica, conciernen a las finanzas o al patrimonio de un individuo (puede ser, por ejemplo, la información de su cuenta bancaria o

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

de su cuenta de inversión, los datos de su tarjeta de crédito, la información de sus activos patrimoniales, etcétera). Es importante saber que la obtención y/o tratamiento de este tipo de datos también requiere el consentimiento expreso de su titular.

Como dijimos anteriormente, el eje rector de la Ley es el "aviso de privacidad", que es definido como "el documento físico, electrónico o en cualquier otro formato generado por la empresa, que es puesto a disposición del titular de los datos personales, previo a la obtención o tratamiento de sus datos personales".

Otro concepto importante es el término de "tratamiento". En términos legales, "tratamiento" significa cualquier forma de obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

La Ley tutela los llamados derechos (ARCO) a favor de los titulares de los datos: "ARCO" es el acrónimo de los derechos de Acceso, Rectificación, Cancelación y Oposición. Estos son los derechos que tiene cualquier persona física ante un responsable del tratamiento de sus datos personales. El titular de los datos puede solicitar acceso a sus datos; puede solicitar una rectificación de ellos; puede solicitar que se cancelen de la base de datos del responsable si se trata de datos que ya no cumplen con una finalidad, y finalmente, puede oponerse a que el responsable mantenga o trate sus datos, bajo ciertas circunstancias y condiciones previstas en la Ley.

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) es el ente garante de proteger los derechos de los titulares de los datos frente a los responsables o tratantes de sus datos personales. El IFAI tiene facultades de verificación, de oficio o a petición de parte y puede imponer multas en su caso. También tiene la facultad de atender procedimientos administrativos relacionados con derechos ARCO que los particulares ejerzan ante las empresas privadas.

5. *Privacidad bajo Diseño (Privacy by Design)*[139]

Un problema que pueden tener las leyes de privacidad en el mundo es que en muchos aspectos no están diseñadas expresamente para los fenómenos que ocurren en el ambiente digital.

[139] Véase en *http://privacybydesign.ca/about/* (consultada en noviembre de 2011).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

Como una alternativa a ese conflicto que se da por la complejidad y conjunción de jurisdicciones aplicables en el caso del cómputo en la nube, y el flujo de datos que conlleva el mismo, se ha consolidado la "privacidad por diseño" o "bajo diseño".

La privacidad por diseño ha pasado de ser un concepto, a convertirse en un componente esencial de la protección de datos, e indica que los organismos reguladores reconocen la importancia de integrar desde el principio a la privacidad en las nuevas tecnologías y prácticas de negocio.

En virtud de que las legislaciones quedaban rápidamente en obsolescencia, se establece ahora la privacidad bajo diseño.

Así, la creadora Ann Cavoukian en los años noventa, decía: "estaba claro para mí que el tiempo estaba sobre nosotros, cuando la legislación y la regulación ya no serían suficiente para proteger la privacidad. En mi opinión, con la creciente complejidad e interconectividad de las tecnologías de la información, nada menos que la construcción de derecho de privacidad en el diseño del sistema podría ser suficiente".

Así que desarrolló el concepto de privacidad bajo diseño (PBD), para describir la filosofía de la incorporación de privacidad de forma proactiva en la propia tecnología --lo que es el valor por defecto-- "(octubre de 2008).

La privacidad por diseño (*Privacy by Design*) cobró reconocimiento internacional cuando se firmó la resolución en la materia durante la 32a Conferencia Internacional de Comisionados de Protección de Datos y Privacidad en Jerusalén. La resolución pretende ayudar a consolidar la privacidad de la información en el futuro.

El concepto de privacidad por diseño no es nuevo. La doctora Ann Cavoukian, comisionada de Información y Privacidad de Ontario, Canadá, se ha encargado de promocionar la idea desde los años noventa.

El modelo ofrece un enfoque que no busca dar un mayor beneficio a la seguridad en aras de una afectación a la privacidad, o viceversa. En lugar de sacrificar una por la otra, el concepto de privacidad por diseño sugiere que las organizaciones creen sistemas que desde sus etapas iniciales de concepción consideren a ambas, y ofrezcan de esta forma una respuesta proactiva y prescriptiva que esté integrada en el tejido propio de la organización.

La Resolución de Privacidad bajo Diseño busca que:[140]

— Este concepto se convierta en un componente clave de la protección

[140] Para saber más sobre el tema de privacidad por diseño, véase *http://privacybydesign.ca/*, además los 7 principios Fundamentales del PrivacybyDesign, en *http://viepriveeintegree.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf* (consultada en noviembre de 2011).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

de datos personales, al integrarlo a nuevas tecnologías y prácticas de negocio desde el principio, en su concepción original.
— Las organizaciones adopten los principios de Privacidad por Diseño como un medio importante para las operaciones.
— Los comisionados de protección de datos y privacidad promuevan globalmente la Privacidad por Diseño e incorporen sus principios en las futuras políticas y leyes de privacidad en sus jurisdicciones.

En 2011 se llevó a cabo en la ciudad de México la 33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[141], donde las autoridades o comisionados debatieron abiertamente "Privacidad bajo Diseño" y "Cómputo en la nube" al mismo tiempo que discutieron los retos que representa la Era Global en torno al valor y diversidad cultural de la Privacidad y la posibilidad de armonización de los varios sistemas legales por regiones y de manera global.

El concepto elevará la función importante que los profesionales de privacidad asumen en sus organizaciones. También aumentará su participación en las consideraciones operativas iniciales; es decir, aquellas que influyen sobre el rumbo de la organización.

Algunos conceptos complementarios a la noción de "privacidad bajo diseño" *(Privacy by Design)* son privacidad como regla *("Privacy by Default")*, que generalmente suele referirse a la obtención de consentimiento para el tratamiento de datos personales sensibles y privacidad en el desarrollo *("Privacy in Deployment")*, que suele referirse a la divulgación de los mecanismos de privacidad y protección de datos personales a los usuarios, para que estos estén en posibilidad de fijar los parámetros o preferencias que deseen entre un catálogo de alternativas.

6. *El esfuerzo internacional de la armonización de los diversos marcos regulatorios de protección de datos*

Como hemos visto y reiterado durante el curso del presente estudio, la certeza sobre el marco jurídico que rodea a los bienes y servicios de TIC

[141] 33a. Conferencia Internacional de Autoridades de Protección de Datos (33a. CIAPDP) y Privacidad que tendrá lugar los días 31 de octubre al 4 de noviembre de 2011, en la Ciudad de México, en *http://www.privacyconference2011.org/index.php?lang=Esp* (consultada en octubre de 2011). Véase también la Resolución de la Ciudad de México 2011 en *http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/Declaracion_Mexico_ESP.pdf* (consultada en febrero 2012).

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas

Este libro forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx http://biblio.juridicas.unam.mx

—en el caso particular al cómputo en la nube— es fundamental para asegurar una protección efectiva de la información, en particular cuando esta involucra datos personales (y más aún si estos son sensibles).

Actualmente cada país tiene normas y controles de seguridad y privacidad de la información y protección de datos personales que ciertamente suelen ser similares, pero no iguales. Esta circunstancia crea inevitablemente ciertas fricciones contractuales, de cumplimiento normativo, y es susceptible de incrementar los costos de los servicios basados en cómputo en la nube.

Esta desarmonía también es un inhibidor de competencia, en particular para pequeños agentes económicos, que se vean impedidos de participar en un determinado mercado debido a los altos costos de entendimiento de las leyes locales y su interacción con otras leyes extranjeras, que varían en poco o mucha medida de las leyes de su jurisdicción.

Por lo anterior, es previsible que los organismos internacionales de normalización procurarán amainar esta situación, muy probablemente a través de la creación de estándares internacionales de privacidad, o de la inclusión de conjuntos de normas de privacidad en estándares existentes.

Un documento que naturalmente podría recibir como anexo un conjunto de normas de privacidad de este tipo es la serie de normas ISO/IEC 27000, que hoy constituyen un estándar ampliamente aceptado en materia de seguridad de la información.

Este esfuerzo de armonización resultaría sin duda muy beneficioso para el aprovechamiento de los servicios de cómputo en la nube, que podría adoptarse de manera más ágil en la medida en que las contingencias o costos asociados a ellos se vean reducidos con motivo de una importante cooperación internacional.

Es de anticiparse, pues, que muy probablemente en el corto tiempo veremos esfuerzos de normalización internacional para generar controles armonizados de tratamiento de información o de datos personales, que puedan ser reconocidos y adoptados por varios países.

DR © 2013, Universidad Nacional Autónoma de México,
Instituto de Investigaciones Jurídicas