La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo

Mario Casasola Robles (cloudMIDDLEtrust)
María Solange Maqueo Ramírez (CIDE)
Marlon Molina Rodríguez (cloudMIDDLEtrust)
Jimena Moreno González (CIDE)
Miguel Recio Gayo (cloudMIDDLEtrust)

Publicación Auspiciada por Microsoft

Distribución gratuita

Nota del CIDE:

"Las opiniones y datos contenidos en este documento son de la exclusiva responsabilidad de sus autores y no representan el punto de vista del CIDE como institución. Su elaboración corresponde a una de las líneas de investigación de la División de Estudios Jurídicos."

Contenido

Abreviaturas

AMIPCI	Asociación Mexicana de Internet
APF	Administración Pública Federal
Art(s).	Artículo(s)
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DOF	Diario Oficial de la Federación
ECE	Expediente Clínico Electrónico
EDN	Estrategia Digital Nacional
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
INEGI	Instituto Nacional de Estadística y Geografía
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
MIR	Manifestación de Impacto Regulatorio
NIST	Instituto Nacional de Estándares y Tecnología *(National Institute of Standards and Technology)*
OCDE	Organización para la Cooperación y Desarrollo Económicos
Pág(s).	Página(s)
SGDP	Sistema de Gestión de Datos Personales
TIC	Tecnologías de la Información y las Comunicaciones

Resumen ejecutivo

El cómputo en la nube ("cloud computing") es un concepto todavía desconocido por muchas organizaciones, sean éstas de gobierno o privadas, así como quiénes tienen a su cargo su regulación, o, en ocasiones, no entendido realmente, de manera que se pierden oportunidades de ser competitivas e innovadoras. Y la posibilidad del uso personal de la nube es todavía desconocida para muchos individuos como consumidores o ciudadanos digitales, que se podrían beneficiar en su vida diaria de aquélla en aspectos como comunicaciones, acceso a información, etc. Además, es también una oportunidad para el sector público, que gracias al mismo puede ser más eficiente y destinar recursos públicos a otros fines en beneficio de los ciudadanos.

Lograr que el aprovechamiento óptimo del cómputo en la nube sea una realidad requiere medidas que impulsen una rápida adopción o uso del mismo. Y para que ello sea posible es necesario tomar en consideración todos los aspectos, especialmente desde un punto de vista normativo y tecnológico en materia de protección de datos personales, privacidad y seguridad, que sean detonadores del mismo. Entre estos aspectos está el cumplimiento legal el cual en algunos casos puede ser decisivo y en otros simplemente servir de indicativo, de manera que se analicen previamente los requisitos normativos para tomar una decisión al respecto.

El cumplimiento tiene que darse también en materia de seguridad, ya que nos encontramos en un escenario tecnológico caracterizado por ciberataques diarios e intentos de robo de información de manera incesante. Es decir, los proveedores de servicios de cómputo en la nube ponen a disposición de sus usuarios una plataforma de recursos informáticos para que los usuarios puedan administrar sobre ella su información, ya sean datos personales u otra información, sin la que sus clientes podrían continuar su negocio u operativa en caso de que ésta se pierda, sea robada, alterada o afectada de otra manera.

En cuanto a la privacidad, es otro de los detonadores del cómputo en la nube, por lo que requiere de especial atención por todas las partes interesadas ya que es necesario garantizarla y para ello se requieren medidas que estén basadas en buenas prácticas internacionales, entre las que se incluye la autorregulación. La privacidad es también un factor a tomar en consideración, en tanto que puede influir en el desarrollo tecnológico y a, su vez, el desarrollo tecnológico tiene implicaciones sobre cómo entendemos el concepto de privacidad.

Ante un escenario tecnológico que avanza hacia el concepto de servicios ("as-a-service") y que da lugar a nuevos modelos de negocio es necesario considerar si en México se dan los factores necesarios para que el cómputo en la nube pueda ser catalizador de la innovación y la competitividad.

Además, el cómputo en la nube puede suponer una revolución en sectores como la sanidad, impulsando definitivamente el desarrollo del expediente clínico electrónico, y la educación, sin perjuicio de que otros sectores, regulados o no, puedan hacer también uso del mismo con todas las garantías necesarias y, en particular, un alto nivel de protección de los titulares de datos personales.

El sistema al que da lugar el cómputo en la nube implica que se deba prestar atención también a los diferentes actores que participan, o pueden participar, en el mismo. El papel que puedan desempeñar dichos actores o agentes es fundamental para el desarrollo del cómputo en la nube, que se traduce en millones o incluso billones de pesos y que puede situar a México en lo alto de rankings internacionales si se miden los indicadores oportunos.

No obstante, el camino no es fácil y requiere identificar obstáculos, superarlos y ver las oportunidades que ofrece el cómputo en la nube, de manera que el país no se quede rezagado con respecto a otros países o regiones que ya han avanzado. Al respecto, cuestiones como la llamada "soberanía de datos", la privacidad, o un escenario sin garantías que pudieran cuestionar la confianza de los titulares de datos personales u otros problemas que pudieran desincentivar la adopción del cómputo en la nube, tienen que ser tratadas si se quiere hacer un uso eficiente de una tecnología innovadora como lo es el cómputo en la nube.

1. ¿Qué es el cómputo en la nube?

Aunque todavía desconocido o poco entendido por muchas empresas[1], el cómputo en la nube (*"cloud computing"*, en inglés) ya no es un concepto nuevo y se ha convertido en una necesidad para las empresas y Administraciones Públicas que quieren hacer un uso eficiente de las Tecnologías de la Información y las Comunicaciones (en lo sucesivo, TIC).

En cuanto a la definición de cómputo en la nube, ésta puede encontrarse en México en el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[2], que indica que 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 distribuye de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente."*

También, el Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal[3] define, en la fracción V del artículo segundo, el cómputo en la nube como:

> *"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."*

Y de igual manera lo define el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias[4], en la fracción X del artículo 2.

Es decir, el cómputo en la nube permite a cualquier empresa, con independencia de su tamaño y sector de actividad; entidad o dependencia de la Administración Pública o, incluso, persona, acceder desde cualquier lugar, a través de cualquier dispositivo conectado (máquina, tableta, teléfono inteligente u otro dispositivo con conexión) y a cualquier hora, a recursos informáticos (software, infraestructura o plataforma) como un servicio, según las necesidades que se tengan en cada momento.

---

[1] Según una encuesta realizada por ISACA en 2011, el 38% de las empresas entrevistadas no utilizaba ningún servicio de cómputo en la nube. ISACA 2011, *IT Risk/Reward Barometer – Mexico Edition*, citada por Instituto Mexicano para la Competitividad (2012), *"Cómputo en la nube": nuevo detonador para la competitividad de México*. Disponible en el siguiente vínculo electrónico http://imco.org.mx/wp-content/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

[2] Publicado en el Diario Oficial de la Federación de 21 de diciembre de 2011 y disponible en el vínculo electrónico http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

[3] Publicado en el Diario Oficial de la Federación de 6 de septiembre de 2011 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011

[4] Publicado en el Diario Oficial de la Federación de 8 de mayo de 2014 y disponible en el vínculo electrónico http://www.dof.gob.mx/DOFmobile/nota_detalle_popup.php?codigo=5343881

Se trata de una tecnología en constante innovación y desarrollo, por lo que veremos cómo evoluciona hasta alcanzar su máximo potencial durante los próximos años.

Además, la nube supone también la posibilidad de desarrollar nuevos productos y/o servicios (aplicaciones, software, etc.), de manera que se presenta como una oportunidad que debe ser tomada en consideración en la medida en que puede posicionar a México entre las primeras economías digitales[5] a nivel global. Según algunas proyecciones[6], el impacto económico del cómputo en la nube podría ser de trillones de dólares.

La nube es, por tanto, una oportunidad y un reto. Como todo avance tecnológico, se plantean cuestiones que requieren tomar en consideración diversos aspectos, por ejemplo en materia de protección de datos personales, privacidad y seguridad, ya que tales aspectos suelen ser temas de interés de las diferentes partes y ello con independencia de que nos encontremos en un país o territorio que cuenta con normatividad en la materia o en otro con una aproximación diferente, basada en normatividad sectorial y/o auto-regulación.

Como fenómeno global y que implica una revolución tecnológica, cualquier solución a los retos que se plantean tiene que ser considerada en favor de la adopción de las nuevas tecnologías, con una regulación mínima razonable y adecuada a la vista de las buenas prácticas seguidas en derecho comparado y la autorregulación de la industria. Se trata así de no obstaculizar los beneficios que conlleva la innovación, a través de su adopción y uso intensivo.

Los citados aspectos requieren de un correcto entendimiento y en su caso, de la toma de acciones por elaboradores de políticas públicas, autoridades reguladoras y legisladores, entre otras partes interesadas, especialmente cuando México ha previsto que la nube sea una de las líneas de acción a impulsar para conseguir la transformación gubernamental. Y también por lo que se refiere al desarrollo de la economía digital. Se trata, en definitiva, de que México no pierda oportunidades con respecto a países o regiones que ya cuentan con programas para el impulso de la nube y que están trabajando en aspectos o cuestiones regulatorias.

Entre los países o regiones que están impulsando el cómputo en la nube en y desde el sector público, cabe señalar los siguientes ejemplos de estrategias y/o proyectos:

País	Estados Unidos	Unión Europea	Reino Unido	Chile
Iniciativa, estrategia o proyecto	Política pública de "Cloud First" incluida en el 25 Point Implementation Plan to Reform Federal	European Cloud Computing Strategy[8]	G-Cloud Framework[9]	Política y Convenio marco "Cloud"[10]

[5] La economía digital es, además, uno de los cinco objetivos estratégicos de la Estrategia Digital Nacional (EDN) del Gobierno de la República, que fue publicada en noviembre de 2013. Disponible en el vínculo electrónico http://www.presidencia.gob.mx/edn/

[6] Al respecto, véase McKinsey Global Institute (2013), *Disruptive technologies: Advances that will transform life, business, and the global economy*. Disponible, en ingles, en el vínculo electrónico http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx

	Information Technology[7], diciembre de 2010

Es por ello que el presente documento busca analizar algunos de estos aspectos, prestando especial atención a la protección de datos personales, la privacidad y a la seguridad. En particular, aquéllos pueden ser un detonador y un diferenciador que convierta a México en un país altamente competitivo e innovador, por ejemplo, en el desarrollo del expediente clínico electrónico, la educación y otras áreas de la industria que supongan que pueda ofrecer y exportar productos o servicios tecnológicos que garanticen un alto nivel de cumplimiento desde el diseño y por defecto.

Al respecto, las partes interesadas ya mencionadas, tienen un importante papel que desempeñar en el día a día para conseguir que México pueda alcanzar sus objetivos, tanto en el sector público como en el privado, de manera que ellos son, en buena medida, los destinatarios del análisis que se desarrolla a continuación, puesto que pueden incorporarlo, entre otros, a sus medidas legislativas, políticas públicas, planes de desarrollo u otros instrumentos a través de los que se pueda impulsar un uso y desarrollo seguro así como confiable de la nube en México.

[8] Sobre esta estrategia, puede verse más información en el vínculo electrónico https://ec.europa.eu/digital-agenda/node/10565

[9] En relación con este proyecto, puede verse más información en el vínculo electrónico https://www.gov.uk/how-to-use-cloudstore#g-cloud-framework

[10] Al respecto, puede verse más información en el siguiente vínculo electrónico http://www.observatoriodigital.gob.cl/proyectos/politica-y-convenio-marco-cloud

[7] Disponible, en inglés, en el vínculo electrónico https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

2. El cómputo en la nube como una tecnología innovadora

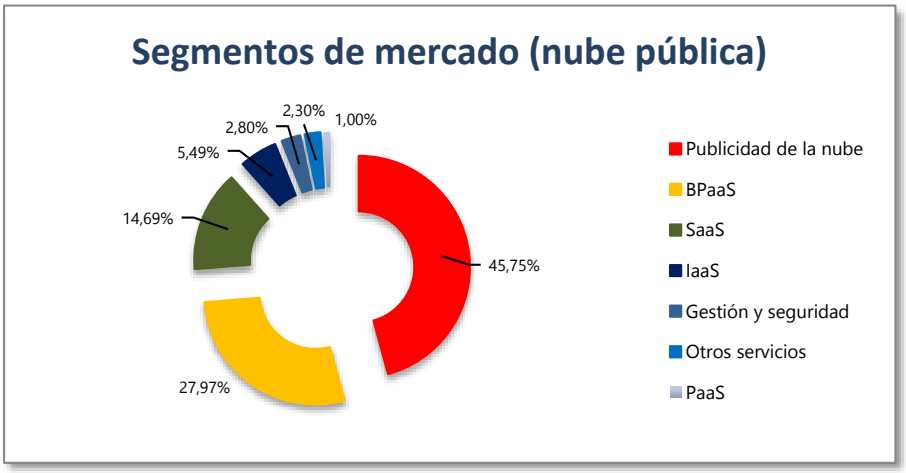
A nivel internacional, Business Software Alliance (BSA) publicó el 2013 BSA Global Cloud Computing Scorecard, en la que compara 24 países alrededor del mundo con base en las principales leyes y regulaciones de estos países, en siete categorías de políticas públicas así como el despliegue de la infraestructura de TIC y la banda ancha. En concreto, México aparece en el puesto 15, por delante de Argentina y Brasil.

Según Gartner[11], el crecimiento de los servicios basados en nube pública, a nivel mundial, seguirá en aumento hasta 2017. Dicho crecimiento aumentará un 17.4% en comparación con 2011 y pasará de 132 billones de dólares que los usuarios invirtieron en 2011 a casi 250 billones de dólares en 2017, incluyendo publicidad. Es así que los servicios de nube pública seguirán creciendo, ya que para 2013 Gartner[12] había pronosticado que lo harían en un 18.5% a nivel mundial, de manera que superarían los 111 billones de dólares alcanzados en 2012.

Siguiendo con las proyecciones de Gartner, en 2013 predecían que desde dicho año hasta 2016, a nivel mundial se invertirán 677 billones de dólares en servicios de nube, lo que supone una media de 169 billones de dólares anuales.

Por otra parte, según un informe de McKinsey Global Institute[13], el impacto económico total del cómputo en la nube podría estar entre 1,7 trillones de dólares y 6,2 trillones de dólares en 2025.

Por segmentos de mercado, según Gartner[14], el primero es el relativo a la publicidad (*"cloud advertising"*), respecto al que predice que desde 2013 hasta 2016 las empresas gastarán un total de 310 billones de dólares en todo el mundo. En segundo lugar se encuentra los servicios de proceso de negocio de cómputo en la nube (*"busines process as a service"*, BPaaS), seguido a su vez por los diferentes modelos de servicio de cómputo en la nube (*Software as a Service*, SaaS; *Infraestructure as a Service*, IaaS y *Platform as a Service*, PaaS) y también por los servicios de gestión y seguridad.



[11] https://www.gartner.com/doc/2642020/forecast-public-cloud-services-worldwide
[12] http://www.gartner.com/newsroom/id/2352816
[13] Disruptive technologies: Advances that will transform life, business, and the global economy.
[14] http://www.gartner.com/newsroom/id/2352816

3. Necesidad de considerar el cómputo en la nube en un contexto global

3.1. Privacidad y seguridad como detonadores de la innovación y competitividad

Desde el punto de vista de la innovación y la competitividad, la privacidad y la seguridad deben ser detonadores de aquéllas, generando la confianza necesaria. Se trata, por tanto, de que la regulación en materia de privacidad y la seguridad permitan el desarrollo de la tecnología, sin que la innovación y la competitividad supongan renunciar a derechos y, en particular, el derecho fundamental a la protección de datos personales.

La privacidad y la seguridad son paradigmas que están en constante evolución, debido entre otros aspectos a que fundamentalmente la tecnología y la sociedad lo hacen igualmente. Es decir, se produce una interrelación que hace que los cambios tecnológicos y sociales influyan en la percepción que tenemos de la protección de datos personales, la privacidad y la seguridad, y de manera inversa, estas tres últimas pueden influenciar en su caso el desarrollo tecnológico y social.

El cómputo en la nube, como una de las tecnologías innovadoras que más atraen la atención de todas las partes, es un claro ejemplo de cómo la protección de datos, la privacidad y la seguridad no pueden ser consideradas como algo estático, sino que deben irse adecuando de manera que estén en equilibrio con los cambios que se producen día a día. Esta circunstancia exige que la seguridad deba ser tomada en consideración en atención al estado de la tecnología, entre otros factores.

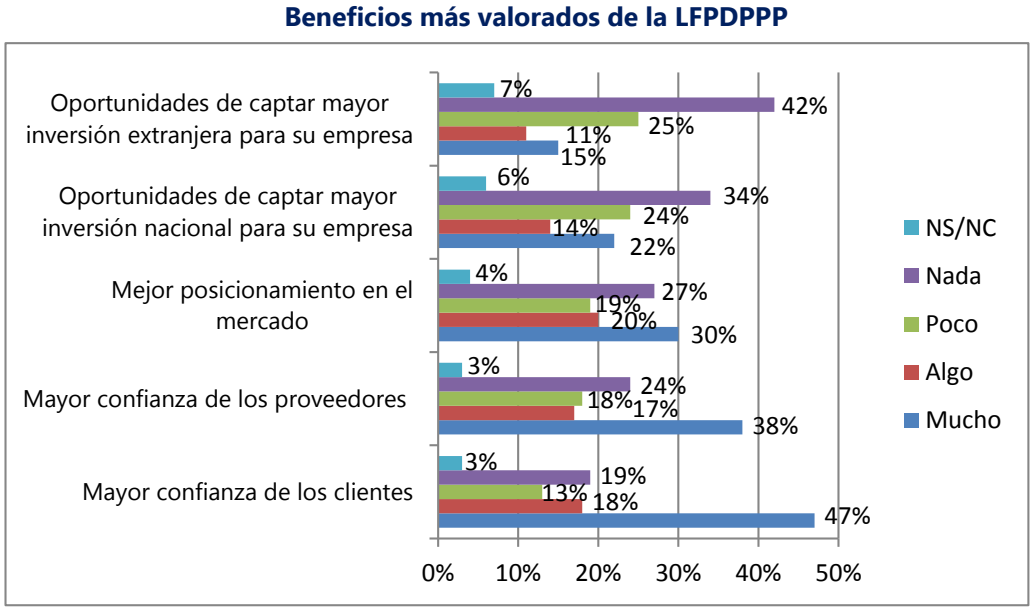
En el caso de México, resulta relevante tomar en consideración la Encuesta Nacional sobre Protección de Datos Personales (2012)[15] que en el apartado relativo a los costos y beneficios de cumplir con la LFPDPPP señala que en promedio, el 29% de los entrevistados (siendo la base de entrevistas un total de 4729) considera que no es difícil cumplir con la LFPDPPP y que entre los beneficios de dicho cumplimiento se encuentran, por una parte, la mayor confianza de los clientes y proveedores y, por otra parte, el mejor posicionamiento de mercado.

En cuanto a los costos de cumplimiento, poniendo foco en este caso en la autorregulación pero sirviendo también para calcular los costos de implementación de un Sistema de Gestión de Datos Personales (SGDP), la Manifestación de Impacto Regulatorio (MIR) expone determinados datos estadísticos con base en los cuales se estima que *"en una micro y pequeña empresa se invertirían un total de 220 horas en instaurar un SGDP, mientras que en una mediana y grande empresa se invertirían 700 horas"*, siendo el 99% micro y pequeñas empresas y el 1% medianas y grandes empresas, de acuerdo con la información estadística del Censo Económico 2009 elaborado por el INEGI. Además, el sueldo promedio por hora de un profesionista, según un estudio de tendencias de empleo profesional realizado en el primer trimestre de 2013 por la Secretaría del Trabajo y

[15] Véase el Reporte de resultados Encuesta en empresas, "Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General", preparado por Ipsos México para la Secretaría de Protección de Datos Personales. Disponible en el siguiente vínculo electrónico http://inicio.ifai.org.mx/EncuestaNacionaldeProteccciondeDatosPersonales2012/02ReporteEmpresas.pdf

Previsión Social , es de $64.6 pesos por lo que *"el monto total de la implementación de un SGDP por unidad económica el cual asciende a $14,212 pesos para las micro y pequeñas empresas y $45,220 para medianas y grandes empresas"*, de manera que *"el costo total de la implementación de un SGDP es de $30,876,866,827 pesos"* considerando el número total de empresas.

Entre los beneficios más valorados de la LFPDPPP, los participantes en la encuesta respondieron lo siguiente[16]:



Fuente: Encuesta Nacional sobre Protección de Datos Personales (2012).

En materia de medidas de seguridad, según la MIR de impacto moderado con análisis de impacto en la competencia, por lo que se refiere al "grupo o industria al que beneficia la regulación" se estima que el número promedio de registros en una base de datos con información personal es de 18,285 aproximadamente y el costo que tendría una vulneración es de $3,770,656 pesos, además del impacto reputacional negativo, de manera que el beneficio unitario de adoptar un esquema de autorregulación es de $4,963,310 pesos y al multiplicarlo por el número efectivo de unidades económicas el beneficio total anual de la regulación sobre parámetros de autorregulación vinculante en protección de datos personales asciende a $10,552,996,039,152 pesos[17].

Destaca que la mayoría de las empresas consideren que la LFPDPPP no supone una oportunidad para captar mayor inversión nacional o extranjera, lo que debería ser tomado en consideración ya que generar confianza a través del cumplimiento de una normatividad sobre protección de datos personales es uno de los factores que puede incrementar el número de clientes, máxime si se piensa en clientes que están establecidos en la Unión Europea o en otras regiones o países que también tienen normatividad en la materia.

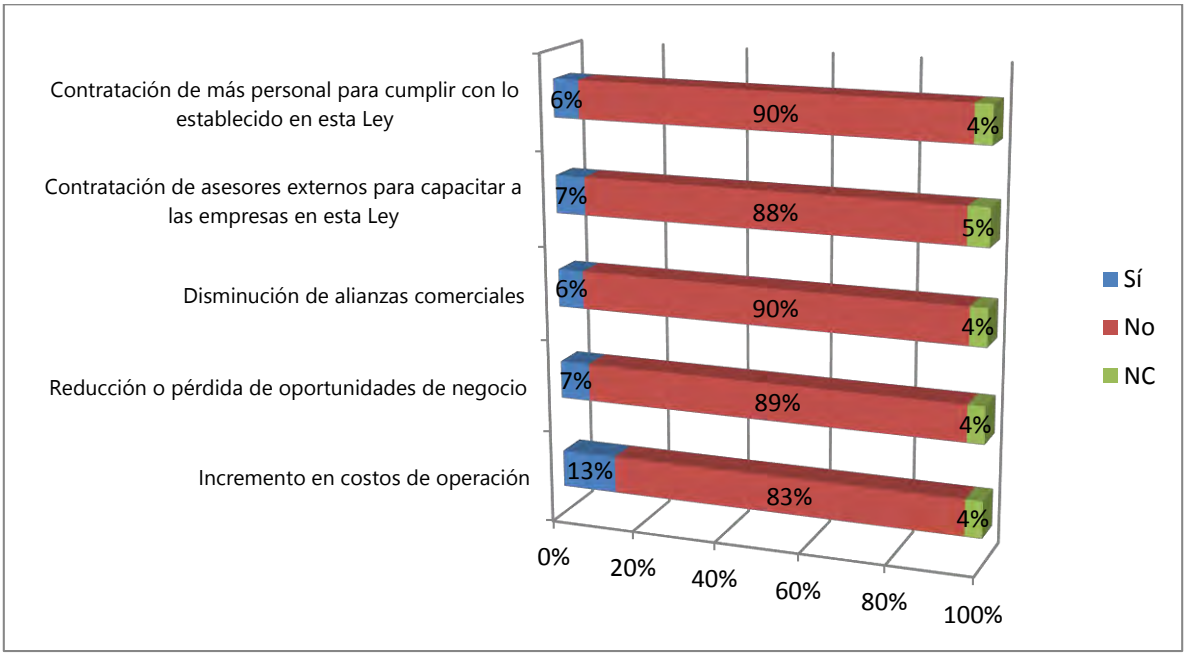
[16] Encuesta Nacional sobre Protección de Datos Personales (2012), pág. 79.

[17] Véase la citada MIR en el vínculo electrónico http://207.248.177.30/mir/formatos/MIR_ImpactoModeradoViewAIC.aspx?SubmitID=408291

Además, cabe señalar que sólo un promedio del 13% de las empresas entrevistadas había incurrido en un incremento de costos de operación como consecuencia de la entrada en vigor de la LFPDPPP. Y de entre este porcentaje, en mayor medida las empresas que han visto incrementado dichos costos de operación son las financieras y de telecomunicaciones.

Es posible, por tanto, afirmar que el cumplimiento de la normatividad sobre protección de datos personales no es una barrera u obstáculo para las empresas mexicanas además de que supone que éstas puedan ser competitivas incluso con las de otros países que también cuentan con normatividad en la materia. En este sentido, la citada encuesta proporciona los siguientes datos[18]:

Proporción de empresas que han incurrido en incremento de costos de operación



Fuente: Encuesta Nacional sobre Protección de Datos Personales (2012).

La protección de datos personales y la privacidad y la seguridad son necesarias para generar la confianza de los consumidores en la nube, el comercio electrónico y el gobierno electrónico, por ejemplo. Al efecto, protección de datos personales y seguridad tienen que estar alineadas con la prestación de servicios, ya sean de comercio electrónico o de gobierno electrónico, en el sentido de que la protección de datos personales no sea una barrera u obstáculo indebido y la seguridad tienen que estar alineada con el negocio ya que de otra manera éste podría llegar a ser inviable.

Por lo que se refiere a la seguridad, el cómputo en la nube implica, como cualquier otra tecnología, independientemente de si la información consta en servidores locales o en la nube, que ésta tenga que ser una prioridad a tomar en consideración. Es así que los usuarios deben adoptar medidas de seguridad sobre la información que tratan y asegurarse, en consecuencia, de contratar servicios en la nube con proveedores que pongan a su disposición medidas de seguridad bajo el más alto estándar disponible en el mercado.

[18] Encuesta Nacional sobre Protección de Datos Personales (2012), pág. 85.

Es decir, la seguridad es una cuestión crítica, máxime en un escenario global en el que el uso de las TIC implica estar expuesto a ciberataques y otros riesgos, de manera que resulta necesario adoptar medidas que sirvan para prevenir y/o, en su caso, corregir brechas de seguridad.

Al respecto, el proveedor de servicios de cómputo en la nube tiene una importante responsabilidad en la materia, de manera que sus servicios tienen que cumplir altos estándares en la materia e implementar procedimientos que permitan ayudar al cliente de sus servicios a cumplir y a no exponer el derecho fundamental a la protección de datos personales de los titulares a riesgos.

El estado de la tecnología y los riesgos comprendidos deben ser factores a tomar en consideración por las partes interesadas, de manera que sirvan como criterios para la adopción de medidas, en el caso de los proveedores de servicios de cómputo en la nube, y la evaluación de dichas medidas, en el caso de los clientes de dichos servicios.

Es así que la adopción de medidas tales como el control de accesos basado en roles (en inglés, *Role Based Access Control*, RBAC), la adopción de medidas para proteger la continuidad de los servicios de cómputo en la nube, la encriptación o cifrado de los datos, el establecimiento de procedimientos de notificación de brechas de seguridad y otras medidas como los sistemas de detección de intrusiones (en inglés, *Intrusive Detection System*, IDS) y los reportes de transparencia, son relevantes a la hora de determinar cómo enfrenta el proveedor de servicios de cómputo en la nube el cumplimiento en la materia.

Es por ello que el cómputo en la nube, como tecnología que puede ser usada tanto por el sector público como el privado, requiere tomar en consideración las implicaciones que tiene tanto en materia de protección de datos personales como de seguridad, siendo una de las mismas el hecho de que el proveedor de servicios de cómputo en la nube actúa, en la mayoría de los casos como encargado del tratamiento, de manera que es necesario que el responsable del tratamiento se informe de, y en su caso verifique a través de los procedimientos correspondientes, cómo dicho encargado del tratamiento cumple con sus obligaciones.

El hecho de que el encargado del tratamiento cumpla con estas obligaciones no significa que el responsable deje de tener responsabilidad, ya que ésta le será exigible en caso de incumplimiento de la normatividad sobre protección de datos personales por aquél.

Dichas obligaciones pueden cumplirse a través de diferentes instrumentos, siendo relevante el hecho de que México, en el caso del sector privado, haya previsto la posibilidad de desarrollar esquemas de autorregulación vinculante. En este sentido, por ejemplo es importante asegurarse que el proveedor cuenta con certificaciones a nivel internacional, tales como la ISO 27001 y clausulado de protección de datos personales consistente con las normas de la Unión Europea, aprobado por las autoridades de protección de datos personales de la Unión Europea en consistencia con la Decisión 2010/87/CE de la Comisión[19], lo que supone que en muchos casos ya no sea necesaria autorización de las autoridades de protección de datos de la Unión Europea para poder transferir datos a países sin nivel adecuado.

[19] Decisión 2010/87/CE de la Comisión de 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, publicada en el Diario Oficial de la Unión Europea L 39, de 12 de febrero de 2010 y disponible en el vínculo electrónico http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010D0087&qid=1397633446891&from=ES

Por tanto, acciones como ésta demuestran el compromiso de determinados proveedores de servicios de cómputo en la nube de cumplir con los requisitos exigidos en diferentes regiones y países alrededor del mundo, además de que hacen importantes inversiones para ofrecer soluciones tales como certificarse en el cumplimiento de estándares internacionales tanto en materia de protección de datos personales como de seguridad.

Estas certificaciones y las soluciones, tanto en materia de protección de datos personales como de seguridad, en las que trabajan algunos proveedores de servicios de cómputo en la nube son una tendencia a tomar en consideración por las autoridades competentes y por el legislador nacional, ya que el nivel de desarrollo del comercio electrónico y el gobierno electrónico, a través del uso de tecnologías como el cómputo en la nube requiere de respuestas que superen esquemas meramente nacionales y estrictamente legislativos.

Esto supone, además, la necesidad de potenciar la colaboración entre la industria y dichas autoridades competentes así como los legisladores, ya que es necesario encontrar un punto de equilibro que permita desarrollar tecnologías que permitan a las empresas ser competitivas y a las Administraciones públicas realizar una gestión eficiente garantizando al mismo tiempo un alto grado de protección de los usuarios y sus ciudadanos[20].

3.2. El cómputo en la nube como diferenciador competitivo

La competitividad se ha convertido en una de las prioridades de muchos países alrededor del mundo en la medida en que es necesario interactuar en un mercado digital global. La posibilidad de exportar productos o servicios, fundamentalmente digitales, así como en su caso proporcionar también servicios de gobierno electrónico, son esenciales si se quiere estar en las primeras posiciones de los diferentes rankings que se elaboran de manera constante. La nube es, sin duda, una oportunidad, junto con otras tecnologías innovadoras.

El cómputo en la nube, principalmente, y otras tecnologías son una oportunidad para alcanzar un diferenciador competitivo tomando en consideración que a nivel global los países buscan día a día hacer un uso eficiente de las mismas que les permitan posicionarse en el nivel más alto de las listas (*"rankings"*) comparativas. De esta manera los países tratan de atraer inversiones y ser competitivos ofreciendo productos o servicios basados en el uso de las TIC.

Por ello es que el sector de las TIC está evolucionando de manera imparable hacia un modelo de servicios (*"as a service"*), siendo incluso la información uno de dichos servicios. Una evolución que da lugar, sin duda alguna, a una revolución que surgida por el uso de las TIC de una forma

[20] Al respecto, por ejemplo Microsoft viene desarrollando desde hace años el concepto de *"Trustworthy Computing"*, prestando especial atención a cuestiones tales como la privacidad desde el diseño (*"privacy by design"*), compromiso o rendición de cuentas (*"accountability"*), ciberseguridad, notificaciones de violaciones de seguridad (*"data breach notification"*) o privacidad en la nube. Vésase su publicacción *Building Global Trust Online Volume 3: Policymaker Guide to Security, Privacy and Safety* disponible en el vínculo electrónico http://www.microsoft.com/en-us/twc/policymakers.aspx

desconocida hasta la fecha, determina que sea necesario replantear cómo nos aproximamos a éstas, lo cual tiene una clara trascendencia económica, jurídica y social[21].

Esta evolución es una oportunidad tanto para las Administraciones Públicas como para las empresas u otras organizaciones, que son los principales usuarios del cómputo en la nube, pero sin olvidar a los profesionistas y a los usuarios de dichas TIC[22]. El cómputo en la nube se traduce en ahorros debido al cambio de modelo de negocio en cuanto al uso de las TIC, de manera que en lugar de necesitar adquirir servidores, máquinas u otros dispositivos, basta con dispositivos que permitan a los usuarios conectarse a Internet para acceder a la nube. Y también, en vez de adquirir software, infraestructura o plataforma, éstos pueden ser utilizados en un modelo bajo demanda, como un servicio más.

Se trata, por tanto, de hacer un uso eficiente de la tecnología, que permita a las empresas (comercio electrónico)[23] ser más competitivas y a las Administraciones Públicas (gobierno electrónico), en los diferentes órdenes de gobierno, ser más eficientes. Dicha competitividad, tanto al interior del país como al exterior en el marco de una economía electrónica interconectada, no puede alcanzarse a cualquier costo sino que depende en gran medida de que el responsable del tratamiento analice previamente con quién está contratando sus servicios. Por ejemplo, un servicio gratuito de cómputo en la nube puede ser desaconsejable si el responsable no desea que el proveedor de cómputo en la nube pueda usar su información personal para efectos publicitarios, o para transmitirla a anunciantes, en la medida en que los servicios y aplicaciones que en apariencia son "gratuitos", en realidad obtienen su pago correspondiente a través del costo y valor de la explotación de información personal.

El cómputo en la nube debe significar que la relación entre el responsable del tratamiento y el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, sea de confianza. Y dicha confianza sólo se alcanza cuando el proveedor de servicios de cómputo en la nube es transparente en relación con los usos que dará a los datos personales comprometiéndose a utilizarlos sólo con el propósito de prestarle al cliente el servicio contratado.

— *Modelos de negocio*

A diferencia de un modelo de negocio que podemos calificar ya como "tradicional", el cómputo en la nube da lugar a un nuevo modelo de negocio basado, por una parte, en el software, la infraestructura y la plataforma "como un servicio" (*"as a service"*) y, por otra parte, en el pago en virtud de los recursos que se consuman (*"pay-as-you-go"*).

La elasticidad de la nube, que permite consumir recursos en virtud de la demanda que una organización, aprovechando las economías de escala, bien sea del sector público o privado, tenga

---

[21] Véase, en inglés, *2013 Microsoft Computing Safety Index*, disponible el vincula electrónico http://www.microsoft.com/security/resources/mcsi.aspx

[22] Al respecto, puede verse, en inglés, el artículo *"Personal technology is changing lives around the world – what we learned from talking to 10,000 people in 10 countries"*, disponible en el vínculo electrónico http://blogs.technet.com/b/microsoft_blog/archive/2014/01/23/personal-technology-is-changing-lives-around-the-world-what-we-learned-from-talking-to-10-000-people-in-10-countries.aspx

[23] En relación con el comercio electrónico en México, puede verse el Estudio de Comercio Electrónico: México 2013, elaborado por la Asociación Mexicana de Internet (AMIPCI). Dicho estudio está disponible en el vínculo de Internet http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=434&Type=1

en cada momento, es ahora uno de los factores que determina el costo que tenga el servicio de cómputo en la nube para el cliente. Dicha posibilidad que, por ejemplo, en el caso del software supone que no sea necesario adquirir la licencia para instalar el software, sino hacer uso del mismo como un servicio (*Software as a Service* -SaaS-), significa que las organizaciones puedan traspasar costos de inversión (Capex) a costos de operación (Opex)[24].

En cuanto a los diferentes modelos de servicio, relativos al software, la plataforma o infraestructura, en el caso de la nube pública es posible hacer referencia a las siguientes definiciones y ejemplos:

Modelo de servicio	Software (SaaS)	Plataforma (PaaS)	Infraestructura (IaaS)
Significado	El proveedor de servicios de cómputo en la nube aloja un programa (software), una aplicación (app), o varios programas y aplicaciones.	El cliente puede desarrollar y correr sus propias aplicaciones de software en la plataforma, las herramientas y el sistema operativo que le proporciona el proveedor de servicios de cómputo en la nube.	El cliente renta recursos computacionales, tales como hardware o máquinas virtuales, en los que despliega y corre su propio sistema operativo y aplicaciones de software.

Y en particular por lo que se refiere al modelo de pago según los recursos que se utilicen (*"pay-as-you-go"*) hay algunas características específicas que definen este modelo frente a uno que puede considerarse ya como "tradicional". Entre dichas características cabe señalar las siguientes:

Cuestión	Modelo tradicional	Modelo "pay-as-you-go"
Hardware	Necesidad de adquirir servidores, máquinas y otro hardware de escritorio	Reducción del hardware y, en su caso, cambio a hardware que facilite la movilidad
Uso y licenciamiento del software	Requiere de instalación y adquisición de licencias	En su mayoría no requiere de instalación y en lugar de adquirir licencia, se renta el software
Elasticidad y escalabilidad	No hay posibilidad de que sea inmediata	Inmediata
Conectividad	Coste fijo y servicio para una oficina (sin movilidad)	Necesidad de servicio para un escenario de movilidad
Otros costos (servidor, luz, etc.)	Costos fijos	Costos variables

Es así que en comparación con un modelo "tradicional", el modelo de pago por uso (*"pay-as-you-go"*) al que da lugar el cómputo en la nube se caracteriza fundamentalmente por las siguientes tres ventajas: 1) bajo demanda; 2) agilidad, flexibilidad y elasticidad, y 3) traspasar costos de inversión (Capex) a costos de operación (Opex).

El cómputo en la nube supone una auténtica revolución para los usuarios ya que permite un nivel de movilidad; acceso a la información desde cualquier lugar, dispositivo y momento así como

[24] Al respecto, véase el apartado relativo a impactos económicos del cómputo en la nube en la publicación del Instituto Mexicano para la Competitividad, *"Cómputo en la nube": nuevo detonador para la competitividad de México*, disponible en el siguiente vínculo electrónico http://imco.org.mx/wp-content/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

trabajo colaborativo que hasta la fecha no eran posibles en la medida en que el cómputo los facilita.

Por último, el cómputo en la nube significa también que las pequeñas empresas puedan competir con las grandes, ya que los diferenciales competitivos que se daban en cuanto al uso tradicional de las tecnologías de la información desaparecen gracias a aquél[25].

— Prácticas de negocio

El cómputo en la nube también es un detonador para nuevas formas de negocio ya que permite el desarrollo de software, aplicaciones (*"apps"*) y toda una serie de servicios relacionados con la nube. Sobre este último aspecto, cabe recordar que, tal y como hemos señalado, en el caso de la nube pública es posible encontrar diferentes nichos o segmentos de mercado que van desde la gestión y la seguridad hasta la publicidad.

Si tenemos en consideración que la nube puede ser considerada todavía como una tecnología emergente, ya que su máximo esplendor, y por tanto el despliegue de todo su potencial, está por llegar, ello supone que las posibilidades de negocio sean innumerables y que, incluso, como señala McKinsey Global Institute, el impacto económico del cómputo en la nube en 2025 pueda llegar a ser de 6,2 trillones de dólares a nivel mundial.

Por ejemplo, la Comisión Europea, en una Comunicación relativa al potencial de la nube en la Unión Europea[26], de la que México es un socio comercial, ha calculado que la nube podría tener un impacto económico de más de nueve (9) billones de euros (957.000 millones de euros) y crear casi cuatro (4) millones de puestos de trabajo en un período de poco más de siete (7) años, desde finales de 2012 hasta 2020.

En el caso de Estados Unidos, en el ámbito del gobierno federal, la estrategia de cómputo en la nube supondría que frente al gasto en tecnologías de la información que anualmente asciende a 80 billones de dólares[27], se pudiera ahorrar hasta un 30% por lo que se refiere al gasto en infraestructura de centros de datos[28].

Lo anterior significa que México debe avanzar en una rápida adopción de la nube, con la finalidad de poder ser competitivo y tomando en consideración que tiene acuerdos comerciales[29] con

[25] En este sentido, puede verse *The Global Information Technology Report 2013, Growth and Jobs in a Hyperconnected World*, elaborado por el Foro Económico Mundial y disponible, en inglés, en el vínculo electrónico http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf

[26] Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM(2012), de 27 de septiembre de 2012. Disponible, en español, en el vínculo electrónico http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF

[27] Véase la cifra en el documento *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service*, de 24 de febrero de 2012. Disponible, en inglés, en el vínculo electrónico https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

[28] Véase la *Federal Cloud Computing Strategy*, de 8 de febrero de 2011, pág. 7. Disponible, en inglés, en el vínculo electrónico http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

[29] Además del Tratado de Libre Comercio de América del Norte (TLCAN), firmado con Canadá y Estados Unidos el 17 de diciembre de 1992, y que entró en vigor el 1 de enero de 1994, México tiene firmado también un

diversos países y potencias económicas, de manera que debe aprovechar las oportunidades que tiene.

— Funcionalidades del producto

La competitividad que puede alcanzarse a través de los servicios de cómputo en la nube depende, en buena medida, de que los usuarios conozcan las funcionalidades y opciones que ofrecen aquéllos.

Para una pequeña empresa las posibilidades que ofrece el cómputo en la nube, tanto por lo que se refiere al acceso a tecnología innovadora como al acceso a la información desde cualquier lugar, dispositivo y en cualquier momento (movilidad), significa que pueda competir incluso con grandes empresas. Por lo tanto, las opciones que ofrecen los servicios de cómputo en la nube y el uso que se haga de las mismas por una empresa, son claves para competir de manera efectiva.

Al respecto, a modo de ejemplo pueden indicarse algunas de las funcionalidades a tomar en consideración en cuanto a servicios de cómputo en la nube enfocados en la productividad de una empresa y que facilitan que ésta pueda ser más eficiente a través del uso de las TIC y, por lo tanto, competitiva:

Funcionalidades de un servicio enfocado a la productividad de la empresa

Funcionalidad	Ventaja	Explicación
1. Sincronización con sistemas operativos móviles	Movilidad y rapidez	Posibilidad de sincronizar, entre otros, correos electrónicos, calendarios y contactos en diferentes dispositivos.
2. Aplicaciones web ("Web Apps")	Movilidad, rapidez y acceso a software o aplicaciones	Posibilidad de acceder a software para edición de documentos, presentaciones, etc., de manera que se facilita la colaboración y se ahorra la distribución de documentos por correo electrónico u otros medios.
3. Sitio web	Comunicación	Hacía clientes y terceros de forma fácil.
4. Videoconferencias	Comunicación	Permite la realización de videoconferencias.
5. Mensajería instantánea	Comunicación	Facilita la comunicación instantánea.
6. Uso compartido de archivos	Colaboración	Permite una mejor distribución de archivos.
7. Equipos sincronizados	Movilidad y colaboración	Facilita la comunicación interna así como la colaboración a través de blogs, wikis, etc.
8. Plataforma social	Comunicación	Ofrece un medio de comunicación social interno.
9. Correo electrónico y calendario	Movilidad y disponibilidad	Ya que es posible el acceso al correo electrónico y a otros servicios desde cualquier lugar.
10. Privacidad	Cumplimiento	Uso de servicios que cumplan y permitan

Acuerdo de asociación económica, concertación política y cooperación ("Acuerdo Global") entre la Comunidad Europea y sus Estados miembros, por una parte, y los Estados Unidos Mexicanos, por otra. El "Acuerdo Global", publicado en el Diario Oficial de la Unión Europea serie L número 276, de 28 de octubre de 2000. En este último acuerdo con la Unión Europea cabe señalar que incluye artículos que hacen referencia a la cooperación entre ésta y México en materia de protección de datos personales y tecnologías de la información, siendo por tanto una oportunidad para México. El texto del acuerdo está disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:276:0045:0061:ES:PDF y puede verse más información sobre el mismo en http://www.bruselas.economia.gob.mx/swb/swb/bruselas/Marco_juridico.

		cumplir con la normatividad aplicable en cada caso.
11. Seguridad	Seguridad	Uso de un servicio de cómputo en la nube que esté certificado conforme a la norma ISO 27001 u otros estándares internacionales.

4. La situación actual en México

4.1. Sector privado: regulación sobre protección de datos personales

Por lo que se refiere al cómputo en la nube en el sector privado, México es uno de los primeros países en haber regulado en su normatividad sobre protección de datos personales. Se trata de una decisión relevante, siendo aconsejable que se revise periódicamente si dicha normatividad responde a la necesidad de facilitar la innovación y garantizar la seguridad jurídica, de manera que ello sirva para atraer inversión y que el país pueda prestar servicios en competencia con otros países.

En particular, por lo que se refiere a la regulación sobre protección de datos personales, México adoptó en 2010 su Ley Federal de Protección de Datos Personales en Posesión de los Particulares[30] (LFPDPPP). A su vez, la Ley ha sido desarrollada por el Reglamento de la Ley Federación de Protección de Datos Personales en Posesión de los Particulares (Reglamento de la LFPDPPP)[31].

Esta normatividad, sin perjuicio de otra que en su caso desarrolla determinados aspectos, es la básica y general en materia de protección de datos personales. Y que sea la normatividad básica y general significa que los principios, deberes y derechos tengan que ser cumplidos por los responsables y encargados del tratamiento, sin perjuicio de que exista normatividad sectorial específica que concrete, en su caso, dicha regulación general.

Normatividad básica sobre protección de datos personales (sector privado)		
Materia	**Norma**	**Publicación en el DOF**
Previsión constitucional	Constitución Política de los Estados Unidos Mexicanos (arts. 16 y 73, fracción XXIX-O).	— Art. 16: DOF de 1 de junio de 2009 — Art. 73: DOF de 30 de abril de 2009
Regula la protección de datos personales	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).	5 de julio de 2010
Desarrolla la LFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.	21 de diciembre de 2011
Medidas compensatorias	Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos.	18 de abril de 2012
Autorregulación vinculante	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[32].	17 de enero de 2013
Aviso de Privacidad	Lineamientos del Aviso de Privacidad.	17 de enero de 2013

[30] Publicada en el Diario Oficial de la Federación de 5 de julio de 2010 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010.

[31] Publicado en el Diario Oficial de la Federación de 21 de diciembre de 2011 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

[32] Dichos Parámetros fueron modificados en virtud de la publicación en el Diario Oficial de la Federación de 16 de julio de 2013.

Medidas de seguridad	Recomendaciones en materia de seguridad de datos personales.	30 de octubre de 2013

Por lo que se refiere a la LFPDPPP, en su tramitación, se tuvieron en consideración los avances tanto normativos como tecnológicos que se estaban produciendo, mientras que en la misma no hay ninguna referencia al cómputo en la nube, el Reglamento sí dedica un artículo a esta materia.

Se trata, por tanto, de una cuestión a tener presente de manera que la tecnología como fenómeno global, en un sentido amplio, pueda desarrollarse en un marco que facilite la innovación al mismo tiempo que garantiza la seguridad jurídica que esperan todas las partes implicadas. Es decir, una combinación de legislación y autorregulación puede ser la base para el desarrollo de servicios, pudiendo ser México un ejemplo al respecto ya que además es un punto medio por lo que se refiere a los modelos que siguen, por una parte, la Unión Europea y, por otra parte, Estados Unidos.

Además, cualquier acción que se lleve a cabo desde el punto de vista de regulación normativa debe ser tomada en consideración a la vista de requisitos tales como la neutralidad tecnológica[33], en un contexto tecnológico claramente marcado a nivel global por la innovación y la evolución hacía un modelo basado en la prestación de servicios, y todo ello con el objetivo último de garantizar un alto grado de protección de los derechos fundamentales, de manera que las diferentes partes que intervengan en un tratamiento de datos personales estén claramente definidas en cuando a su papel y responsabilidades, evitándose así tratamientos ilícitos de datos personales.

Por su parte, el Reglamento de la LFPDPPP dedica un artículo específico al cómputo en la nube, ya que el artículo 52 tiene por objeto regular el tratamiento de datos personales en el denominado cómputo en la nube. Y a dicho artículo nos referiremos en particular al tratar los retos jurídicos del cómputo en la nube en México.

Respecto a dicha normatividad para el sector privado, cabe señalar que se produce una asimetría si lo comparamos con el sector público, ya que mientras que se adoptaba la LFPDPPP quedaba pendiente la reforma de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[34] (en adelante, LFTAIPG) para el sector público y en la actualidad hay diferencias en cuanto al grado de regulación en ambos sectores que pueden llegar a ser críticas para el desarrollo del cómputo en la nube y otras tecnologías actualmente en desarrollo. Por lo tanto, se trata de un aspecto que las autoridades competentes y los legisladores deberían tomar en consideración.

[33] Siguiendo al Dr. Julio Téllez cabe señalar que *"La neutralidad tecnológica radica básicamente en el respeto del principio de igualdad y no discriminación llevado al campo de las TIC; es decir, no establecer preferencias o restricciones a favor o en contra de alguna tecnología o modelo de negocio y garantizar esto mediante reglas, normas y pautas que faciliten la interacción entre sistemas de distintas tecnologías, que permitan el disfrute de los servicios tecnológicos y todo tipo de contenido para los usuarios, sin importar el tipo de tecnologías (dispositivo, formato, sistema, aplicación, etcétera.) que se quiera usar"*. Véase la definición en Lex Cloud Computing: Estudio Jurídico del Cómputo en la Nube en México, pág. 80.

[34] Publicada en el Diario Oficial de la Federación de 11 de junio de 2002 y disponible, con las sucesivas reformas, en el vínculo electrónico http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf

Cabe señalar que dicha normatividad, tanto el artículo 52 del Reglamento de la LFPDPPP como el resto de disposiciones del mismo y de las otras normas que sean aplicables, es la que regula el desarrollo y prestación de servicios de cómputo en la nube en México.

En definitiva, al aprobar la LFPDPPP México se alineó con otros países alrededor del mundo que ya contaban con una normatividad sobre protección de datos personales. No obstante, y a pesar de que en la elaboración de la Ley se tuvieron en consideración el estado de la tecnología y los instrumentos jurídicos adoptados a nivel internacional, sería conveniente que México revise periódicamente si su normatividad responde a la necesidad de facilitar la innovación, la integración económica y comercial de los países, y garantizar la seguridad jurídica, de manera que ello sirva para atraer la inversión necesaria y que el país pueda prestar servicios en competencia con otros países a nivel internacional.

4.2. Sector público: la Estrategia Digital Nacional

En el caso del sector público es necesario tomar en consideración la asimetría que se produce en cuanto a la regulación de la protección de datos personales. Al mismo tiempo, la Estrategia Digital Nacional incluye como líneas de actuación potenciar el cómputo en la nube desde la Administración Pública Federal y también un principio de "soberanía de datos", siendo necesario revisar este último de manera que no se convierta en una barrera que pueda dar lugar a que México quede aislado. Por último, las reformas que México está llevando a cabo, entre las que se encuentran las de telecomunicaciones y transparencia, deben servir de base para un México más competitivo a nivel internacional.

A diferencia del sector privado en donde la competencia legislativa es federal, en el sector público hay que tomar en consideración que en materia de protección de datos personales, hay normatividad federal y estatal debido al reparto de competencias.

No obstante, siendo el cómputo en la nube una tecnología, no debería haber mayor problema en la medida en que es susceptible de ser utilizada por todos los órdenes de gobierno, si bien ello requerirá que no se regule de manera que se creen barreras o prohibiciones indebidas. En su caso, dicha regulación debería ser además acorde con la que resulte aplicable al sector privado, ya que se trata de garantizar la competitividad del país, siendo esta un área en la que el sector público también tiene cierta responsabilidad.

Normatividad básica sobre protección de datos personales (sector público)		
Materia	**Norma**	**Publicación en el DOF**
Previsión constitucional	Constitución Política de los Estados Unidos Mexicanos (art. 6).	20 de julio de 2007 y 7 de febrero de 2014
Regula la protección de datos personales	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.	11 de junio de 2002
Políticas generales y procedimientos para entidades y dependencias de la APF	Lineamientos de Protección de Datos Personales.	30 de septiembre de 2005

Por lo que se refiere a la LFTAIPG, incluye una disposición específica en su artículo 22, relativo a la excepción al consentimiento para proporcionar datos personales a terceros, cuya fracción V indica:

> *"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."*

Es decir, en estos supuestos que dan lugar a una comunicación de datos personales, los terceros podrán tratar los datos personales únicamente para prestar un servicio que implique el acceso a los mismos, si bien queda prohibido el uso de los mismos para cualesquiera otros fines distintos.

Por su parte, el artículo 47 del Reglamento de la LFTAIPG[35] establece que *"los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades deben garantizar 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"*.

Por último, los Lineamientos de Protección de Datos Personales dictados por el IFAI establecen con toda claridad que los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima y solo pueden ser objeto de tratamiento para cumplir con los fines para los cuales se hubieren recabado. Dichos Lineamientos igualmente imponen la obligación a las entidades públicas de estipular en el contrato que se celebre con terceros para la realización del tratamiento de los datos personales, medidas de seguridad y custodia de la información, imponiendo penas convencionales en caso de incumplimientos.

A diferencia de otros países en los que hay una única normativa sobre protección de datos personales, salvando cualesquiera cuestiones específicas aplicables en su caso tanto al sector público como al privado, el hecho de que México tenga una normatividad para el sector privado y otra para el sector público puede crear asimetría y heterogeneidad si el legislador o las autoridades reguladoras, en su caso, según quien tenga competencia, no tienen presentes que tecnología y normatividad son dos caras de la misma moneda cuyo valor se traduce en el índice de competitividad de México y que además dicho índice es medido a nivel internacional ya que vivimos inmersos en una economía digital global.

Tomar en consideración éstos y otros aspectos a la hora de regular o actualizar la normatividad vigente es clave para que México pueda avanzar, tanto a nivel nacional como internacional. Y no debe olvidarse que no se trata simplemente de una cuestión de competitividad para el sector privado, sino que tiene efectos para la economía nacional y también para las propias Administraciones Públicas, en el sentido de que México compite con otros países en materia de gobierno electrónico, siendo el cómputo en la nube uno de los indicadores que deberían estar ya presentes en cualquier evaluación en la materia.

Unido a lo anterior, México cuenta con una Estrategia Digital Nacional (EDN) que incluye cinco objetivos que, a su vez, están ligados a las metas nacionales planteadas en el Plan Nacional de Desarrollo 2013-2018. Los cinco objetivos son los relativos a transformación gubernamental, economía digital, educación de calidad, salud universal y efectiva y seguridad ciudadana.

[35] Disponible en el vínculo electrónico http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf

Estos cinco objetivos estratégicos se basan en cinco habilitadores, que son los de conectividad, inclusión y habilidades digitales, interoperabilidad, marco jurídico y datos abiertos. Además de estos cinco objetivos estratégicos, la EDN incluye otros 23 objetivos secundarios.

Cabe señalar que esta Estrategia Digital Nacional tiene su origen en el Programa para un Gobierno Cercano y Moderno 2013-2018, cuyo principal objetivo es *"atender con oportunidad las demandas ciudadanas y resolver los principales problemas públicos"*, de manera que se busca *"ubicar como eje central de su actuación al ciudadano y utilizar de forma estratégica las herramientas institucionales con las que cuenta para promover un gobierno eficiente, eficaz y que rinda cuentas a la población"*[36].

En concreto, una de las líneas de acción que se plantea en el marco del objetivo secundario relativo a crear una política de TIC sustentable para la Administración Pública Federal, y que a su vez es parte del objetivo estratégico relativo a transformación gubernamental, es la de privilegiar el cómputo en la nube, lo cual supone una clara apuesta tecnológica que, a su vez, permitirá alcanzar otros objetivos tanto a nivel nacional como internacional.

Y la mencionada "Política TIC" fue creada a través del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias[37].

Cabe mencionar que, en virtud de dicha política de TIC, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) que elaboren las entidades y dependencias de la Administración Pública Federal y demás sujetos a los que se refiere el Acuerdo, conforme a lo dispuesto en la fracción I del artículo 5, deberá *"favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, teniendo en consideración la seguridad de la información*".

Sin perjuicio de lo anterior, entre otros aspectos, hay señalar que en virtud de lo previsto en la fracción V del artículo 13 del Acuerdo, las instituciones públicas deberán *"almacenar y administrar en los Centros de Datos que se encuentren* ***en las instalaciones de las Instituciones****, los datos considerados de seguridad nacional, seguridad pública e información reservada y confidencial, conforme a la normatividad aplicable"* (énfasis añadido). Esta referencia a las *"instalaciones de las instituciones"* significa que la información indicada tenga que almacenarse en sitio *("on premise")*, dando así lugar a una situación en la que se atiende a un criterio *"local"*, con independencia de tomar en consideración otros criterios tales como la propiedad de los servidores o el territorio en el que éstos se encuentren.

Además, el citado artículo, en su fracción IV, también indica que si la institución pública no tuviera su propio centro de datos o contratos servicios de centro de datos, deberá analizar el alojamiento en el centro de datos de otra institución de su mismo sector, o en su defecto, en el de otra institución, *"bajo un modelo de cómputo en la nube"*.

[36] El citado Programa fue publicado en el Diario Oficial de la Federación de 30 de agosto de 2013.
[37] Publicado en el Diario Oficial de la Federación de 8 de mayo de 2014 y disponible en el vínculo electrónico http://www.dof.gob.mx/DOFmobile/nota_detalle_popup.php?codigo=5343881

Y finalmente también que, en caso de que se recurriera a contratar servicios de centro de datos en lugar de utilizar un centro de datos propio o compartido con otra institución pública; tomar dicha decisión se debe hacer evaluando el beneficio de los siguientes factores conforme a lo que indica la fracción II del citado artículo 13 del Acuerdo: *"económico, eficiencia, privacidad, seguridad de los datos y de la información"*.

Junto con los servicios de centro de datos, el Acuerdo también incluye previsiones para la contratación de otros servicios, tales como los de correo electrónico o servicios de plataformas de procesamiento de datos.

Específicamente por lo que se refiere a la seguridad de la información, el Acuerdo, en su artículo 28, incluye las disposiciones que deberán observar las instancias de seguridad nacional, estableciendo al respecto tres rangos o niveles de clasificación de información, en atención a la sensibilidad de la misma, siendo la información sobre seguridad nacional la más sensible.

Es necesario recordar que el cómputo en la nube debe ser considerado en un contexto global, por lo que otra de las líneas de acción, la relativa a la soberanía de datos[38], debería ser reconsiderada. La soberanía de datos es un concepto que entra claramente en conflicto con otros principios ya que puede ser utilizada para negar la posibilidad de despliegue de tecnologías de la información o servicios proporcionados por prestadores de servicios extranjeros e incluso es una postura que ha sido rechazada a nivel internacional por países tales como Brasil, que inicialmente la había incluido en su proyecto de Marco Civil de Internet pero que finalmente la ha eliminado[39].

Este principio podría ser contrario al artículo XIV del Acuerdo General sobre el Comercio de Servicios de la Organización Mundial del Comercio (OMC), que se refiere a las excepciones generales y establece lo siguiente[40]:

> *"A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas:*
> *[…]*
> *c) necesarias para lograr la observancia de las leyes y los reglamentos que no sean incompatibles con las disposiciones del presente Acuerdo, con inclusión de los relativos a:*
> *[…]*

[38] Al respecto, el Dr. Julio Téllez, en Lex Cloud Computing: Estudio Jurídico del Cómputo en la Nube en México, indica que *"nuestro marco jurídico debe atender, entre otras cosas" "1. Romper con la idea tradicional de soberanía por cuanto hace a la economía digital y el uso de medios electrónicos y de comunicación, como es Internet y el procesamiento de datos, pues los retos implican una nueva comprensión del fenómeno social y la economía, cosa que el derecho no debe limitar, sino armonizar, para su óptimo desarrollo; la protección de los datos o la información de los usuarios no depende del territorio donde estos residan o estén alojados, son del estándar de privacidad y seguridad bajo el cual están protegidos."* Pág. 99.

[39] Sobre esta cuestión, puede verse la nota de prensa publicada el 19 de marzo de 2014 en The Wall Street Journal, que anunciaba cambios en el proyecto de ley del Marco Civil de Internet con la finalidad de retirar el principio de soberanía de datos. Véase la nota de prensa en el vínculo electrónico http://online.wsj.com/news/articles/SB10001424052702304026304579449730185773914

[40] El citado Acuerdo puede consultarse en http://www.wto.org/spanish/docs_s/legal_s/26-gats.pdf

> *ii) la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales;"*

Y también podría estará en contradicción con los principios del Tratado de Libe Comercio de América del Norte (TLCAN), en particular el principio relativo a eliminar los obstáculos al comercio y facilitar la circulación transfronteriza de bienes y de servicios, entre los que podría entenderse incluido el cómputo en la nube como servicio tecnológico.

Lo anterior no quiere decir que México no adopte las medidas que estime oportunas para garantizar su soberanía, pero en particular el concepto de soberanía de datos, ya sea en el sector público o en el privado, debe ser considerado con especial cuidado, ya que México podría quedarse aislado como país[41] o incluso este concepto podría ser visto como una oportunidad por algunas empresas para no cumplir con la normatividad vigente en la materia[42].

En todo caso, cualesquiera medidas que se adopten al respecto tienen que ser adecuadas y compatibles con el derecho internacional. También, con el desarrollo tecnológico, pudiendo citar en este sentido que Internet y otras tecnologías no deben verse sometidas a barreras nacionales[43] que, en última instancia, pueden suponer una discriminación para los usuarios mexicanos.

E incluso cabría plantear que el principio de soberanía de datos, en el sector privado, supone crear una barrera contraria al principio de libre flujo lógico de los datos personales[44] en el que se basa y garantiza la normatividad sobre protección de datos personales. También, el Convenio 108 del Consejo de Europa[45], de 28 de enero de 1981, o el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC)[46].

En definitiva, se trata de que México se beneficie como país, tanto por lo que se refiere al sector público como al privado, del uso del cómputo en la nube y otras TIC. Dicho beneficio redundará, sin duda, en el crecimiento del gobierno electrónico, en el caso del sector público, y del comercio electrónico, en el caso del sector privado, de manera que los ciudadanos y consumidores

---

[41] Al respecto, puede verse Castro, Daniel, "The False Promise of Data Nationalism", The Information Technology & Innovation Foundation, Diciembre de 2013. Disponible, en inglés, en el vínculo de Internet http://www2.itif.org/2013-false-promise-data-nationalism.pdf

[42] En concreto, la EDN indica que la línea de acción en relación con la soberanía de datos es *"Generar acciones para garantizar la Soberanía de datos, como país, y hacia dentro de las organizaciones."* Pág. 20.

[43] Respecto a Internet, puede verse por ejemplo el NETmundial Multistakeholder Statement, adoptado durante el Global Multistakeholder Meeting on the Future of Internet Governance que tuvo lugar durante los días 23 y 24 de abril de 2014 en Brasil y disponible en el vínculo electrónico http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

[44] En este sentido, debe tomarse en consideración las Recomendaciones de la OCDE sobre la protección de la privacidad y las transferencias internacionales de datos (2013) entre cuyos principios se encuentra el relativo al libre movimiento internacional de datos. Véanse las Recomendaciones, en inglés, en el vínculo de Internet http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[45] Véase el texto, en español, en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

[46] Véase, en español, en el vínculo electrónico https://www.sellosdeconfianza.org.mx/legal/Marco%20de%20privacidad%20APEC.pdf

mexicanos se verán también beneficiados por aspectos tales como el ahorro de costos públicos así como el despegue de aplicaciones y servicios.

Y además, cabe señalar que México inició una serie de reformas constitucionales con la finalidad, entre otros objetivos, de impulsar la competencia, lo que debería traducirse en mejores servicios a los ciudadanos y más oportunidades para éstos.

Entre las reformas constitucionales destacan, por una parte, la reforma constitucional en materia de telecomunicaciones y, por otra parte, la de transparencia, ambas claves para el desarrollo del cómputo en la nube en el país, por lo que a continuación nos referimos a cada una de las mismas.

— Reforma constitucional en materia de telecomunicaciones

En la reforma constitucional en materia de telecomunicaciones y competencia económica[47], adoptada en el marco de los acuerdos políticos del "Pacto por México", el Constituyente Permanente estableció en el artículo 6o., tercer párrafo, que *"[e]l estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios."* En consonancia con lo anterior, en el mismo precepto constitucional, inciso B, fracción I, se adicionó que *"[e]l Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales."*

De tal forma que con esta reforma constitucional se pretenda extender los beneficios de una economía formada por mercados competitivos y garantizar un acceso equitativo a las telecomunicaciones. Como ponen de manifiesto Mariscal y Gil-García (p. 10), con esta reforma constitucional se promete incrementar significativamente el acceso a la banda ancha a través de la construcción de dos redes mayoristas. "Una es la red troncal que utilizará la fibra obscura, hoy propiedad de la Comisión Federal de Electricidad y la otra es una red abierta que proporcionará banca ancha móvil empleando el espectro del dividendo digital. Más aún, se estipula la creación de un nuevo entre regulador con autonomía constitucional que fortalecerá la capacidad reguladora en el sector." Todo lo cual genera las condiciones favorables para fomentar el uso del cómputo en la nube tanto en el sector público como en el sector privado.

— Reforma constitucional en materia de transparencia

Por otra parte, resulta significativo para el tema que nos ocupa, la reforma constitucional en materia de transparencia de 2014 que modifica de nueva cuenta el artículo 6º constitucional[48]. A pesar de adoptar este nombre referido a la transparencia, esta reforma constitucional introduce importantes retos para el derecho a la protección de datos personales en México. Por una parte, modifica el diseño institucional del Órgano Garante del derecho a nivel nacional y federal, así como de sus homólogos en las diversas entidades federativas, para otorgarles autonomía constitucional.

[47] Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la CPEUM, en materia de Telecomunicaciones, publicado en el Diario Oficial de la Federación el 11 de junio de 2013.

[48] Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el Diario Oficial de la Federación el 7 de febrero de 2014.

De igual forma confiere a dicho Órgano Garante nuevas facultades con el objetivo de generar estándares homogéneos para la tutela del derecho a la protección de datos personales, entre las que destacan la facultad de atracción de aquellos recursos de revisión que por su interés y trascendencia nacional así lo ameriten, así como la facultad para revisar las resoluciones de los organismos autónomos especializados en las entidades federativas.

Finalmente, por la parte que a nosotros interesa, se establece la facultad del Congreso de la Unión para emitir una Ley General reglamentaria en materia de protección de datos personales en posesión de los sujetos obligados del sector público para fijar los principios, bases y procedimientos respecto de este derecho (artículo 73, fracción XXIX-S constitucional). A lo cual se añade la necesidad de revisar y, en su caso, reformar las disposiciones normativas vigentes en la materia, incluida la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Artículo Segundo Transitorio del Decreto de reforma constitucional). Todo lo cual tiene por objeto generar estándares homogéneos del derecho a la protección de datos personales, dadas las importantes asimetrías en los niveles de tutela que actualmente se observan entre la Federación y las entidades federativas, a lo cual se añaden las asimetrías entre el sector público y el sector privado.

De tal forma que con esta reforma constitucional, misma que implica un marco jurídico renovado, se establece la oportunidad de adoptar los más altos estándares y las mejores prácticas tanto nacionales como internacionales respecto de los principios rectores de la protección de datos personales, los procedimientos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, los recursos con los que cuentan los titulares del derecho, las medidas de seguridad que adopten tanto los responsables como los encargados de datos personales y los mecanismos necesarios para su efectividad, incluidas las facultades para imponer medidas de apremio y sanciones por el incumplimiento de este derecho.

Aunado a lo anterior, cabe considerar la posibilidad de que México suscriba el llamado Convenio 108, de 28 de enero de 1981, y su Protocolo Adicional para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos, de 2001, todo lo cual redundaría en claros beneficios para el intercambio comercial internacional, que implica la transferencia de datos, con los Estados parte que hasta el momento lo han suscrito (siendo actualmente 43 países en total).

Las recientes reformas constitucionales en materia de telecomunicaciones y transparencia, así como la posición internacional de nuestro país en sus relaciones hacia el exterior en un contexto de economías globalizadas, se constituyen en una clara ventana de oportunidad para adoptar un marco regulatorio robusto que fortalezca el derecho a la protección de los datos personales y, con ello, genere espacios seguros para el intercambio de información. Esto permitiría impulsar los beneficios económicos que suponen las nuevas tecnologías de la información, incluido el uso de la banda ancha y, con ello, el cómputo en la nube, atenuando los riesgos que las mismas suponen en cuanto a la privacidad de las personas. De ahí que la regulación en materia de *cloud computing* se haga indispensable, con mayor razón cuando se trata de un servicio a través del cual se tratan datos personales sensibles, como en el caso de los datos en salud, cuya vulneración o acceso ilegal a este tipo de datos trae aparejada una afectación mayor al individuo.

5. Retos jurídicos y tecnológicos que plantea el cómputo en la nube en México

5.1. Conectividad

El despegue del cómputo en la nube en México, al igual que el de otras tecnologías, depende en buena medida de garantizar una conectividad ubicua y accesible. La banda ancha es, por tanto, fundamental para el desarrollo del gobierno electrónico, en el caso del sector público, y del comercio electrónico, por parte del sector privado. Además, la conectividad permitirá a los mexicanos tener acceso a más y mejores recursos, así como poder ofrecer servicios.

El desarrollo del cómputo en la nube en México, al igual que el de otras tecnologías y en otros países, depende de la capacidad de conectividad.

Al respecto, la conectividad es uno de los cinco habilitadores claves previstos en la Estrategia Digital Nacional (EDN) a través de los que se plantea conseguir los objetivos, tanto primarios como secundarios, contemplados en la misma.

La conectividad implica varias medidas, entre las que se encuentran la ampliación de las redes existentes, el desarrollo de redes y la ampliación del despliegue de una mejor infraestructura así como garantizar dicha conectividad.

Desde un punto de vista jurídico, con la reforma de la Constitución Política de los Estados Unidos Mexicanos en materia de telecomunicaciones[49], se reconoce el **derecho constitucional de acceso a Internet de banda ancha**, garantizando así la conectividad, y el acceso a las tecnologías de la información y comunicación. En concreto, esta garantía constitucional se basa en tres mandatos concretos:

1. La construcción de una robusta red troncal de telecomunicaciones;
2. La instalación de la red compartida de servicios móviles al mayoreo, y
3. La cobertura universal en sitios públicos.

Y desde un punto de vista instrumental, a efecto de hacer efectivo este derecho, el Gobierno Federal ha puesto en marcha el programa México Conectado[50], que busca promover el despliegue de redes telecomunicaciones por todo el país con la finalidad de proveer conectividad en sitios y espacios públicos.

Se trata de esta manera de hacer posible un México próspero e incluyente que deje atrás la brecha digital, siendo buena muestra de ello la posibilidad de que, gracias a la conectividad, los estudiantes podrán acceder a mejores oportunidades educativas y prepararse para un mercado global de trabajo con independencia de su ubicación física.

[49] Ya citado

[50] Sobre dicho proyecto, puede verse más información en el siguiente vínculo electrónico http://www.mexicoconectado.gob.mx

En definitiva, la conectividad es una condición necesaria y fundamental para el desarrollo del cómputo en la nube y otras tecnologías en México. Y gracias al cómputo en la nube será posible, entre otros, desarrollar aplicaciones ("apps") dirigidas a los estudiantes o posibilitar que las escuelas puedan acceder a recursos educativos que se concreten en mejores oportunidades de desarrollo educativo, con lo que ello supone para los futuros profesionistas y líderes del país. De igual forma, en el caso de los centros sanitarios, el cómputo en la nube puede significar la posibilidad de contar con un Expediente Clínico Electrónico (ECE) que sirva para prestar una mejor atención sanitaria, el desarrollo de "apps", o incluso la salud móvil (en inglés, *"mobile health"*, mHealth). Y, en cualquier caso, que México sea competitivo y se posicione entre los países de cabeza en el ámbito de la OCDE u otros foros internacionales.

5.2. Protección de datos personales

El cómputo en la nube, al igual que otras tecnologías, implica tener que revisar esquemas jurídicos pensados para un entorno "tradicional", convirtiéndose así en un nuevo paradigma. Y como tecnología, es necesario que la regulación sobre protección de datos personales responda a los retos que se plantean de manera que se garantice la innovación y la seguridad jurídica necesarias para atraer inversión y proteger el derecho fundamental a la protección de datos personales.

Entre los principales retos jurídicos que se plantean en relación con la nube se encuentra la protección de datos personales, pudiendo señalarse al respecto que es una de las principales cuestiones que se han planteado por diferentes Gobiernos y en diversos foros internacionales[51].

En concreto, la protección de datos personales, tanto por lo que se refiere al cumplimiento como a posibles soluciones, es una de las cuestiones que ha centrado en los últimos años la atención de legisladores, autoridades garantes y reguladoras, foros y elaboradores de políticas públicas. Al respecto, es necesario señalar que México incluso cuenta en su Reglamento de la LFPDPPP con el artículo 52, relativo al tratamiento de datos personales en el denominado cómputo en la nube.

Cabe señalar que México se convirtió así en uno de los primeros países en el mundo, y el primero en Latinoamérica[52], en legislar en esta materia en el sector privado, ya que en el caso del sector público,

---

[51] Al respecto, pueden verse, entre otros, en el caso de Estados Unidos el White Paper del National Institute of Standards and Technology (2012), *Challenging Security Requirements for US Government Cloud Computing Adoption*, disponible, en inglés, en el siguiente vínculo electrónico http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/Challenging_Security_Requirements_for_US_Government_Cloud_Computing_Adoption_v6-WERB-Approved-Novt2012.pdf. También, en el caso de la Unión Europea, puede verse, en el caso del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, el Dictamen 5/2012 sobre la computación en la nube, WP 196, adoptado el 1 de julio de 2012 y disponible en el vínculo electrónico http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf; así como la atención dedicada a esta cuestión por el International Working Group on Data Protection in Telecommunications (2012), *Working Paper on Cloud Computing – Privacy and data protection issues -"Sopot Memorandum"-*, Polonia. Disponible en http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083

[52] En Perú, el Decreto Supremo Nº 003-2013-JUS, por el que se aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales, publicado en el Diario Oficial El Peruano Nº 12399, de 22 de marzo de 2013, se refiere, en su artículo 33, al tratamiento de los datos personales por medios tecnológicos tercerizados. Y en Costa Rica, el artículo 29 del Decreto Ejecutivo Nº.37554-JP, del 30 de octubre de 2012, por el que se

a nivel federal, la figura del encargado del tratamiento no está desarrollada en la LFTAIPG, excepto por lo que se refiere a las previsiones sobre el tratamiento de datos por terceros en los Lineamientos de Protección de Datos Personales[53], si bien se trata de una regulación parcial.

Específicamente por lo que se refiere al artículo 52 del Reglamento de la LFPDPPP, es posible señalar lo siguiente:

1. **Necesidad de que el IFAI expida los Lineamientos sobre cómputo en la nube:** El artículo 52 del Reglamento de la LFPDPPP prevé que el IFAI pueda emitir criterios para el debido tratamiento de datos personales en el cómputo en la nube, de manera que es necesario y urgente que se proceda a desarrollar dichos Lineamientos. Es deseable que los Lineamientos que se emitan atiendan a todos los aspectos que se plantean en relación con el cómputo en la nube y, especialmente, por lo que se refiere al uso que los proveedores de servicios de cómputo en la nube puedan dar a los datos personales a los que tienen acceso para prestar sus servicios así como las prohibiciones aplicables. Se trata de proteger así de manera efectiva el derecho fundamental a la protección de datos personales, de manera que los titulares de los datos personales no vean vulnerado su derecho.

   Es decir, el uso de los datos personales con fines no previstos y que den lugar a un tratamiento que no cumpla con los principios que lo legitimen, implica una infracción de la normatividad sobre protección de datos personales y da lugar también a que pueda haber casos en los que se ofrezcan servicios de computación en la nube de manera anticompetitiva. Una actuación anticompetitiva que, por una parte, podría suponer infringir la normatividad aplicable y, por otra parte debe ser evaluada en términos económicos es un escenario comercial y tecnológico que se basa en el uso de datos personales, como materia prima u "oro", que no puede dar lugar a que las prácticas comerciales puedan ser desarrolladas a cualquier costo para el derecho fundamental a la protección de datos personales, la privacidad y la seguridad.

   Por lo tanto, el IFAI, junto con las autoridades reguladoras correspondientes en su caso, debería tener presente la necesidad de Lineamientos que ayuden a garantizar el derecho fundamental a la protección de datos personales en el caso de los tratamientos de datos personales en el cómputo en la nube, prestando atención a todos los aspectos y retos que se plantean. Entre dichos retos, la minería de datos y el uso de los datos personales con fines de publicidad son cuestiones que deben recibir la máxima atención por la autoridad garante y las autoridades reguladoras.

2. **Tecnología y regulación deben estar alineadas:** Unido a lo anterior, se tome la decisión de legislar o no, es necesario garantizar que ni la evolución tecnológica se haga a cualquier precio, por ejemplo vulnerando derechos fundamentales como el derecho a la protección de

---

aprueba el Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, publicado en El Alcance Nº 42 a La Gaceta Nº 45, de 5 de marzo de 2013, se refiere también a esta cuestión al regular la contratación o subcontratación de servicios del intermediario tecnológico.

[53] Publicados en el Diario Oficial de la Federación de 30 de septiembre de 2005. Puede verse en el siguiente vínculo electrónico http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf. Dichos Lineamientos fueron reformados en virtud de Acuerdo por el que se modifica el Cuadragésimo de los Lineamientos, publicado en el Diario Oficial de la Federación de 17 de julio de 2006 y disponible en el siguiente vínculo electrónico http://www.dof.gob.mx/nota_detalle.php?codigo=4925429&fecha=17/07/2006

datos personales, ni que la legislación suponga un obstáculo a la innovación y la competitividad.

En caso de legislar o regular a través de un instrumento normativo una tecnología como el cómputo en la nube, es necesario también tomar en consideración que la tecnología sigue evolucionando, de manera que la legislación o regulación aplicables deberían hacerlo en consonancia.

Por último, con independencia de la regulación específica que se ha adoptado en el caso de México en el sector privado, también se debe atender al hecho de que la legislación vigente puede estar, en ocasiones, obsoleta bien por ser previa a una nueva tecnología o bien por no haber previsto obviamente la aparición y/o desarrollo de dicha tecnología.

En cualquier caso, que tecnología y legislación estén alineadas, sin que ello signifique que tengan que ser simultáneas, es totalmente necesario.

3. **Necesidad de buscar el equilibrio entre el sector público y el privado:** Como ya se ha señalado, México sí ha regulado el tratamiento de datos personales en el cómputo en la nube para el sector privado, pero dicha regulación puede presentar diferencias en el sector público. Sin perjuicio de lo anterior, es necesario recordar que los principios previstos en la normatividad aplicable y que legitiman el tratamiento de datos personales tienen que observarse en todo tratamiento de datos personales que se lleve a cabo, incluidos aquellos en los que un proveedor de servicios de cómputo en la nube pudiera prestarlos a una entidad o dependencia de la Administración Pública. Además de los principios, los deberes de confidencialidad y medidas de seguridad son también aplicables en el sector público y por lo tanto tienen que observarse en los servicios de cómputo en la nube que sean proporcionados por proveedores a dichas entidades y dependencias. Por último, los artículos 22 de la LFTAIPG y 47 de su Reglamento son claros, de manera que quienes presten algún servicio a las Administraciones Públicas sólo podrán utilizar los datos personales para prestar el servicio correspondiente, pero no para fines distintos.

4. **Cuestiones específicas sobre el artículo 52 del Reglamento de la LFPDPPP:** En relación con el mismo, puede ponerse foco en los siguientes aspectos:

    a. *Se refiere a un supuesto concreto y específico:* Que es en el que el responsable se adhiera a servicios de cómputo en la nube mediante condiciones o cláusulas generales de contratación, prohibiendo expresamente la adhesión "a servicios que no garanticen la debida protección de datos personales".

        Nótese que el citado artículo centra la atención en los requisitos que cumpla y los mecanismos con los que cumpla el proveedor de servicios de cómputo en la nube, con independencia de dónde se encuentre establecido en mismo.

    b. *Prevé que las dependencias reguladoras puedan emitir criterios sobre el tratamiento de datos personales en el cómputo en la nube:* Lo harán en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos[54] (IFAI), por lo

[54] Sobre este Organismo Autónomo, véase http://www.ifai.org.mx

> que, si se emitieran, sería conveniente que se tomarán en consideración todos los aspectos que se plantean en relación con el cómputo en la nube de manera que no se limite de manera indebida el desarrollo de esta tecnología ni la prestación de servicios o el desarrollo de servicios relacionados con la nube.

Dejando ya a un lado el artículo 52 del Reglamento de la LFPDPPP, hay otras cuestiones que también se plantean en materia tratamiento de datos personales en el cómputo en la nube, pudiendo señalar las siguientes:

1. **Necesidad de delimitar claramente las figuras de responsable y encargado del tratamiento:** Prestando de nuevo atención a las definiciones de responsable y encargado del tratamiento proporcionadas por la LFPDPPP[55] y su Reglamento, ya que en el sector público a nivel federal es aconsejable comenzar con la revisión en profundidad las correspondientes definiciones de responsable y encargado del tratamiento en los Lineamientos de Protección de Datos Personales[56], hay que tomar en consideración que dichas figuras, en la práctica, pueden plantear cuestiones como el hecho de que el proveedor de servicios de cómputo en la nube, a pesar de ser considerado como el encargado del tratamiento, determine los medios o ciertas condiciones relativas al tratamiento de los datos personales[57].

   Es importante también considerar que no siempre el proveedor de servicios de cómputo en la nube es un encargado del tratamiento, pudiendo actuar como un responsable del tratamiento más si decide sobre el tratamiento de los datos personales. Es decir, el esquema en el que se considera al proveedor de servicios como encargado del tratamiento es sólo una posibilidad de las varias que pueden darse, por lo que es importante delimitar claramente qué situaciones se producen en la práctica de manera que la partes cumplan con los requisitos y obligaciones que les son exigibles para garantizar así el derecho fundamental a la protección de datos personales.

   En el esquema general en virtud del que se considera al proveedor de servicios de cómputo en la nube como encargado del tratamiento, en ningún caso puede hacer uso de los datos

---

[55] La LFPDPPP define la figura del responsable en la fracción XIV del artículo 3 como *"persona física o moral de carácter privado que decide sobre el tratamiento de datos personales"* y al encargado del tratamiento en la fracción IX del citado artículo como *"la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable."* A su vez, el artículo 49 del Reglamento de la LFPDPPP define la figura del encargado del tratamiento como *"la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio."*

[56] En el Lineamiento tercero, relativo a las definiciones, se define en la fracción IV al responsable como "el servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales" y en la fracción II al encargado del tratamiento como *"el servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales."*

[57] Al respecto, puede verse Butarelli, Giovanni (2012), *Security and privacy regulatory challenges in the Cloud*, Bruselas. Disponible en el vínculo siguiente electrónico https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2012/12-03-21_Cloud_computing_EN.pdf

personales que se le proporcionan ni con una finalidad distinta a la instruida por el responsable ni al margen de las instrucciones proporcionadas por éste[58].

2. **Importancia de tomar en consideración el verdadero valor (económico) de los datos personales y la necesidad de garantizar el derecho fundamental a la protección de datos personales:** El fundamento básico para entender cuál será el foco de atención por parte del proveedor de servicios de cómputo en la nube es su modelo económico ya que en él se sustenta la viabilidad de la operación.

   El negocio de la publicidad en Internet es el que se lleva más del 45% de la cuota de participación del mercado[59], siendo por mucho el más importante actualmente, lo que significa que es el más lucrativo, y como tal requiere de un enfoque importante, por parte de los proveedores de servicios que tienen este mercado como su principal fuente de ingreso, para seguir siendo relevantes y continuar conectando a las empresas con su más potenciales clientes, de forma que la inversión en publicidad tenga un mejor retorno de inversión.

   Es por esto que a la hora de que un proveedor obtiene sus ingresos derivados del análisis meticuloso, aunque anónimo, de los datos de los usuarios este se vuelve más eficiente en "conocer" las necesidades y gustos de los usuarios de forma que la publicidad que ofrece sea más acertada y por lo tanto beneficie al anunciante con más negocio, al usuario con un producto que deseaba y al proveedor del servicio que cobra el servicio de haber realizado esa conexión.

   Esto en pocas palabras significa que los proveedores que tienen el modelo de publicidad como principal fuente de ingreso, centran todos sus esfuerzos en atraer la mayor cantidad de clientes posible para que dejen y transen su información en su nube, de forma que su negocio se vuelva más relevante. Sin embargo, esto no necesariamente es lo que los usuarios están esperando que suceda a la hora de aceptar de manera informada las condiciones del servicio, especialmente que están contribuyendo potencialmente a que un competidor, empresa o producto no deseado se beneficie de sus datos personales.

   Es así que el uso de los datos personales por algunos proveedores de servicios de cómputo en la nube puede no responder a la expectativa de privacidad de los titulares de los datos personales, además de que si se usan sin su consentimiento y vulnerando otros principios de la protección de datos personales, tales como una información clara y fácilmente comprensible, ello determina que dichos proveedores estén haciendo un uso indebido de los mismos, lo que además les reporta una ventaja anticompetitiva[60].

[58] Al respecto, véanse las fracciones I y II del artículo 50 del Reglamento de la LFPDPPP.

[59] Véase el gráfico relativo a los segmentos de mercado en el caso de la nube pública, incluido en el apartado 2 del presente documento.

[60] Sobre la interrelación entre protección de datos personales y derecho de la competencia, en el ámbito europeo, puede vesre la siguiente nota de prensa del Comisario Europeo de Competencia: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm

El hecho de que un servicio sea gratuito para un usuario no avala al proveedor de servicio de forma automática para que haga lo que le plazca con los datos personales[61]. Es decir, hay derechos protegidos por la legislación aplicable que si no son cumplidos por el proveedor puede ser sometido a algún tipo de sanción puntual. El problema se da cuando estas sanciones no se corresponden con la magnitud del negocio que está detrás y por lo tanto para el proveedor del servicio resulta más rentable asumir el costo de la sanción que no utilizar los datos personales con fines que le reportan un mayor beneficio, tales como la minería de datos o la publicidad.

3. **Ámbito de aplicación de la normatividad mexicana sobre protección de datos personales:** Un aspecto importante que se encuentra en el Reglamento de la LFPDPPP, aunque la Ley no dice nada al respecto, es el relativo al ámbito *(extra)*territorial de aplicación del Reglamento, ya que la fracción II del artículo 4 se refiere a la aplicación obligatoria del Reglamento a todo tratamiento de datos personales cuando éste *"sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano."*

   Que el Reglamento sea de aplicación obligatoria supone qué habría que analizar específicamente las obligaciones que tiene que cumplir en este caso el encargado del tratamiento.

   De nuevo, el Reglamento deja claro que el proveedor de servicios de cómputo en la nube puede estar establecido y prestar sus servicios desde cualquier país del mundo si bien la aplicación extraterritorial del Reglamento debe ser analizada de manera específica ya que podría tener importantes efectos. Es decir, podría haber proveedores de servicios de cómputo en la nube que decidiesen no prestar sus servicios a responsables establecidos en México o, en otros casos, habría que ver cómo hará el IFAI o la autoridad reguladora competente en caso de que sea necesario aplicar medidas sobre un encargado del tratamiento establecido en otro país y sobre el que, por tanto, no tiene competencia jurisdiccional[62].

Sin perjuicio de lo anterior, la regulación del tratamiento de datos personales en el cómputo en la nube, por lo que se refiere en particular al sector privado, no se agota con la LFPDPPP y su Reglamento, ya que ésta es la normatividad básica general en la materia, de manera que se debe tomar en consideración otra normatividad que pudiera aplicar sectorialmente, como, por ejemplo, ocurre en el sector sanitario, en el financiero o en el de las telecomunicaciones. Se trata, en cualquier caso, de sectores con una importante dispersión normativa que, en muchas ocasiones, fue aprobada incluso mucho antes de la aplicación de las TIC, hace ya muchos años.

---

[61] Al respecto, puede verse la Resolución R/02882/2013, de 18 de diciembre de 2013, de la Agencia Española de Protección de Datos en el Procedimiento Sancionador Nº PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L., en virtud de la que impone tres sanciones por una suma total de 900,000 euros al declarar ilegal, entre otros, el uso de datos personales sin informar con claridad de que los mismos serán utilizados con fines de publicidad. La citada Resolución está disponible en el vínculo de Internet http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2013/common/pdfs/PS-00345-2013_Resolucion-de-fecha-18-12-2013_Art-ii-culo-15-16-4.5-6-LOPD_Recurrida.pdf

[62] No obstante, habría que ver cómo ejercita el IFAI su atribución en un caso concreto, conforme a la fracción VII del artículo 39 de la LFPDPPP, de *"cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos."*

Además, es necesario tomar en consideración que México participa activamente en diversos foros internacionales; es la segunda economía integrante del Sistema de Reglas de Privacidad Transfronteriza de APEC[63], y sigue, por ejemplo, en el proceso hacia la firma del Convenio 108 del Consejo de Europa. Por lo tanto, es necesario prestar atención también al derecho internacional y a la normativa de otras regiones y países en la materia.

En el caso del sector público, los sujetos obligados también tienen que cumplir con la normatividad sobre protección de datos personales aplicables. Al respecto, cabe señalar que a nivel federal la reforma constitucional en materia de transparencia[64] implica que el Congreso de la Unión emita una ley general "en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados" cuya finalidad es "establecer las bases, principios generales y procedimientos del ejercicio de este derecho".

Esto supone que frente a un esquema actual que, para el caso del sector público, la citada ley general se convierta en una valiosa oportunidad para tratar aspectos que deben servir para proteger el derecho fundamental a la protección de datos personales de los ciudadanos mexicanos así como el acceso a la información pública.

Y unido a lo anterior, la reutilización de información, especialmente cuando ésta es personal, debe ser una cuestión relevante a tratar durante el proceso de reforma que se está produciendo. La reutilización de datos personales que están en posesión de sujetos obligados del sector público debe hacerse con todas las garantías necesarias, debiendo recordar que actualmente el artículo 21 de la LFTAIPG prohíbe la difusión, distribución o comercialización de datos personales, salvo que se obtenga *"el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información"*.

Dichas garantías deben permanecer, ya que de otra manera podrían darse situaciones en las que los datos personales de los ciudadanos pudieran ser utilizados con finalidades no previstas o incluso desconocidas. Y dichas garantías también buscan proteger, en este caso en el sector público, un alto nivel de protección de datos personales que es necesario, máxime cuando México podría llegar a plantear la obtención del nivel adecuado por la Comisión Europea.

Al respecto, se debe tomar en consideración la participación de todas las partes interesadas, especialmente la sociedad civil.

Las organizaciones de la sociedad civil deben ser, por tanto, uno de los actores a los que el Gobierno debe facilitar su participación en diversas acciones que tienen como destinatarias a la sociedad mexicana, de manera que la consulta y participación de las mismas es fundamental. En concreto, acciones que tengan implicaciones en materia de protección de datos personales, acceso

---

[63] Sobre la aceptación de México en dicho sistema, puede verse la nota de prensa del IFAI, de 4 de febrero de 2013, en el vínculo electrónico http://inicio.ifai.org.mx/Comunicados/Comunicado%20IFAI-016-13.pdf Además, en relación con dicho Sistema de Reglas de Privacidad Transfronteriza (Cross-Border Privacy Rules, CBPRs) puede verse también http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

[64] Véase el Decreto por el que se reforman y adicionan disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. Disponible en el vínculo electrónico http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014

a la información pública y uso de las TIC, deben llevarse a cabo con la participación de la sociedad civil como parte interesada.

Como usuarios de servicios de cómputo en la nube, también las Administraciones Públicas tienen que buscar en todo momento velar por los derechos fundamentales, y entre ellos el derecho fundamental a la protección de datos personales.

Nótese que la LFTAIPG, a pesar de incluir algunas previsiones sobre la protección de datos personales, es complementada en la materia a través de unos Lineamientos de Protección de Datos Personales[65] cuyo objeto, según se indica en el Lineamiento primero, es "establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado." Es decir, los Lineamientos son los que, a nivel federal, desarrollan las previsiones de la LFTAIPG en materia de protección de datos personales por los correspondientes sujetos obligados.

En particular, por lo que se refiere a los proveedores de servicios de cómputo en la nube, en el caso de que intervengan como encargados del tratamiento, aplica el Lineamiento vigésimo primero, relativo al tratamiento de datos por terceros. Dicho Lineamiento indica que:

> *"Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia 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."*

El citado Lineamiento aplica a los proveedores de servicios de cómputo en la nube que presten sus servicios a las dependencias y entidades contratantes de la Administración Pública Federal, de manera que en dichos casos habrá que asegurarse de que el correspondiente contrato incluye las previsiones indicadas en el mismo y que son las relativas a medidas de seguridad y custodia tanto establecidas en los Lineamientos como en la normatividad específica que sea aplicable a aquéllas.

Además, el contrato deberá incluir también penas convencionales en caso de que el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, incumpla con sus obligaciones.

Específicamente en el caso de las medidas de seguridad, cabe señalar que los Lineamientos dedican a éstas su Capítulo V, Lineamientos vigésimo séptimo a trigésimo octavo. Una de dichas medidas de seguridad establecidas es la relativa al documento de seguridad (Lineamiento trigésimo tercero) que hace referencia a que *"contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales"*.

Esta obligación de adoptar medidas de seguridad debe tomarse en consideración en el sector público, al igual que ocurre en el sector privado, a la vista de los servicios de cómputo en la nube proporcionados por el correspondiente proveedor. Es decir, el citado proveedor es también un

[65] Desarrollados en virtud de la atribución del IFAI que le confiere la fracción IX, del artículo 37 de la LFTAIPG en cuanto a *"Establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias y entidades"*.

socio estratégico de sus clientes del sector público, por lo que los Lineamientos deben ser tenidos en consideración en el caso de los sujetos obligados a nivel federal.

Y a nivel estatal, habría que tomar en consideración en su caso la normatividad aplicable en la materia, recordando que la competencia en la materia recae en las correspondientes entidades federativas. Esto hace que, en el caso del sector público, sea necesario prestar atención a esta cuestión con el reparto competencial presente.

5.3. Seguridad de la información

La seguridad es otro de los paradigmas que se plantean en relación con la nube y otras tecnologías innovadoras. Resulta claro que "no hay protección de datos personales sin seguridad" y, por lo tanto, es necesario que se tome en consideración la necesidad de que los responsables del tratamiento consideren la seguridad que ofrecen los prestadores de servicios a la hora de contratar servicios de cómputo en la nube.

La seguridad de la información, en general, y de los datos personales, en particular, es otro de los retos que plantea la tecnología y así ocurre con el cómputo en la nube.

En cuanto a lo referente a la seguridad podemos establecer puntos de referencia importantes que nos definan el grado de seguridad que debe tener un sistema para considerarse verdaderamente seguro, esto quiere decir que en teoría el sistema más seguro posible es aquel al cual no se tiene ningún tipo de acceso y por lo tanto el riesgo es cero, pero su usabilidad también es cero por lo que a partir de ese punto y hasta llegar al grado de que el sistema es totalmente accesible y con total usabilidad existen una serie de gradientes donde el balance entre la razonabilidad económica, el nivel de riesgo aceptable, la usabilidad y la seguridad se deben balancear.

El tema de la razonabilidad económica es de un valor determinante, pues las empresas dedicadas a dar servicios en la nube están sometidas a un fuerte nivel de presión en dos sentidos opuestos, uno es la viabilidad económica como empresa y el otro es tener que minimizar el riesgo de problemas en su operación que por definición acarrea costos que ponen en peligro el modelo económico. Es ahí donde hay que poner más atención en cuanto a los modelos económicos de los diferentes proveedores de nube, ya que si en el mismo el uso de la información en su poder supera con creces el beneficio económico de una posible multa o infracción en temas de seguridad, entonces estamos ante un proveedor que si bien puede tomar medidas de seguridad "generales", éstas puedan tener deficiencias en cuanto a los casos de su interés particular comercialmente hablando.

Las tecnologías actuales de seguridad han avanzado mucho desde que en los años setentas se desarrollara el concepto de llave pública y privada y se hicieran públicos los algoritmos asimétricos de encriptación de Diffie, Hellman, Rivest, Shamir y Adleman. Estos protocolos de seguridad han venido avanzado a pasos agigantados siendo cada vez más transparentes para el usuario cotidiano y cada vez más robustos a la hora de resistir ataques informáticos, sin embargo esta arquitectura no está exenta de riesgos ya que, como es habitual, el factor humano en la manipulación de los diferentes elementos puede incurrir en riesgos que comprometen la seguridad de forma parcial o total.

La seguridad de una infraestructura PKI (Infraestructura de clave pública, *Public Key Infraestructure*, por sus siglas en inglés) tiene seis (6) componentes fundamentales:

1. La autoridad de certificación (o, en inglés, CA, *Certificate Authority*): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

2. La autoridad de registro (o, en inglés, RA, *Registration Authority*): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

3. Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, *Certificate Revocation List*) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

4. La autoridad de validación (o, en inglés, VA, *Validation Authority*): es la encargada de comprobar la validez de los certificados digitales.

5. La autoridad de sellado de tiempo (o, en inglés, TSA, *TimeStamp Authority*): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

6. Los usuarios y entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.).

Estos componentes son gestionados por factor humano, con lo que lo primordial es tener implementados los procesos adecuados para su gestión y a través de las certificaciones respectivas poder comprobar que en cada uno de los pasos existen los controles apropiados.

El fundamento de todas las garantías de seguridad se basan en la certificación por parte de terceros que a su vez tienen que rendir cuentas y por lo tanto son responsables de sus acciones, esto genera confianza en el sistema. En ese sentido, para entornos distribuidos como es el caso del cómputo en la nube, es fundamental la figura de un tercero de confianza que permita hacer una monitorización experta de los puntos de control que permitan garantizar que los procesos están funcionando adecuadamente y en el eventual caso de una falla en algún proceso, dar la alerta lo antes posible para poder lanzar diferentes acciones de corrección o mitigación.

En definitiva un buen sistema de seguridad no sólo requiere una excelente tecnología y procesos certificados sino que además requiere participación de un tercero experto que constantemente monitorice el correcto funcionamiento de ambas, de forma que el que recibe el servicio pueda tener confianza bien fundamentada.

Si prestamos de nuevo atención al artículo 52 del Reglamento de la LFPDPPP, uno de los mecanismos con los que debe contar el proveedor de servicios de cómputo en la nube es *"establecer*

y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio."

Por lo que se refiere al deber de medidas de seguridad previstas en la normatividad básica general en protección de datos personales en México, dicho deber se encuentra, aunque menciona únicamente al responsable del tratamiento, en el artículo 19 de la LFPDPPP[66] y desarrollado en su Reglamento.

La LFPDPPP prevé también la obligación del responsable de notificar a los titulares de los datos las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa a sus derechos patrimoniales o morales[67]. A su vez, el Reglamento de la LFPDPPP desarrolla determinados aspectos sobre las vulneraciones de seguridad.

Además, el IFAI, a efectos de la atenuación de las sanciones tal y como se prevé en el artículo 58 del Reglamento de la LFPDPPP, emitió unas Recomendaciones en materia de seguridad de datos personales[68], que basadas en estándares internacionales, sirvan a los responsables y encargados del tratamiento para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

Cabe resaltar que las Recomendaciones son orientativas, sirviendo a los responsables y encargados del tratamiento como un marco de referencia sobre las acciones mínimas a adoptar para garantizar la seguridad de los datos personales. El IFAI podrá tomar en consideración su cumplimiento para atenuar la sanción en caso de se verifique una vulneración a la seguridad de los datos personales.

La referencia al encargado del tratamiento es relevante, ya que al ser considerado como tal, el proveedor de servicios de cómputo en la nube, un aspecto a tomar en consideración por el responsable cuando contrata sus servicios es que aplique medidas de seguridad adecuadas y otro

---

[66] El citado artículo indica que:

> *"Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.*
>
> *Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."*

[67] Este deber se regula en el artículo 20 de la LFPDPPP, que dice así:

> *"**Artículo 20.-** Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos."*

[68] Dichas Recomendaciones fueron publicadas en el Diario Oficial de la Federación de 30 de octubre de 2013 y están disponibles en el siguiente vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013. El IFAI ha publicado, también, una Metodología de Análisis de Riesgo BAA, disponible en el vínculo electrónico http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf y una Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, disponible en el vínculo electrónico http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementacion_SGSDP_marzo2014.pdf.

criterio podría ser también que dicho proveedor de servicios cuente, en su caso, con una certificación, tal como aquellas a las que hacen referencia las Recomendaciones del IFAI.

En el caso del sector público, a nivel federal, la LFTAIPG no prevé medidas de seguridad, si bien los Lineamientos de Protección de Datos Personales[69] dedican su Capítulo V, Lineamientos vigésimo séptimo a trigésimo octavo a la seguridad de los sistemas de datos personales.

Desde el punto de vista del cliente de servicios de cómputo en la nube, a la hora de tomar una decisión sobre la contratación de dichos servicios es fundamental obtener información del prestador de servicios sobre las medidas de seguridad que haya adoptado. Entre otros aspectos a tomar en consideración, el cliente debe atender a si el proveedor de servicios de cómputo en la nube ha adoptado medidas de seguridad; cómo cumple con las mismas; si tiene certificaciones tales como la ISO 27001, así como si ha implementado en su caso las normas recomendadas por el IFAI en sus Recomendaciones en materia de seguridad de datos personales.

En cualquier caso, la máxima "no hay protección de datos sin seguridad" aplica también al cómputo en la nube, siendo además la protección de datos y la seguridad condiciones esenciales para generar la confianza necesaria en la prestación de servicios de cómputo en la nube.

Y unido a lo anterior está la privacidad, ya que una protección efectiva de los usuarios, que permita generar dicha confianza, requiere tomarla en consideración. Es decir, se trata de que los servicios de cómputo en la nube garanticen también la privacidad, siendo éste uno de los retos que se plantean en relación con el cómputo en la nube. Dicha protección de la privacidad debe llevarse a cabo también tomando en consideración como referentes las buenas prácticas y estándares seguidas a nivel internacional.

5.4. Otras cuestiones a considerar

El cómputo en la nube también pone de manifiesto la necesidad de tomar en consideración otros retos que se presentan como consecuencia de la globalización de la tecnología y de la prestación de servicios. Entre dichas cuestiones, cabe prestar atención a las solicitudes de acceso a la información por terceros países, los ciberataques o la portabilidad. En definitiva, se trata de otros retos jurídicos y tecnológicos sobre los que las partes interesadas tienen que colaborar para superarlos.

— Solicitudes de acceso a la información por terceros países

Las solicitudes de acceso a la información no son una cuestión nueva que surja con el cómputo en la nube. No obstante, sí se ha generado un profundo debate, pero quizás debido en buena medida a ciertos acontecimientos relacionados con Estados Unidos y sobre los que la Unión Europea ha incidido en virtud de las negociaciones que lleva a cabo.

En concreto, las solicitudes de acceso a la información son una cuestión en la que los países deben actuar ya que las mismas suponen el ejercicio de potestades que, además, tienen importantes

[69] Ya citados.

implicaciones económicas para los proveedores de servicios de cómputo en la nube y otras tecnologías.

Por ejemplo, en el caso de la Unión Europea se ha apuntado que las solicitudes de acceso a la información por terceros países con fines de cumplimiento legal (en inglés, *"law enforcement"*), sólo deberían atenderse en caso que haya autorización expresa de hacerlo en virtud de un acuerdo internacional o de tratados de asistencia jurídica mutua o de una autorización de la autoridad de supervisión[70].

Se trata de una cuestión delicada en la que los responsables y proveedores de servicios de cómputo en la nube sí requieren que los países busquen soluciones con la finalidad de que aquéllos no puedan llegar a verse sujetos a sanciones por incumplimiento de órdenes que reciban en cuanto a facilitar el acceso a información que pueda encontrarse en sus sistemas.

Por lo tanto, las solicitudes de acceso a la información son otra de las cuestiones a tomar en consideración por los clientes en relación a sus proveedores de servicios de cómputo en la nube[71].

— Ciberataques

Los ciberataques son una de las principales preocupaciones de los proveedores de servicios de cómputo en la nube y sus clientes, ya que todos los usuarios, ya sean del sector público o privado, están expuestos a los mismos.

La ciberseguridad es esencial para el desarrollo de la economía digital. Y por ciberseguridad, siguiendo la definición dada por la fracción X del artículo segundo del Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, se entiende *"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"*[72].

En relación con la ciberseguridad es necesario tomar en consideración, especialmente, el *"Programa para la Seguridad Nacional 2014-2018, Una política multidimensional para México en el siglo XXI"*[73]. En concreto, el programa dedica un apartado específico a la ciberseguridad en el que señala la necesidad de desarrollar una *"política de Estado en materia de ciberseguridad"* debido a que *"quizás la principal vulnerabilidad del país actualmente" es "una acotada cultura de la seguridad de la información"*. Es decir, a pesar de algunas medidas que ya se han adoptado, tales como el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT MX), México estaría rezagado en

---

[70] Al respecto, véase el Dictamen 5/2012 sobre la computación en la nube, adoptado el 1 de julio de 2012, pág. 26. Disponible, en español, en el vínculo electrónico http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

[71] Al respecto, cabe señalar como ejemplo que en el caso de Microsoft elabora semestralmente un informe de solicitudes de acceso (*"Law Enforcement Requests Report"*) y en el segundo semestre de 2013 no hubo solicitudes de acceso a contenido y apenas un pequeño porcentaje que no se referían a datos personales de los usuarios. El informe puede verse en http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

[72] Véase la definición citada en el glosario de la obra de Julio Téllez, Lex Cloud Computing: Estudio Jurídico del Cómputo en la Nube en México, ya citada. Pág. 695.

[73] Este programa fue publicado en el Diario Oficial de la Federación de 30 de abril de 2014.

materia de ciberseguridad lo que implica que sean necesarias medidas para proteger de manera efectiva de la información, ya sean datos personales de personas físicas frente a la suplantación de identidad, fraudes financieros, etc. Y también resguardar la información de entidades públicas y organizaciones del sector privado.

Al respecto, el citado Programa señala que la Administración Pública Federal tendrá entre sus diversas tareas la de desarrollar y actualizar el marco jurídico en materia de seguridad de la iinformación, ciberdefensa y delitos cibernéticos. A tal fin, tomará en consideración los estándares y mejores prácticas internacionales e impulsará los mecanismos de intercambio de información. Asimismo, se deberá tomar en consideración la cooperación internacional, por ejemplo en la forma de instrumentos internacionales de asistencia o ayuda mutua (en inglés, *Mutual Legal Assistance Treaty*, MLAT).

Y en este sentido, México tiene la oportunidad[74] de incorporarse al Convenio del Consejo de Europa sobre el Cibercrimen (Convenio nº 185)[75], con las declaraciones y reservas que estime oportunas. Cabe señalar que dicho Convenio ha sido ya firmado y ratificado por otros países no miembros del Consejo de Europa, como por ejemplo, los Estados Unidos de América[76].

Además, deben ser también una cuestión a tomar en consideración por las autoridades competentes, ya que una caída del servicio puede tener importantes consecuencias. Este riesgo de caída del servicio es un posible escenario para grandes proveedores de servicios de cómputo en la nube[77].

Adoptar medidas para prevenir los ciberataques es necesario, máxime cuando hay infraestructuras críticas o información sensible que proteger. Y al igual que en otras áreas de acción se requiere la colaboración entre los sectores público y privado.

Este y otros riesgos determinan que la seguridad que ofrecen los proveedores de cómputo en la nube tenga que ser tomada en consideración a la vista de tanto de las medidas implementadas como de otras acciones que permitan evaluar riesgos. Al respecto, se debe tomar en consideración si el proveedor de servicios de cómputo en la nube ofrece información sobre análisis geográficos de amenazas cibernéticas, vulnerabilidades y software malicioso ("malware") o qué otras medidas ha adoptado, en su caso, para informar a los clientes sobre amenazas de seguridad.

Y la seguridad no depende sólo de las medidas adoptadas por el proveedor de servicios de computación en la nube, ya que en un escenario en el que todo está conectado electrónicamente, incluso un dispositivo puede ser un punto débil. Por lo tanto, la seguridad también depende del

---

[74] Como nota, cabe señalar que el Consejo de Europa organizó con el Gobierno de México un taller de trabajo sobre legislación en materia de delito cibernético que se llevó a cabo entre los días 31 de Marzo y 2 de Abril de 2014 en México, D.F. Sobre dicho taller puede verse la referencia publicada por el Consejo de Europa en http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

[75] Una traducción al español del citado Convenio puede verse en el vínculo electrónico http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

[76] La lista de Estados miembros y no miembros del Consejo de Europa que han firmado y/o ratificado el Convenio sobre el Cibercrimen puede verse en el vínculo electrónico http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=09/05/2014&CL=ENG

[77] Así lo apunta el *Global Risks 2014*, elaborado por el Foro Económico Mundial. Pág. 39. Disponible, en inglés, en el vínculo electrónico http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

cliente y de las medidas que éste adopte en relación con el dispositivo que utiliza para conectarse y la importancia de que mantenga sus sistemas actualizados.

En definitiva, la seguridad es una cuestión que involucra a todos, de igual manera que ocurre con cualquier otra situación en la vida en la que intervenimos.

— *Portabilidad*

La portabilidad es una de las cuestiones que tienen que garantizarse a los clientes de servicios de cómputo en la nube para garantizar que éstos no queden atrapados (en inglés, "vendor lock in") al mismo tiempo que se garantiza también la continuidad de su negocio.

Básicamente significa que el cliente de servicios de cómputo en la nube pueda recuperarlos en cualquier momento, de manera que como propietario de la información, sin perjuicio de que esté en posesión de datos personales, pueda utilizarlos siendo independiente del proveedor de servicios de cómputo en la nube.

Es decir, se trata de considerar qué medidas facilita el proveedor de servicios de cómputo en la nube al cliente, como poseedor de los datos que van a ser objeto de portabilidad en su caso, asegurando que dicho poseedor conserva todos los derechos, títulos e interés sobre los datos que almacena con dichos servicios.

En definitiva, se trata de que el proveedor de servicios de cómputo en la nube, proporcione al responsable del tratamiento garantías también al momento de finalizar el contrato de servicios, de manera que éste pueda recuperar fácilmente la información y no pierda el control sobre la misma.

6. Hacia nuevos paradigmas de privacidad y seguridad en el cómputo en la nube

6.1. El proveedor de servicios de cómputo en la nube certificado

Los proveedores de servicios de cómputo en la nube también marcan la diferencia entre meros servicios tecnológicos y servicios tecnológicos enfocados a que el responsable del tratamiento encuentre en ellos un aliado que les ayude a garantizar el cumplimiento. La colaboración entre dichos proveedores de servicios y los usuarios de sus servicios es fundamental para garantizar el cumplimiento, debiendo ofrecer el primero información para la toma de decisiones basadas en la misma y el segundo actuar con diligencia cuando contrata servicios de cómputo en la nube.

Contratar servicios de cómputo en la nube, como cualquier otra acción, supone que el responsable tome una decisión sobre el tratamiento de datos personales. Dicha decisión debe basarse en un análisis de las diferentes ofertas y opciones ofrecidas por los proveedores de servicios de cómputo en la nube.

El foco debe ponerse en las garantías que ofrece el proveedor de servicios de cómputo en la nube, ya que el responsable, que está en posesión de los datos personales, pone también uno de sus principales activos estratégicos en manos de quien es contratado para prestarle un servicio. Es así que algunos criterios que el responsable debe considerar a la hora de tomar su decisión sobre la contratación de un proveedor de servicios de cómputo en la nube son:

- Si ha desarrollado sus servicios y/o productos con base en el principio de ***privacidad por diseño***;
- Que ***no utilice los datos personales*** que se tratan o alojan a través de sus servicios y/o productos ***para otros fines*** distintos de la prestación del servicio, tales y como serían, por ejemplo, la minería de datos con fines publicitarios, salvo que se cuente con el consentimiento expreso de los titulares de los datos después de haber sido informados de forma clara y trasparente sobre tales usos;
- Los compromisos, ***cláusulas contractuales y certificaciones*** con las que cuente tanto en materia de protección de datos personales como seguridad;
- Los medios que el proveedor pone a disposición del cliente para informarle sobre diferentes aspectos del servicio y en su caso los cambios que se produzcan.

Se trata de que los servicios ofrecidos por el proveedor de servicios de cómputo en la nube y los requisitos que éste cumple al ofrecer aquellos responden a las expectativas del cliente, de manera que, por una parte, protejan de manera efectiva los datos personales y, en su caso, otra información que suba a la nube y, por otra parte, le permitan cumplir con los requisitos legales o regulatorios que le son exigibles[78].

[78] Como ejemplo, puede verse que Microsoft ha desarrollado un Security TechCenter, disponible en el vínculo electrónico http://technet.microsoft.com/en-us/security/jj554736

Y de entre los aspectos aquí señalados a modo de ejemplo, cabe destacar el hecho de que el proveedor de servicios de cómputo en la nube, ya sea como encargado del tratamiento o incluso como un nuevo responsable del tratamiento, no pueda tratar los datos personales para otros fines que no sean los autorizados de manera expresa. Es así que en caso de ser un encargado del tratamiento incumpliría con sus obligaciones como tal y si fuera un nuevo responsable del tratamiento, tendría que obtener en su caso el consentimiento necesario, que debería ser expreso en este supuesto concreto, además de cumplir con el resto de principios aplicables al tratamiento de datos personales.

Es decir, se trata de que el consentimiento, como uno de los principios que legitima el tratamiento de datos personales, responda a las necesidades que se plantean en el entorno electrónico pero que también sea una garantía cuando un responsable trata datos personales con finalidades que no son necesarias o primarias, de manera que sea una verdadera garantía para el titular de los datos personales frente a modelos de negocio que pueden explotar puntos débiles o basarse en una reducción de costos que tienen un impacto en la privacidad de dichos titulares de datos personales, tales como la minería de datos con fines no previstos inicialmente, los fines mercadotécnicos, publicitarios o de prospección comercial[79], o el uso de dichos datos personales para otros servicios[80].

Es decir, se suele tratar de modelos de negocio que aparentemente ofrecen servicios a precio muy bajo o incluso de manera "gratuita", pero que en realidad explotan el valor económico de los datos personales, que se han convertido en la materia prima y uno de los activos más valiosos así como estratégicos de muchas empresas.

Por ejemplo, el uso de datos personales que un cliente, como responsable, entrega al proveedor de servicios de cómputo en la nube, como encargado del tratamiento, con fines de publicidad por este último resulta un incumplimiento tanto de las obligaciones que le son exigibles como de la normatividad sobre protección de datos personales, ya que se requiere del consentimiento a tal fin. Incluso sería posible tomar en consideración la conveniencia de exigir un consentimiento expreso en el caso de uso de los datos personales por un proveedor de servicios de cómputo en la nube cuando actúa por su cuenta, de manera que se desincentive claramente posibles abusos por el mismo.

Situaciones como las apuntadas, demuestran que el esquema actual del consentimiento, como principio que legítima el tratamiento de datos personales, no es suficiente y debe ser revisado de manera que responda de manera efectiva a la necesidad de protección de los usuarios. Más que nunca, es necesario que el principio de consentimiento sea puesto en relación con los principios de información y, sobre todo, el de finalidad del tratamiento de los datos personales. Un uso de los datos personales que no sea claramente informado ni sobre el que se dé una clara oportunidad de oponerse al mismo, puede llevar a la necesidad de plantear un consentimiento basado en el consentimiento expreso para determinados usos o finalidades. Y al respecto, las autoridades garantes en materia de protección de datos deben analizar esta cuestión de manera específica, así como otras partes interesadas que puedan aportar soluciones adecuadas para un entorno tecnológico y en constante evolución.

---

[79] Además de la normatividad sobre protección de datos personales, debería tomarse también en consideración la normatividad específica aplicable, tal y como señala el artículo 30 del Reglamento de la LFPDPPP con la finalidad de proteger a los titulares de datos personales.

[80] En el caso de finalidades distintas, véase también el artículo 43 del Reglamento de la LFPDPPP.

En la medida en que el proveedor de servicios de cómputo en la nube sea un encargado del tratamiento no podrá tratar, en ningún caso, los datos personales que se la han proporcionado para prestar el servicio correspondiente con otra finalidad, ya que incumpliría con sus obligaciones y vulneraría el derecho fundamental a la protección de datos de los correspondientes titulares de los datos personales. El encargado del tratamiento tiene que limitarse así a prestar los correspondientes servicios de cómputo en la nube a su cliente, sin poder utilizar los datos personales que se le han confiado para ninguna finalidad ya que no puede decidir sobre el tratamiento de los mismos. Utilizarlos para enviar publicidad o proporcionarlos a un tercero para que a su vez envíe dicha publicidad es reprochable y probablemente ilícito.

Como encargado del tratamiento, en el sector privado, éste incumpliría sus obligaciones en caso de que tratase los datos personales que le proporciona el cliente con finalidades que no sean las instruidas por el responsable del tratamiento (art. 50 del Reglamento de la LFPDPPP).

Y en el sector público, es necesario recordar que entre los principios que legitiman el tratamiento de datos personales, en virtud del artículo 20 de la LFTAIPG, se encuentra en su fracción III el relativo a que los datos personales sólo se podrán tratar *"cuando éstos sean adecuados pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido."* Además, los Lineamientos de Protección de Datos Personales indican en el segundo párrafo del Lineamiento, relativo al principio de licitud, que *"los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad deberá ser determinada y legítima."*

También, los Lineamientos de Protección de Datos de Personales imponen a dicho encargado un deber de custodia que implica que no puedan ser revelados a terceros (Lineamiento vigésimo primero). En uno y otro caso, el encargado del tratamiento no puede tratar los datos personales fuera de la relación jurídica que le vincula con el responsable del tratamiento, incurriendo en responsabilidad en caso de que lo haga, además de que supondría una clara vulneración del derecho fundamental a la protección de datos personales.

Incluso desde el punto de vista de quien actúe como responsable del tratamiento, el uso de los datos personales con fines secundarios requerirá del consentimiento, que tendrá que ser válido con lo que ello implica en cuanto a que sea específico para una concreta finalidad. De no ser así, el tratamiento de los datos personales sería de nuevo ilícito, pudiendo incurrir en infracción de la normatividad sobre protección de datos personales tanto el cliente de los servicios de cómputo en la nube como el proveedor de servicios de cómputo en la nube, asumiendo que este último actuase en este caso concreto como responsable del tratamiento.

Es decir, frente al consentimiento conocido como *"opt-out"* y que implica que se considere que el tratamiento de los datos personales puedan ser tratados salvo que el interesado diga lo contrario, en determinadas circunstancias es necesario un consentimiento *"opt-in"*, con la finalidad de obtener las máximas garantías de manera que el titular de los datos personales no vea infringido su derecho por situaciones en las que podría producirse una falta de transparencia, en cuanto a la información que necesita para tomar una decisión sobre el tratamiento de sus datos personales, o incluso del consentimiento necesario[81].

[81] Sobre esta cuestión, puede verse el Dictamen de la LFPDPP, pág. 30. Disponible en el vínculo de Internet http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf

El proveedor de servicios de cómputo en la nube se convierte en un socio estratégico ya que, por ejemplo, en el caso de pequeñas empresas, éstas no podrían tener acceso a una tecnología que les permite competir con grandes empresas y sin fronteras[82].

En cualquier caso, la necesidad de que el proveedor de servicios de cómputo en la nube cumpla con altos estándares regulatorios y normativos, jurídicos y tecnológicos, tanto en materia de protección de datos personales como de seguridad y privacidad, implica que los clientes deban tener presentes qué certificaciones ha obtenido en su caso dicho proveedor. En este caso un ejemplo válido puede ser la certificación en la familia de Estándares ISO/IEC 27000, la ISO/IEC 20000 o la Norma ISO/IEC 19770.

También, en el caso específico del sector público, es necesario tomar en consideración normas como la ISO 18091:2014 Sistemas de Gestión de la Calidad – Directrices para la aplicación de la norma ISO 9001:2008 en el gobierno local.

Y, en particular, debe tomarse en consideración la ISO/IEC DIS 27018 – Information technology – Security techniques – Code of practice for PII protection in public clouds acting as PII processors[83], que si bien todavía se encuentra en desarrollo, proporcionará un código de prácticas para el control de la protección de datos personales para servicios de nube pública.

La certificación es además un valor agregado en el sentido de que demuestra el compromiso del proveedor de servicios de cómputo en la nube, que no se limita a cumplir cláusulas contractuales con su cliente, y es también una forma de estandarizar el cumplimiento más allá de un esquema normativo nacional. Es decir, las prácticas seguidas por el proveedor de servicios de cómputo en la nube certificado deben ser consideradas como la base para cumplir un elevado nivel de protección de datos personales y seguridad en diferentes jurisdicciones.

También el hecho de que el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, busque soluciones en sus prácticas de negocio y funcionalidad de producto y/o servicio ofrecido que faciliten el cumplimiento en materia de protección de datos personales, significa que se trata de un proveedor proactivo comprometido con sus clientes y con las autoridades reguladoras competentes.

Por último, el proveedor de servicios de cómputo en la nube debe comprometerse también con sus clientes ayudándoles a conocer sus servicios y las condiciones que se prestan los mismos. En el caso de pequeñas y medianas empresas esto puede ayudarles también a cumplir con sus obligaciones, de manera que el proveedor debe ser transparente y guiar al cliente. Al ser transparente y guiar al

---

[82] Véase Gutiérrez, Horacio E. y Korn, Daniel, F*acilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America*, University of Miami School of Law, 2014. El artículo está disponible, en inglés, en http://inter-american-law-review.law.miami.edu/wp-content/uploads/2014/03/Facilitando-the-Cloud.pdf

[83] Sobre este estándar, puede verse la presentación disponible en http://www.eurocloudcongress.org/wp-content/uploads/2013/09/14.20-ebrc-e%C3%8Aurocloud-2013-presentation-ebrc.pdf así como http://dataprotection.gov.mu/English/Documents/Workshop/Wrkshop19feb14/Cloud%20n%20Privacy%20MS%20Approach%20-%202nd%20presentation.pdf

cliente se facilita también que el cliente pueda tomar una decisión informada sobre la contratación de servicios de cómputo en la nube[84].

— Transparencia

Que el proveedor de servicios de cómputo en la nube sea transparente es fundamental para que el cliente de sus servicios pueda conocer los términos que gobiernan éstos.

En particular, es importante que los clientes puedan conocer cómo el proveedor de servicios de cómputo en la nube cumple en materia de protección de datos personales y seguridad.

Es así que la información que se proporciona al cliente es la base para que éste pueda tomar una decisión sobre la contratación de un producto o servicio, de manera que la misma debería ser clara, fácilmente comprensible y completa.

La transparencia también significa que el proveedor de servicios de cómputo en la nube proporcione información que es fundamental para el desarrollo del contrato, como por ejemplo el hecho de que el cliente, como responsable del tratamiento, pueda saber dónde residen los datos personales que son objeto de tratamiento, quién y en qué casos puede acceder a los datos personales o información sobre el método establecido para informar sobre cambios que se produzcan en relación con el tratamiento de los datos personales.

Se trata, por lo tanto, de que el cliente pueda acceder a la información necesaria para poder tomar en cada momento la decisión correspondiente. De nuevo, es necesario insistir en que el proveedor de servicios de cómputo en la nube debe ser un socio estratégico de negocio, cumpliendo así con un papel fundamental a la hora de impulsar la competitividad de las empresas y la eficiencia de las entidades y dependencias gubernamentales.

— Guiar al cliente

En el proceso de toma de decisión por el cliente sobre la contratación, y también durante el tiempo en que un determinado producto o servicio haya sido contratado, es necesario que el proveedor de servicios de cómputo en la nube guíe al cliente de manera que pueda acceder, u obtener, la información que es necesaria al respecto.

Una muestra del compromiso del proveedor de servicios de cómputo en la nube, al igual que en otros casos de contratación de productos o servicios tecnológicos en particular, es la adopción de medidas que sirvan a los clientes para encontrar fácilmente la información[85] sobre la configuración de determinados parámetros relativos a la protección de datos personales, medidas de seguridad u otros requisitos a tomar en consideración en el uso de los servicios de cómputo en la nube; así

---

[84] Al respecto, puede verse también el documento publicado por Microsoft titulado *Protecting Data and Privacy in the Cloud*, disponible en inglés en el siguiente vínculo electrónico http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf

[85] Al respecto, en el caso de Microsoft, pueden verse el Centro de Confianza de Office 365 (disponible en http://office.microsoft.com/es-es/business/centro-de-confianza-office-365-seguridad-informatica-FX103030390.aspx); de Azure (disponible en http://azure.microsoft.com/es-es/support/trust-center/) o de Microsoft Dynamics CRM (disponible en http://www.microsoft.com/es-es/dynamics/crm-trust-center.aspx).

como sobre el cumplimiento y las herramientas e información que el proveedor de servicios de cómputo en la nube pone a disposición del usuario de dichos servicios. Se trata, por tanto, de que el encargado del tratamiento colabore activamente con el responsable para garantizar el cumplimiento o, en su caso, para que este pueda saber cómo el encargado del tratamiento cumple con los requisitos exigibles.

Al respecto, el hecho de que el proveedor de servicios de cómputo en la nube esté certificado, por ejemplo en materia de seguridad de la información conforme a la norma ISO 27001, debe ser tomado también en consideración a la hora de ayudar al usuario de los servicios de manera que sus decisiones puedan tomarse con base en dicha información.

Sin perjuicio de las acciones que lleve a cabo el proveedor de servicios de cómputo en la nube, el usuario de sus servicios, como responsable del tratamiento, también tiene un deber de diligencia de manera que debe adoptar una posición activa a la hora de solicitar y obtener información de aquél. Y una vez más el usuario y el proveedor de servicios de cómputo en la nube deben verse como socios estratégicos, entre cuyos objetivos comunes está ofrecer y utilizar, respectivamente, servicios que les permitan ser competitivos.

Por lo tanto, ofrecer información específica, clara, completa y actualizada sobre cómo el proveedor de servicios de cómputo en la nube cumple en materia de protección de datos personales y medidas de seguridad, así como las opciones que pone a disposición del usuario de sus servicios para que, a su vez, pueda cumplir, determinan que ambos colaboren para garantizar dicho cumplimiento, sin perjuicio de que la responsabilidad última sea del cliente como responsable del tratamiento de datos personales y sin que pueda transferir dicha responsabilidad al encargado del tratamiento.

6.2. El tercero de confianza

Se trata de una figura ampliamente extendida aunque en buena medida desconocida ya que quizás en pocas ocasiones se toma en consideración las funciones que puede desempeñar. En el ámbito de los servicios de cómputo en la nube, el tercero de confianza puede ser una parte relevante a la hora de acelerar la adopción de dichos servicios, ya que su papel puede ser el de auditar determinados aspectos y prestar otros servicios que generen confianza para todas las partes.

La figura del tercero de confianza puede desempeñar, y de hecho está desempeñando ya en algunos casos, un papel importante en el avance de la adopción del cómputo en la nube. Entre otros servicios, el tercero de confianza proporciona servicios de control externo de la calidad de los servicios de cómputo en la nube de un proveedor, puede certificar o auditar determinados aspectos de los servicios o del cumplimiento por dicho proveedor e incluso puede ofrecer otros servicios que redunden en beneficio de las partes interesadas.

Estos terceros de confianza, en relación con el cómputo en la nube, son uno de los actores que forman parte del ecosistema a que dan lugar la gestión de los servicios, la seguridad y el cumplimiento normativo y regulatorio en protección de datos personales.

Es así que el tercero de confianza se convierte en un agente que dinamiza la contratación y prestación de servicios de cómputo en la nube, convirtiéndose también en una posibilidad de

negocio relacionado con el cómputo en la nube. Y dicho tercero puede ser tanto tecnológico como jurídico o, en ocasiones, una combinación de ambos.

La posibilidad de recurrir al tercero de confianza en la prestación de servicios de cómputo en la nube puede servir también para acreditar el cumplimiento, de manera que dicho tercero desempeñaría el papel de auditor externo, en unos casos, o tercero en el que las partes confían, en otros casos.

Un ejemplo de tercero de confianza en materia de cómputo en la nube es el de la certificación ofrecida por Cloud Security Alliance (CSA)[86], que cuenta con una matriz de controles aplicables a la nube[87]. Cuando el usuario final confía a su vez en la certificación ofrecida y en que dicha acreditación se ha realizado siguiendo estándares de mercado, entonces tanto el cliente como el proveedor reconocen al tercero y a sus servicios, generando la confianza necesaria para que el intercambio comercial se produzca.

Además de la certificación de servicios de cómputo en la nube, cada vez más surgen certificados dirigidos a personas, que prestan servicios relacionados con el cómputo en la nube. Y dichas certificaciones requieren incluir también conocimientos y habilidades en diversas materias, entre ellas la protección de datos personales y la seguridad.

Cabe señalar que la certificación en materia de cómputo en la nube está en pleno desarrollo, siendo buena muestra de ello que se estén preparando varias normas internacionales, tales como la ISO/IEC 17788 *Tecnología de la Información. Servicios y plataformas para aplicaciones distribuidas. Computación en la nube. Generalidades y vocabulario* o la ISO/IEC 17789 *Tecnologías de la Información. Computación en la nube. Arquitectura de referencia*.

Por tanto, proporcionar confianza a través de diferentes servicios que inciden a su vez en los servicios de cómputo en la nube se convierte también en una oportunidad para muchos profesionistas, que debe ser tomada en consideración en la medida en que son servicios que pueden proveerse tanto a nivel nacional como internacional.

[86] Sobre esta organización, puede verse más información en el vínculo electrónico https://cloudsecurityalliance.org/

[87] Se trata de la *Cloud Controls Matrix*, disponible, en inglés, en el vínculo electrónico https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

7. Oportunidades que ofrece el cómputo en la nube: Algunos casos de ejemplo

El nivel de dependencia de la tecnología en la empresa es tal que se hoy representa un alto porcentaje de sus proyectos y sus presupuestos. Igualmente, las Administraciones Públicas requieren del uso de la tecnología para una gestión eficiente. Es difícil imaginar un empleado sin uno o más dispositivos conectados a la red y a servicios de las tecnologías de la información, por lo tanto, las oportunidades están en todos los campos, todos los sectores y todo tipo de empresa.

Algunos ejemplos relevantes y especialmente sensibles están en el campo de la salud y la educación, los cuales desarrollamos a continuación.

7.1. Salud: expediente clínico electrónico

La nube puede impulsar el desarrollo del expediente clínico electrónico (ECE) en México ya que, entre otros aspectos, puede ser la solución que dé respuesta a las necesidades de accesos tanto por sujetos obligados del sector público como del privado, garantizando así la interoperabilidad, y ser al mismo tiempo la plataforma a través de la que se desarrollen y faciliten aplicaciones ("apps") para la salud, todo ello en beneficio de los usuarios del Sistema Nacional de Salud, al mismo tiempo que el país avanza con respecto a otros países tanto a nivel regional como internacional.

La computación en la nube es una oportunidad para que, dándose las condiciones necesarias en cuanto a infraestructura de banda ancha y otros factores, el expediente clínico electrónico (en adelante, ECE), pueda llegar a ser una realidad en México de manera que, además, el país pueda alinearse con otros países y regiones que avanzan en la materia[88] y competir con los mismos.

Expediente Clínico Electrónico (ECE)

"Conjunto único de información y datos personales de un paciente, que puede estar integrado por documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de otras tecnologías, mediante los cuales se hace constar en diferentes momentos del proceso de la atención médica, las diversas intervenciones del personal del área de la salud, así como describir el estado de salud del paciente; además de incluir en su caso, datos acerca del bienestar físico, mental y social del mismo" (NOM-004-SSA3-2012).

El uso de la computación en la nube en el ámbito sanitario puede suponer también importantes beneficios para los pacientes y usuarios del Sistema Nacional de Salud y de la población en general. Desde la prescripción electrónica hasta la trazabilidad del consumo de medicamentos, son cuestiones que pueden beneficiarse del cómputo en la nube y ello sin contar con los grandes datos ("*big data*") u otras tecnologías relacionadas.

Es necesario tomar en consideración que la transparencia puede verse reforzada gracias al uso de la computación en la nube, ya que facilita el acceso a la información a las diferentes partes

[88] Conforme a una encuesta realizada en la Unión Europea, los Países Bajos (83,2%), Dinamarca (80,6%) y Reino Unido (80,5%) encabezan la lista de países que más han avanzado en materia de informatización de las historias clínicas. Véase http://europa.eu/rapid/press-release_IP-14-302_es.htm

interesadas, comenzando con el propio paciente o usuario. En particular, el expediente clínico debe estar a disposición del titular de los datos personales y su representante legal, para hacer así efectivos sus derechos[89] de acceso a la información pública y a la protección de datos de carácter personal.

El expediente clínico electrónico es, por tanto, un instrumento clave para la sociedad mexicana ya que a través del mismo se ejercen los derechos citados anteriormente así como el derecho a la protección de la salud.

No obstante, la situación actual es que el expediente clínico electrónico (ECE) todavía no ha despegado e incluso México se está quedando rezagado con respecto a otros países[90], tales como Colombia[91] o Perú[92] que ya han adoptado leyes en materia de expediente clínico electrónico.

Un instrumento jurídico en materia de expediente clínico electrónico a nivel federal es necesario y ello por varias razones, entre las que es posible señalar las siguientes:

- **Interoperabilidad:** tanto tecnológica como jurídica, ya que por lo que se refiere a este último aspecto, cabe señalar que ya hay Estados que están regulando en la materia, como por ejemplo Tamaulipas[93].

- **Estandarización:** unido a la interoperabilidad, la estandarización es necesaria debiendo tomar en consideración los diferentes sujetos obligados y actores, tanto del sector público como del privado, involucrados en la prestación de servicios de salud.

- **Seguridad jurídica:** que sirva para crear el entorno necesario en el que se desarrollen, por ejemplo, aplicaciones y servicios en beneficio de los usuarios del Sistema Nacional de Salud.

Los servicios de cómputo en la nube proporcionados por los proveedores deben buscar facilitar el cumplimiento de los requisitos legales y regulatorios en materia de protección de datos personales y seguridad por los sujetos obligados.

Contar con un instrumento jurídico que sea la base del desarrollo del expediente clínico electrónico y, al mismo tiempo, hacer un uso de la computación en la nube, puede suponer que México consiga alcanzar importantes objetivos que se concreten en una alta competitividad, tanto a nivel nacional como internacional.

---

[89] Al respecto, véase el Criterio 4/09 del IFAI, disponible en el vínculo electrónico http://inicio.ifai.org.mx/Criterios/04-09%20Expediente%20cl%C3%ADnico.pdf

[90] Si bien se presentó en la Cámara de Senadores un Proyecto de Decreto por el que se crea la Ley del Expediente Clínico Electrónico, del Senador Adolfo Romero Lainas, publicada en la Gaceta del Senado de 8 de octubre de 2013 y que se turnó las Comisiones Unidas de Salud y Estudios Legislativos.

[91] Véase la Ley 1438, de 19 de enero de 2011, por medio de la cual se reforma el Sistema General de la Seguridad Social en Salud y se dictan otras disposiciones.

[92] Véase la Ley Nº 30024 que crea el registro nacional de historias clínicas electrónica, publicada en el Diario Oficial El Peruano de 22 de mayo de 2013.

[93] Se trata de la Ley del Expediente Clínico Electrónico en Tamaulipas, aprobada mediante Decreto LXI-895 y publicada en el Periódico Oficial número 112, de 17 de septiembre de 2013.

Es así que, más allá de la revisión de Normas Oficiales Mexicanas que ha dado lugar a la publicación de tres en poco más de dos años, México tiene que afrontar una tarea pendiente que, por un lado, permita ahorrar costos y, por otro lado, dé lugar a la posibilidad de desarrollar una industria que permita atraer inversiones y exportar servicios, tales como el desarrollo de aplicaciones, software, etc.

En vigor	Deja sin efectos a
Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico (DOF de 15 de octubre de 2012).	Norma Oficial Mexicana NOM-168-SSA1-1998, Del expediente clínico (DOF de 30 de septiembre de 1999), y su modificación de 2003 (DOF de 22 de agosto de 2003).
Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro para la salud. Intercambio de información en salud (DOF de 30 de noviembre de 2012)	Norma Oficial Mexicana NOM-024-SSA3-2010, Que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud (DOF de 8 de septiembre de 2010).

Si bien el desarrollo de las tecnologías de la información ha tenido un avance importante en todos los ámbitos de la vida de las personas y de las instituciones, el sector salud no ha quedado ajeno al mismo. Por el contrario, este sector ha sido protagonista en la implementación de nuevas tecnologías, con el objeto de brindar servicios de salud eficientes y de calidad, sin que ello implique una vulneración de la protección de datos personales de los usuarios. Un ejemplo de ello es la adopción del expediente clínico electrónico, a través del cual se pretende facilitar la disponibilidad de la información, mejorar la calidad de la atención de los usuarios e incrementar la eficiencia administrativa del sector salud en sus tres niveles de atención, incluyendo los beneficios de seguridad y salud pública.

Así pues se trata de una herramienta que ofrece información sobre medicación, historia clínica del paciente, protocolos clínicos y recomendaciones de estudios específicos; genera un incremento en la eficiencia en el rastreo de antecedentes clínicos, el cuidado preventivo; y contribuye a reducir las complicaciones incluyendo los errores en la medicación. Además, permite asegurar que los pacientes reciban el más oportuno, conveniente y eficiente cuidado de la salud. Integra información de forma genérica y no agregada en un solo expediente y pone a disposición del médico y/o de los médicos tratantes la información recabada por diferentes actores para tener una visión global del problema y no segmentada, con lo que ayuda al diagnóstico, tratamiento y seguimiento de cada caso.[94]

La historia clínica se transformará en un expediente virtual que circulará por la red, será accesible a otros profesionales y cuya llave de acceso estará en poder del paciente por medio de su clave médica. Lo cierto es que la historia clínica se transforma en un sistema electrónico que resguarda la identidad y la información clínica de un paciente y a su vez, la pone a disposición de las autoridades que le brindan los servicios médicos requeridos. Garantizar estas cuestiones es responsabilidad del

[94] *Manual del Expediente Clínico Electrónico*. Dirección General de Información en Salud. Secretaría de Salud. México, 2011.

cuerpo médico quien deberá respetar las normas de utilización de la historia clínica del paciente, dirigidas a salvaguardar la confidencialidad y la seguridad de la información.[95]

El Sistema Nacional de Salud se integra de diversas fuentes de información médica de un paciente, que deberán cumplir con estándares mínimos de seguridad que garantizan la confidencialidad de la información.

Al respecto, inicialmente se emitió la Norma Oficial Mexicana NOM-024-SSA3-2010 que permitía disponer de toda la información médica de los pacientes en cualquier parte del país, mejorando la calidad, cuidado y atención de los pacientes, reduciendo tratamientos redundantes y previendo errores médicos[96]. Posteriormente, se ha publicado la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud[97].

Cabe señalar que la NOM-024-SSA3-2012 dedica un apartado específico, el 6.6, a las *"Consideraciones Universales de Manejo y Seguridad de la Información"* en el que trata las siguientes cuestiones aplicables a los prestadores de servicios de salud[98]:

Cuestión	Alcance
Sistema de Gestión de la Seguridad de la Información (SGSI)	Implementación de un SGSI de acuerdo a las disposiciones jurídicas aplicables en materia de transparencia, protección de datos personales y estándares en materia de seguridad de la información, que aseguren la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de la información en salud (apartado 6.6.1).
Registro y resguardo de la información así como uso de la firma electrónica	Por una parte, "*Los SIRES deben registrar y resguardar la información derivada de la prestación de servicios de salud en forma de documentos electrónicos estructurados e inalterables de acuerdo a las disposiciones jurídicas aplicables"* y, por otra parte, *"deben permitir la firma electrónica avanzada del profesional de la salud para toda aquella información que determine el Prestador de Servicios de Salud en su sistema de gestión de seguridad de la información, de conformidad con lo establecido en las disposiciones jurídicas aplicables"* (apartado 6.6.2).
Autenticación	De todos los usuarios, organizaciones y dispositivos, **como mínimo**, a través de *"un nombre de usuario y una contraseña cuya definición debe aprobarse por el grupo de trabajo estratégico de seguridad de la información de la organización"* (apartado 6.6.3).
Controles de acceso basado en	Se deben implementar mecanismos de autorización basados en roles y los

[95] Idem. Pág.44

[96] Dicha Norma Oficial Mexicana fue publicada en el Diario Oficial de la Federación de 8 de septiembre de 2010. Norma Oficial Mexicana NOM-024-SSA3-2010, Que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud

[97] Publicada en el Diario Oficial de la Federación de 30 de noviembre de 2012 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5280847&fecha=30/11/2012
Cabe señalar que en virtud de su artículo transitorio, la entrada en vigor de la misma *"deja sin efectos a la Norma Oficial Mexicana NOM-024-SSA3-2010"*.

[98] Por prestador de servicio de salud, conforme a la definición dada en el apartado 3.40, se entiende la *"persona física o moral del sector público, privado o social que proporciona servicios de salud en los términos de las disposiciones jurídicas sanitarias aplicables y que forma parte del Sistema Nacional de Salud."*

roles (*Role Based Access Control*, RBAC)	perfiles de usuario deben ser definidos en cada caso conforme a las disposiciones jurídicas aplicables a la organización (apartado 6.6.4).
Confidencialidad en el intercambio de información	Se deben implementar mecanismos de autenticación, de cifrado y de firma electrónica avanzada de acuerdo a las disposiciones jurídicas, Guías y Formatos aplicables en cada caso (apartado 6.6.5).
Exportación de la información del paciente	Se debe hacer de acuerdo a las disposiciones jurídicas aplicables en materia de transparencia y protección de datos personales (apartado 6.6.6).
Consentimiento	Se deben implementar controles sobre los consentimientos del titular de la información o quien tenga facultad legal para decidir por él, de acuerdo a lo establecido por las disposiciones jurídicas aplicables en materia de transparencia y protección de datos personales (apartado 6.6.6).

Específicamente, cobra especial importancia la obligación de implementar controles sobre el consentimiento del titular de la información o quien tenga facultad legal para decidir por él. Es necesario insistir en que el consentimiento es uno de los principios que legítima el tratamiento de los datos personales, lo que supone que infringir el mismo determina que cualquier tratamiento de datos personales que lo requiera es ilícito y por tanto sancionable en caso de verificarse la infracción.

Sin el consentimiento necesario para el tratamiento de los datos personales se vulnera el derecho fundamental a la protección de datos personales y, además, en el caso de los datos relativos a la salud, como datos sensibles que son, se produce una intromisión en lo más profundo de la dignidad de la persona, pudiendo dar lugar incluso a motivos de discriminación.

Por su parte, la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico[99], tiene como objetivo establecer *"los criterios científicos, éticos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso, manejo, archivo, conservación, propiedad, titularidad y confidencialidad del expediente clínico"*, siendo de obligado cumplimiento para *"el personal del área de salud y los establecimientos prestadores de servicios de atención médica de los sectores público, social y privado, incluidos los consultorios."*

Entre los requisitos que se establecen a lo largo de la NOM-004-SSA3-2012 en relación con el expediente clínico, cabe destacar los siguientes:

Requisito	Alcance
Conservación	Período mínimo de 5 años, contados a partir de la fecha del último acto médico (apartado 5.4).
Confidencialidad	Los datos personales que permitan identificar al paciente no deberán ser divulgados o dados a conocer a terceros, salvo en los supuestos y bajo las condiciones previstas en la Norma (apartados 5.5 a 5.7).
Manejo	Con discreción y confidencialidad por todo el personal del establecimiento (apartado 5.7).
Medios para la integración	Se pueden utilizar medios electrónicos, magnéticos, electromagnéticos, ópticos magneto-ópticos o cualquier otra tecnología en la integración del

[99] Publicada en el Diario Oficial de la Federación de 15 de octubre de 2012 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5272787&fecha=15/10/2012 Esta Norma, en virtud de su artículo transitorio, *"deja sin efectos a la Norma Oficial Mexicana NOM-168-SSA1-1998, Del expediente clínico, publicada en el Diario Oficial de la Federación de 30 de septiembre de 1999 y su modificación publicada el 22 de agosto de 2003."*

	expediente clínico, *"en los términos de las disposiciones jurídicas aplicables"* (apartado 5.12).
Evaluación del expediente clínico	Los establecimientos para la atención médica ambulatoria y hospitalaria del Sistema Nacional de Salud podrán evaluar la calidad del expediente clínico a través de organismos internos o externos (apartado 5.20).

Nada dice la NOM-004-SSA3-2012 respecto a la protección de datos personales y las medidas de seguridad, debiendo entender que en cada caso, bien se trate del sector público o bien del privado, se deberán aplicar las normas tanto generales como específicas en la materia. Al respecto, si bien los sujetos obligados por la Norma cumplirán, en su caso, con diferentes normas en materia de protección de datos personales y seguridad, la nube puede facilitar dicho cumplimiento y garantizar que tanto el sector público como el privado puedan garantizar altos estándares en materia de protección de datos personales y seguridad.

Resulta claro que los datos personales a la salud, son datos personales sensibles por lo que quedan sujetos al régimen específico previsto para los mismos y que se concreta en un mayor nivel de protección.

Es importante señalar que existe cierta complejidad en el tratamiento y resguardo de los datos personales de los pacientes ya que intervienen una gran cantidad de sujetos de carácter público, social y privado que de manera general son denominados prestadores de servicios de salud, los cuales pueden concretarse en todos aquellos que desarrollan actividades preventivas, curativas y de rehabilitación dirigidas a mantener o reintegrar el estado de salud de las personas; que prestan atención odontológica; que prestan atención a la salud mental de las personas; que prestan servicios auxiliares de diagnóstico y tratamiento y las unidades móviles, ya sean aéreas, marítimas o terrestres, destinadas a las mismas finalidades como son ambulancias de cuidados intensivos, urgencias y transporte.

En materia de consentimiento, por lo que se refiere específicamente a protección de datos personales, cabe recordar que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece que, como norma general, será necesario el consentimiento expreso y por escrito, siendo considerados los datos personales de salud como datos sensibles. No obstante, la norma general queda excepcionada en determinados supuestos, tales como el establecido por dicha norma en las fracciones IV del artículo 10 y VII del 37, por lo que puede adelantarse el análisis acerca de que el consentimiento en materia de protección de datos puede encontrarse implícito en aquel necesario para el tratamiento terapéutico de un paciente, siempre y cuando se trate de una finalidad primaria dentro de una relación jurídica (como lo es la prestación de servicios de salud) y sin perjuicio de cumplir con el principio de información.

Asimismo, debe tenerse en cuenta lo dispuesto por la fracción VI, del artículo 10 de la LFPDPPP que el consentimiento no será necesario cuando los datos personales *"[s]ean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables."*

En el caso de los datos de salud, como datos personales sensibles, el Aviso de Privacidad deberá indicar específica y expresamente que se trata de tales datos personales, siendo esta una cuestión relevante a tener en consideración. Se trata de una obligación central, prevista en el artículo 16 de la

LFPDPPP, y sobre la que inciden los Lineamientos sobre el Aviso de Privacidad en los términos previstos en el Lineamiento Vigésimo tercero.

Lo realmente importante es garantizar el cumplimiento de los principios de la protección de datos personales, de manera que se garantice un tratamiento legítimo y lícito, y sobre todo que existan lineamientos de seguridad que garanticen la confidencialidad de la información, elemento indispensable para el resguardo de la intimidad de los pacientes, de su seguridad y de la relación médico-paciente.

Por lo tanto, el uso del cómputo en la nube puede ser un detonador del expediente clínico, además de ser una herramienta útil para que el Sistema Nacional de Salud consiga alcanzar sus objetivos y garantizar, en definitiva, el derecho a la salud así como otros derechos de los usuarios del Sistema Nacional de Salud.

7.2. Educación

El sector educativo también puede beneficiarse del uso del cómputo en la nube, además de ser clave porque los estudiantes son los futuros protagonistas de un mundo que actualmente ya está interconectado y en el que en el futuro ellos tendrán que desarrollar sus competencias en un entorno en el que el papel habrá pasado a ser un soporte secundario.

El cómputo en la nube está transformando también el sector educativo, ya que las escuelas, universidades y otros centros educativos pueden acceder a tecnología que ofrece nuevas oportunidades y que, además, permite que los estudiantes conozcan una tecnología innovadora que utilizarán en sus vidas personales y profesionales.

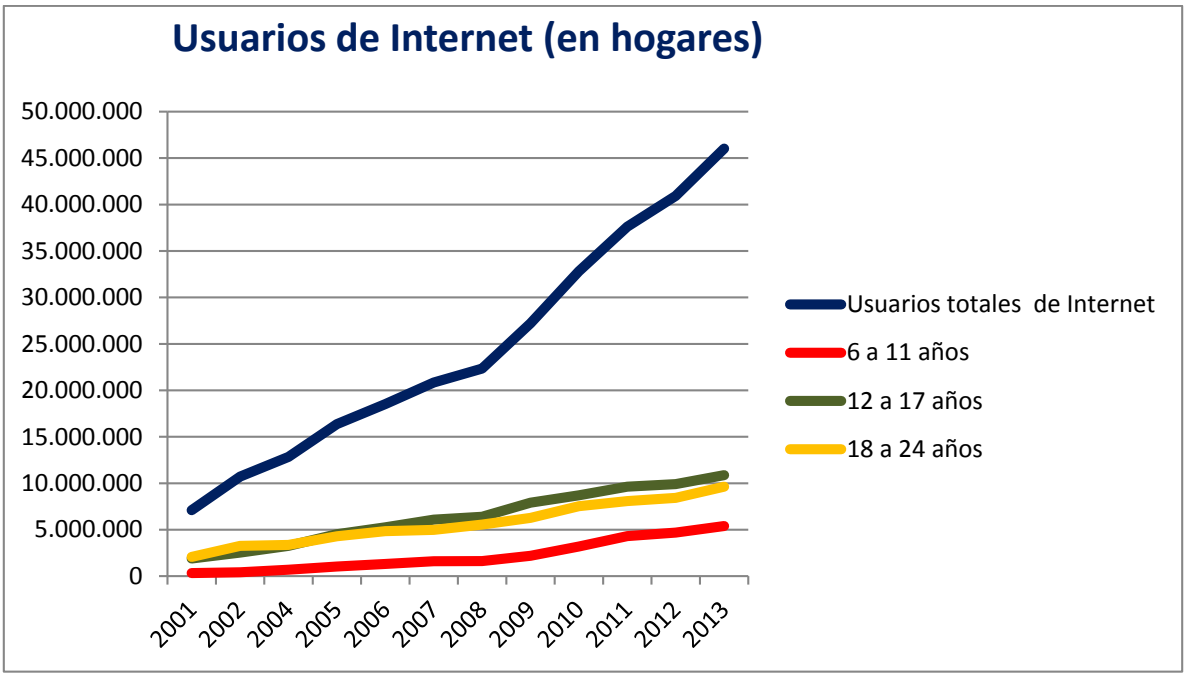
A través del uso de dispositivos conectados a la nube, tales como laptops, notebooks, tabletas u otros dispositivos móviles, los estudiantes tienen la posibilidad de conocer la tecnología de la que se hace uso tanto en empresas como en entidades y dependencias.

Que los estudiantes adquieran conocimientos desde la escuela en materia de tecnologías de la información y que puedan utilizarlas les permitirá adquirir los conocimientos y competencias necesarios para desarrollarse como usuarios y profesionistas.

El uso de la computación en la nube facilita la movilidad de estudiantes y profesores, puede potenciar el intercambio de información entre estudiantes, colegios y a nivel nacional, así como entrar de forma anticipada en una era donde la educación y las habilidades de interactuar en un mundo digital son claves para el desarrollo de un país y para su competitividad global.

Es así que si tomamos en consideración el año 2010, que es el último sobre el que el INEGI ofrece datos de población[100], la población total de 5 a 24 años era de 42.905.857 habitantes, de manera que 19.423.063 eran usuarios de Internet, lo que supone un 45,27%.

[100] Véase la distribución por edad y sexo por grupo quinquenal, disponible en http://www3.inegi.org.mx/sistemas/sisept/Default.aspx?t=mdemo03&s=est&c=17500



Fuente: INEGI. Datos relativos a usuarios de Internet por grupos de edad[101].

Es decir, casi la mitad de los jóvenes mexicanos tienen la posibilidad de acceder a contenidos y hacer uso de la nube. No obstante, es necesario tomar en consideración que sin embargo la mitad de la población de jóvenes mexicanos no tiene esa oportunidad.

Al respecto, la Asociación Mexicana de Internet (AMIPCI), en su noveno Estudio sobre los hábitos de los internautas en México[102] indica que en 2013 el 52% de los usuarios de Internet estaban en el grupo de edad de 6 a 24 años, siendo el 11% menores de edad de 6 a 11 años, el 22% jóvenes de 12 a 17 años y el 21% restante de 12 a 24 años.

En este sentido, las escuelas y centros universitarios de México juegan un papel fundamental debiendo ver la nube como una oportunidad tanto educativa como de desarrollo profesional. Futuros profesionistas que, además de hacer uso de la nube en su empleo, ya sea en el sector público o en el privado, podrían ofrecer sus servicios en los diferentes segmentos de mercado a los que da lugar la nube.

Al respecto, según un estudio desarrollado por IDC[103] en 2012, patrocinado por Microsoft, los servicios públicos y privados de cómputo en la nube generará casi 14 millones de empleos hasta 2015, lo que en el caso de México supondrá un incremento del 382% y supondrá 214,412 puestos

---

[101] Disponible en el vínculo electrónico http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tinf214&s=est&c=19446. Fecha de actualización 27 de noviembre de 2013 y consultada el 13 de abril de 2014.

[102] Publicado en 2013 y disponible en el vínculo electrónico http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=348&Type=1

[103] Sobre el citado estudio, véase https://www.microsoft.com/global/en-us/news/publishingimages/Cloud_Computing_s_Role_in_Job_Creation_Web.jpg http://www.microsoft.com/en-us/news/download/presskits/learning/docs/idc.pdf

de trabajo, cifras que incluso podrían ser superiores si México consigue atraer un mayor volumen de prestación de servicios relacionados con la nube y otras tecnologías innovadoras.

Además, por lo que se refiere a ser usuarios, los estudiantes son nativos digitales, ya que a diferencia de otros sectores de la población que se han ido adaptando al desarrollo de las tecnologías de la información llamados migrantes digitales, aquéllos pueden hacer uso de las mismas desde sus primeros años, lo que hace que puedan adquirir competencias en el marco de una tecnología que ha avanzado de manera vertiginosa.

En relación con el tratamiento de datos personales en los servicios de cómputo en la nube, es necesario insistir en la necesidad de determinar claramente si el proveedor de dichos servicios actúa como responsable o como encargado del tratamiento, ya que a la hora de tomar una decisión sobre el uso de productos o servicios destinados al ámbito escolar o académico, dadas las implicaciones que el uso de los datos personales y el hecho de que se intente utilizar éstos con fines de minería de datos (*"data mining"*) o publicidad[104] que no han sido consentidos expresamente.

Unido al o anterior, otros tratamientos de datos personales que, incluso pueden ir más allá del derecho a la protección de datos personales, tales como el escaneo de correos electrónicos que implica el acceso al contenido de comunicaciones electrónicas, deben ser tomados en consideración y que, de no haberse informado y obtenido el correspondiente consentimiento, podrían dar lugar a situaciones en las que se infrinjan derechos fundamentales. De nuevo, es necesario insistir en la necesidad de garantizar un alto grado de protección de los usuarios, cuyos datos personales son objeto de tratamiento así como su derecho a la protección del contenido de las comunicaciones, de manera que no se utilicen de manera indebida.

Especialmente, en el caso de los menores es necesario tomar en consideración que el desarrollo integral y la protección de los menores debe ser un objetivo prioritario también para el sector privado.

A nivel internacional, entre otros instrumentos, la protección de los menores se encuentra prevista en el artículo 16 de la Convención sobre los Derechos del Niño[105], la cual establece en forma expresa lo siguiente:

> *"1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.*
>
> *2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques."*

[104] En relación con el uso de datos personales con fines de publicidad, cabe señalar que varias autoridades de protección de datos alrededor del mundo, entre ellas el IFAI a través de su Secretario de Protección de Datos Personales, firmaron y enviaron una carta a Google en la que planteaban algunas cuestiones sobre el posible uso de los datos personales con fines de publicidad y otras implicaciones. La carta, en inglés, puede verse en el siguiente vínculo de Internet http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/junio/Carta_En.pdf

[105] Adoptada y abierta a la firma y ratificación por la Asamblea General en su resolución 44/25, de 20 de noviembre de 1989. De conformidad con su artículo 49, entró en vigor el 2 de septiembre de 1990. La Convención, en español, está disponible en el vínculo electrónico http://www2.ohchr.org/spanish/law/crc.htm

En México, en el caso del sector público ya lo es, debiendo destacar al respecto la reforma constitucional que se llevó a cabo y en virtud de la cual se reformaron los párrafos sexto y séptimo del artículo 4 y se adicionó la fracción XXIX-P al artículo 73, de la Constitución Política de los Estados Unidos Mexicanos[106]. En concreto, el párrafo séptimo del artículo 4 constitucional señala que *"En todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos."*

El tratamiento de datos personales de los menores es una cuestión que requiere de especial atención, ya que se trata de un grupo de la población que puede llegar a ser vulnerable. Incluso una acción que tenga por destinatario a un menor, por lo que se refiere a su protección de datos personales, puede involucrar o tener también consecuencias para su familia.

Por lo que se refiere a otros países de Latinoamérica, hay que resaltar que países como Colombia[107] o Perú[108] han incluido expresamente en su normatividad sobre protección de datos personales que los datos de los menores son sensible, lo que implica que estén sujetos a reglas especiales para su tratamiento.

Al respecto, las organizaciones de la sociedad civil están también llamadas a desempeñar un papel relevante, ya que pueden ayudar, y a su vez deben recibir ayuda, a proteger los derechos de los usuarios y especialmente de los menores[109].

En cuanto al consentimiento, de nuevo como principio que legitima el tratamiento de los datos personales, es necesario prestar especial atención, ya que el uso del cómputo en la nube no puede hacerse sin las debidas garantías de manera que en este caso, las escuelas ya sean públicas o privadas, como clientes de dichos servicios, son las que tienen que velar porque se proteja tanto su derecho fundamental a la protección de datos personales como el interés superior de los niños y jóvenes en las actuaciones que lleven a cabo.

Es decir, el uso de servicios de cómputo en la nube en el ámbito educativo es deseable, pero siempre y cuando el proveedor de servicios de cómputo en la nube no base su negocio en la explotación ilícita de los datos personales de los menores, ya que se estaría produciendo una vulneración de su derecho fundamental incluso con implicaciones para sus familias, al obtener indebidamente información personal sobre las mismas.

En conclusión, el tratamiento de datos personales que pueda producirse por el uso de servicios de cómputo en la nube en el caso de estudiantes que sean menores de edad tiene que hacerse con

---

[106] Publicada en el Diario Oficial de la Federación de 12 de octubre de 2011 y disponible en el vínculo electrónico http://www.dof.gob.mx/nota_detalle.php?codigo=5213826&fecha=12/10/2011

[107] Véase el artículo 7 de la Ley estatutaria 1581, de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, así como el artículo 12 del Decreto 1377, de 27 de junio de 2013, por el cual se reglamenta parcialmente la Ley.

[108] Véase el artículo 13.3 de la Ley Nº 29733, Ley de Protección de Datos Personales, publicada en el Diario Oficial El Peruano, de 3 de julio de 2011, así como el artículo 30 del Decreto Supremo Nº 003-2013-JUS, por el que se aprueba el Reglamento de la Ley, publicado en el Diario Oficial El Peruano, de 22 de marzo de 2013.

[109] Como ejemplo, puede verse el caso de la Digital Citizens Alliance (www.digitalcitizensalliance.org). Esta asociación, entre otras actividades publica reportes relativos a diversas cuestiones en materia de protección de datos personales. Uno de dichos reportes es *"Google+ Circles and the new Google+ Gmail integration, a dangerous combination"*, en el que alerta sobre las implicaciones especialmente para menores en relación con el tratamiento de sus datos personales.

apego a la normatividad aplicable y con todas las garantías exigibles, de manera que un proveedor de servicios de cómputo en la nube, con independencia de que actúe como responsable o encargado del tratamiento según el caso concreto, no pueda tratar datos personales sin cumplir con las obligaciones que le son exigibles en la materia[110].

7.3. Otras áreas

El cómputo en la nube es transversal en el sentido de que en todos los ámbitos de nuestras vidas, tanto personales como profesionales, no se entienden en la actualidad sin el uso de la tecnología. Tanto el sector público como el privado tienen a su alcance la posibilidad de hacer uso del cómputo en la nube, lo que supone que las empresas puedan ser más competitivas y las entidades y dependencias más eficientes en la prestación de servicios a los ciudadanos.

Además de la sanidad y la educación, muchas otras áreas de la actividad económica o gubernamental pueden hacer uso del cómputo en la nube, lo que determina que estás puedan ser más competitivas o eficientes, respectivamente.

La competitividad del sector económico y la eficiencia del sector gubernamental deben ser uno de los objetivos prioritarios de todas las partes interesadas, ya que México, por su posición geo-política y otros factores relevantes tales como instituciones, políticas públicas, normatividad, debe seguir compitiendo con países y potencias económicas. Al respecto, según el Reporte Global de Competitividad 2012-2013, que con carácter anual elabora el Foro Económico Mundial[111], México está en el lugar 53, habiéndose producido un avance de cinco posiciones con respecto a 2011-2012. Pero en el mismo Reporte[112] correspondiente a 2013-2014, México ha retrocedido dos posiciones, hasta el lugar 55.

México sigue por detrás de otros países de Latinoamérica, como Chile, que ocupa el puesto 34; Panamá, puesto 40, o Costa Rica, puesto 54, y se pone por delante de Brasil, que ha retrocedido desde el puesto 48 hasta el 56.

Cabe señalar también que en el Reporte Global de Tecnologías de la Información 2014, México aparece en el puesto 79, de un total de 148 países alrededor del mundo[113]. Es así que México queda rezagado con respecto a países como Chile, puesto 35; Panamá, puesto 43; Costa Rica, puesto 53, o Colombia, puesto 63.

---

[110] Al respecto, puede verse el artículo Google Apps for Education: Data Mining and the Threat of Student Privacy, publicado por Sue Scheff y disponible en el vínculo electrónico http://www.huffingtonpost.com/sue-scheff/google-apps-for-education_b_5083478.html?utm_hp_ref=technology&ir=Technology También, la noticia relativa a que Google dejará de escanear las cuentas de correo electrónico de Gmail con fines de publicidad después de que se haya presentado una demanda judicial en Estados Unidos. Esta última noticia puede verse en http://www.theguardian.com/technology/2014/mar/19/google-lawsuit-email-scanning-student-data-apps-education

[111] Véase una referencia al Reporte Global de Competitividad 2012-2013 en el vínculo electrónico http://www.economia.gob.mx/eventos-noticias/informacion-relevante/8567-boletin203-12

[112] El ranking correspondiente al reporte de 2013-2014 puede verse en el vínculo electrónico http://www3.weforum.org/docs/GCR2013-14/GCR_Rankings_2013-14.pdf

[113] Véase The Networked Readiness Index Rankings 2014, del Foro Económico Mundial, en el vínculo electrónico http://reports.weforum.org/global-information-technology-report-2014/#=

El citado reporte indica que después de años de ascenso en el ranking, México ha caído en 2014 un total de 16 puestos. Entre las razones, se apuntan el hecho de que el costo de acceso a la infraestructura TIC permanezca alto y el hecho de que la calidad del sistema educativo siga siendo un reto a la hora de responder a las necesidades de una economía cambiante y cada vez más digital[114].

Entre los pilares de dicho reporte cabe destacar que México ha avanzado 23 posiciones en Sofisticación Empresarial y 22 posiciones en Innovación. Tomando en consideración estos avances, una rápida adopción del cómputo en la nube puede mejorar todavía más la progresión de México en dichos rankings, sin perjuicio de poner foco en otros pilares que requieren de acciones específicas y que también están relacionadas con el cómputo en la nube, como por ejemplo la Eficiencia en el Mercado Laboral, que puede servir para crear oportunidades para los profesionistas mexicanos e incluso atraer intelecto internacional.

En este sentido, el Reporte Global de Competitividad debe ser una llamada de atención para México, ya que se si se pone foco en Latinoamérica y el Caribe, México aparece como el tercer país entre los 10 países más avanzados en materia de educación superior, preparación tecnológica e innovación[115].

Unido a lo anterior, es necesario tomar en consideración que el cómputo en la nube puede ser usado tanto por sectores regulados como no regulados, lo que pone de relieve la necesidad de adoptar medidas que sirvan para impulsar la competitividad en todos los sectores y áreas de actividad.

El uso de la nube en dichos sectores, tanto regulados como no regulados, implica que las partes interesadas, ya sea el legislador o las autoridades competentes, colaboren con los mismos para evitar barreras indebidas que dificulten el desarrollo tecnológico de México e impidan a las empresas el uso de la misma que puede ser el factor diferenciador que les permita competir a nivel global.

Se trata de que, por ejemplo, un sector regulado pueda hacer uso del cómputo en la nube sin encontrar restricciones que deriven de situaciones no pensadas para un escenario tecnológico. Por ejemplo, el acceso a la información por las autoridades –desde luego estricta y únicamente en los casos en que las leyes locales así lo permitan– puede llevarse a cabo sin problema en el caso de una organización que hace uso del cómputo en la nube, ya que no es posible pensar más en archiveros en papel que se guardan en una oficina. Incluso en dicho caso la realidad es que se haya contratado a un tercero que guarde los archivos en papel como medida de seguridad o por razones de gestión eficiente de la documentación.

Por último, también un sector regulado como el financiero, debe poder hacer uso del cómputo en la nube, ya que de lo contrario se estaría marginando a determinados sectores de la posibilidad de beneficiarse del uso de las tecnologías de la información en un contexto global así como de que también los clientes o usuarios de sus servicios lo hagan.

---

[114] Véase el reporte, ya citado, en su página 27.

[115] Véase la información disponible en el vínculo de Internet http://www3.weforum.org/docs/GCR2013-14/GCR_Infographic_LatinAmerica_2013-2014.jpg

8. Propuestas de acción para las partes interesadas

8.1. Partes interesadas: elaboradores de políticas públicas, autoridades reguladoras y legisladores

Entre las partes interesadas en el cómputo en la nube se encuentran desarrolladores de políticas públicas, autoridades reguladoras y legisladores, sociedad civil, e industria quienes, en el ámbito de sus respectivas competencias, pueden adoptar medidas o realizar acciones que ayuden a impulsar la adopción del cómputo en la nube y, por tanto, contribuir a incrementar la competitividad del sector privado y la eficiencia del sector público en México.

Los desarrolladores de políticas públicas, las autoridades reguladoras, la industria y los legisladores, entre otros, son también partes interesadas en el cómputo en la nube y con sus acciones y decisiones pueden ayudar a acelerar su adopción en México, lo cual servirá también para incrementar la competitividad en el caso del sector privado y la eficiencia del sector público.

En el caso de los **desarrolladores o elaboradores de políticas públicas**, éstos pueden ayudar a identificar aspectos en los que México pueda trabajar para impulsar el cómputo en la nube de manera que tanto el sector público como el privado se beneficien, tanto al interior del país como al exterior por lo que se refiere al posicionamiento en los diferentes rankings que se elaborar por diversas organizaciones. Es así que contar con una política pública en materia de cómputo en la nube puede marcar una clara diferencia para México, pudiendo llegar a convertirse en un referente para otros países y regiones alrededor del mundo.

El desarrollo de políticas públicas en la materia debe tomar en consideración todos los aspectos que se plantean y las implicaciones que éstos pueden tener en áreas específicas. Por ejemplo, la protección de datos personales, privacidad y la seguridad son cuestiones que inciden directamente en el cómputo en la nube, pero que también están presentes en el expediente clínico electrónico (ECE) y que deben aplicarse a la vista del estado actual de la normatividad tanto para el sector público como el privado así como posibles esquemas de autorregulación.

En el proceso de toma de decisiones, estas partes interesadas deben tener presentes los beneficios y riesgos del cómputo en la nube.

En cuanto al rol de la **industria**, de manera destacada es la que tiene que desarrollar prácticas de negocio responsables, lo que entre otros aspectos implica que las mismas tengan que garantizar un alto nivel de cumplimiento, especialmente en materia de protección de datos personales, privacidad y seguridad. Asimismo, el diseño de los productos y/o servicios tiene que desarrollarse conforme a principios tales como la privacidad por diseño, la seguridad por diseño así como tomar en consideración la necesidad de transparencia que sirva a los usuarios o potenciales usuarios para tomar decisiones informadas. Y lo anterior debe producirse en un marco en el que la autorregulación y las buenas prácticas, tanto a nivel nacional como internacional, sean un instrumento para el desarrollo tecnológico y un referente para dicho desarrollo.

Y por lo que se refiere a la **sociedad civil** cabe señalar que tiene que ser un actor activo en la defensa de sus derechos fundamentales, si bien esto pasa por la necesidad de informarse en todo momento sobre las condiciones de uso de la tecnología que le proporcionan los diferentes

proveedores de servicios. Al respecto, la sociedad civil también debe ayudar a los usuarios a conocer los diferentes productos y servicios que están a su disposición; las implicaciones del uso de los mismos y proporcionar información para que el usuario pueda tomar una decisión con base en todos los elementos a tomar en consideración.

Que la sociedad civil consiga su objetivo depende en buena medida del apoyo que reciba, debiendo comprometerse al respecto las autoridades públicas a abrir sus puertas, escuchar a la sociedad civil y tenerla presente en todas sus acciones. La colaboración es básica en todos los ámbitos y especialmente en cuestiones relacionadas con el desarrollo, adopción y uso de las TIC. En definitiva, se trata de que la sociedad civil sea llamada cuando las acciones que lleve a cabo el Gobierno tengan implicaciones para la misma y que también aquélla sea consciente de que su opinión cuenta y del rol que desempeñan y que pueden desempeñar a través de las herramientas y derechos que tienen, entre los que se encuentra el relativo al acceso a la información pública.

— Beneficios del cómputo en la nube

El cómputo en la nube genera importantes beneficios tanto para los prestadores de servicios, sean públicos o privados, como para los usuarios, toda vez que reduce los costos de transacción asociados con el diseño, producción y distribución de bienes o servicios (Mariscal y Gil-García, p. 1). Por una parte, quien contrata los servicios de cómputo en la nube reduce sus costos, pues ya no sería necesario que adquiriera nuevos equipos de cómputo, contar con personal capacitado para su gestión, actualización y mantenimiento y, por lo general, tampoco implica el desarrollo de software. Por la otra, los usuarios de servicios públicos o privados pueden agilizar sus trámites y, en un gran número de casos, acceder a centros de datos, aplicaciones y servicios de manera remota en cualquier punto geográfico. De tal forma que el cómputo en la nube suele asociarse a importantes ganancias de eficiencia económica, que repercuten en el bienestar de los consumidores.

Además, dados estos beneficios, las nuevas tendencias de política pública promueven la llamada e-Gobernanza, esto es, aquella que enfatiza las relaciones y redes dentro y fuera del e-Gobierno y que se convierten en un aspecto esencial para el desarrollo centrado en los usuarios (ciudadanos, empresas, etc.), y donde los e-Servicios son un elemento central. Con ello se busca generar servicios de calidad a través de los sitios web o mediante dispositivos electrónicos, para que cualquier persona pueda realizar transacciones, trámites u obtener información en línea, en cualquier momento y lugar (Quintanilla y Gil-García, p. 8 a 13).

Por último, el cómputo en la nube ayuda también a reducir el impacto ambiental ya que gracias al uso de productos y servicios de nube, como una tecnología verde (*"Green IT"*), es posible reducir el gasto en papel, el ahorro energético y optimizar el consumo de otros recursos medioambientales. En particular, reducir la "huella de carbono" ayuda a frenar el cambio climático global. Es así que tanto la industria como los usuarios pueden ayudar a reducir el impacto ambiental a través del uso de tecnologías y dispositivos que permitan hacer un uso más eficiente y menos contaminante.

— Retos del cómputo en la nube

No obstante, el uso de las nuevas tecnologías de la información y específicamente del cómputo en la nube, también presentan importantes retos para la privacidad de las personas, toda vez que su utilización agiliza considerablemente el intercambio de información, su utilización, y su disponibilidad. Si bien tales aspectos son parte de las ventajas del uso del cómputo en la nube, la

falta de adopción de medidas de seguridad que garanticen un resguardo adecuado de la información suponen también un riesgo. Además, un aspecto que contribuye a la percepción de inseguridad que supone el uso del cómputo en la nube es precisamente que su funcionamiento ubica la información en los servidores de los proveedores del servicio de *cloud computing*. De tal forma que tienen acceso a esa información tanto los prestadores del servicio de cómputo en la nube como los prestadores de los servicios dirigidos a los usuarios finales.

De ahí que sea necesario adoptar un marco jurídico local sólido en armonía con disposiciones internacionales y nacionales de otros países que participen en el flujo de información, que permita generar incentivos para la utilización del cómputo en la nube dadas sus ventajas comparativas, pero que a su vez minimice el riesgo de exponer indebidamente la información resguardada y el acceso ilegal a los datos personales.

Ambas caras de la moneda han sido tomadas en consideración a través de las recientes reformas a la Constitución Política de los Estados Unidos Mexicanos.

Las **autoridades reguladoras** también pueden marcar una diferencia para el cómputo en la nube en México, ya que en virtud de las competencias que tienen atribuidas pueden, en su caso en coadyuvancia con otras autoridades, facilitar su adopción con lo que ello supone para la competitividad del sector privado y la eficiencia del sector público.

En particular, las autoridades reguladoras pueden desarrollar acciones a través de las que se proporcione seguridad jurídica que permita a los clientes de servicios de cómputo en la nube adoptar dichos servicios, despejando dudas al respecto. Dichas acciones pueden ser también medidas que permitan impulsar el uso de las TIC en México, en particular el cómputo en la nube, lo que redunda en la competitividad.

Otra cuestión en la que las autoridades reguladoras pueden desempeñar un papel fundamental es el impulso de la autorregulación, lo que en el caso del cómputo en la nube puede ayudar a dar respuesta a muchas cuestiones que se plantean y generar también buenas prácticas en relación con el mismo. A tal fin, la experiencia internacional en la materia debe ser tomada en consideración para el desarrollo de acciones sobre el cómputo en la nube en México.

Se trata así de desarrollar "puertos seguros", de manera que se pueda garantizar un alto nivel de cumplimiento en materia de protección de datos personales y seguridad al interior de las organizaciones, ya sean públicas o privadas, y también al exterior. Y de esta manera se podría aumentar la confianza de los usuarios y consumidores, tanto por lo que se refiere al tratamiento de sus datos personales como al uso de nuevas tecnologías. Y dicho concepto de puerto seguro debe ser dinámico, en el sentido de estar alienado con la evolución tecnológica que permita a las organizaciones a ser competitivas e innovadoras, además de estará alineado con buenas prácticas internacionales.

En cualquier caso, dichas acciones deben estar coordinadas de manera que el marco regulador aplicable al cómputo en la nube en México sea un detonador tanto para el sector privado como para el público. Y dichas autoridades reguladoras deberían contar con el resto de partes interesadas, entre ellas industria y usuarios, de manera que dicho marco regulador responda a las necesidades y retos que se plantean en el día a día.

Por último, el **legislador** es otra de las partes interesadas relevantes ya que la regulación sobre la privacidad, protección de datos personales y seguridad debería ser resultado de un profundo proceso de análisis sobre los retos y oportunidades que plantea aquél, tomando en especial consideración la protección de datos personales y la seguridad.

Además, sería necesario que el legislador tomase en consideración que la continua, rápida y exponencial evolución de las tecnologías de la información, y entre ellas la del cómputo en la nube, requiere que la regulación que se haga en su caso sobre el mismo sea mínima y se adecúe a los cambios y necesidades que se produzcan, de manera que no llegue a convertirse en una barrera a la competitividad o innovación, o no responda a los retos jurídicos, económicos o sociales que se plantean.

8.2. Propuestas de acción para que México se beneficie del cómputo en la nube

Ser competitivo e innovador mediante el uso del cómputo en la nube depende, en buena medida, de contar con un plan estratégico tanto para el sector público como privado. Es por ello que se deben plantear propuestas de acción en relación con el cómputo en la nube en las que se involucren todas las partes interesadas y se tomen en consideración todos los aspectos que se plantean.

Es así que a continuación se incluye una propuesta de medidas para que México se beneficie al máximo del cómputo en la nube tanto en el sector público como en el privado:

1. ***Elaborar un censo de centros de datos y recursos informáticos (equipos, software, aplicaciones) sin restricciones territoriales para el alojamiento y tratamiento de los datos en el sector público que permita medir el impacto económico que tendría el cómputo en la nube:*** esto permitirá un considerable ahorro de recursos públicos, de manera que puedan ser destinados a otros fines, además de conseguir que México suba posiciones en rankings de gobierno electrónico a nivel internacional.
2. ***Considerar el cómputo en la nube como un indicador relevante:*** tanto en encuestas nacionales, por ejemplo las que desarrolla el INEGI, como a la hora de medir el nivel de uso de las TIC en los sectores público y privado. Dicho indicador debe ser puesto en relación con otra información relevante, de manera que ello facilite datos que permitan demostrar cómo México está haciendo uso de tecnologías innovadoras y medir el nivel de competitividad del país.
3. ***Garantizar un alto nivel de protección de datos personales, privacidad y seguridad:*** en particular a través de una regulación efectiva de las finalidades a qué se destinen los datos personales y en atención a los titulares concretos de los mismos; unido todo ello a tomar en consideración que ningún modelo de negocio, y en particular los que se basan en servicios o aplicaciones gratuitas, publicidad o venta o transferencia de datos personales a anunciantes, pueden suponer una intromisión, sin las debidas garantías, al derecho fundamental a la protección de datos personales;
4. ***Analizar cómo la debida protección de datos personales, la privacidad y la seguridad promueven al desarrollo del cómputo en la nube en México:*** de manera que por "afectar" se entienda que la regulación aplicable llegue a ser un detonador o, por el contrario, se convierta en un inhibidor. Además, la protección de datos personales y la

seguridad son susceptibles también de medidas auto-regulatorias que respondan de manera efectiva a cuestiones específicas o sectoriales que se puedan plantear y que requieren de la colaboración de las diferentes partes implicadas.

5. ***Desarrollo de un auténtico mecanismo de autorregulación en materia de protección de datos personales y seguridad:*** de manera que sirva para que los sujetos obligados, tanto responsables como encargados del tratamiento, cuenten efectivamente con una forma de cumplimiento alternativo de las disposiciones legales en materia de privacidad y seguridad de la información, yendo más allá de los parámetros de autorregulación vinculante y respondiendo a la rápida evolución tecnológica;
6. ***Facilitar la prestación de servicios de cómputo en la nube:*** en el sentido de garantizar la seguridad jurídica y condiciones necesarias que permitan atraer inversiones y la prestación de servicios, tanto desde como hacía el mercado mexicano. Los servicios de cómputo en la nube son una oportunidad para el mercado y también para los profesionistas, pudiendo generar empleo y servicios que pueden prestarse tanto en el mercado nacional como exportarse.
7. ***Apoyar e impulsar la expansión de la conectividad de banda ancha:*** *a través de programas como "México Conectado", ya que la conectividad es uno de los pilares fundamentales para la adopción y uso del cómputo en la nube. Además, garantizar la conectividad de banda ancha es esencial, ya que de otra manera los mexicanos estarían perdiendo oportunidades personales y profesionales en su vida diaria.*
8. ***Reconocer el fenómeno global y multi-jurisdiccional de Internet y otras tecnologías:*** Lo que supone adoptar una posición activa para evitar el establecimiento de cualquier forma de fragmentación de Internet o restricción territorial, ya sea en forma de: 1) medidas de inversión local (*"forced localization"*), o de 2) "soberanía de datos", en aras a la supuesta protección de determinada información, ya que en todo caso una protección efectiva de los datos personales y la seguridad de la información dependen del estándar de protección que se aplique y no del territorio en el que la información "resida" o se presuma que "reside". Además, es necesario mantener la legislación y/o regulación aplicables conforme a estándares internacionales de buena regulación (regulación clara y precisa; no sobre-regulación; preferencia hacia normas de armonización internacional y cooperación procesal internacional).
9. ***Analizar barreras o condiciones específicas relativas en el uso del cómputo en la nube:*** dichas barreras pueden surgir, en particular, en el caso de sectores regulados si las condiciones o requisitos a cumplir no fueron pensados para un entorno tecnológico y competitivo, de manera que pueden haber quedado desfasados, tales como requisitos de acceso a información o documentos en soporte papel que ahora son una mera copia, en su caso, del original que se encuentra en soporte electrónico.
10. ***Potenciar el cómputo en la nube en el ámbito sanitario:*** lo que significa que pueda impulsar el desarrollo e implementación del expediente clínico electrónico (ECE), la prescripción electrónica y sea también un instrumento para el desarrollo de otros servicios en el ámbito sanitario.
11. ***Potenciar las habilidades y competencias de los jóvenes:*** tanto por lo que se refiere al uso del cómputo en la nube desde la escuela, lo que permitirá el acceso a más y mejores recursos educativos, como una opción profesional para el futuro así como un conocimiento en caso de futuros profesionistas con responsabilidad en la materia.
12. ***Analizar las posibilidades que ofrece la certificación:*** en particular de productos o servicios de cómputo en la nube, pudiendo ser también la certificación una opción de

servicios a proporcionar, junto con la auditoría y otros servicios que puedan ofrecer los terceros de confianza.

13. ***Desarrollar una hoja de ruta sobre estandarización enfocada en productos y servicios de cómputo en la nube:*** tomando en consideración que el cómputo en la nube supera las fronteras nacionales y que implica también que, en su caso, se adopten medidas para garantizar la interoperabilidad. Es por ello que la estandarización podría plantearse a través de Normas Oficiales Mexicanas (NOM), Normas Mexicanas (NMX) y Normas de Referencia (NRF) que, en su respectivo ámbito, presten atención a las cuestiones que se plantean tanto a nivel nacional como internacional.
14. ***Promover la cooperación de las partes interesadas:*** ya que cada una de las partes desempeña un papel o tiene cuestiones que plantear en relación con el cómputo en la nube y que deben ser atendidas si se quiere impulsar el mismo. Además, cada una de estas partes puede aportar soluciones o medidas que sirvan para facilitar una rápida adopción del cómputo en la nube por los sectores público y privado de manera que los usuarios y ciudadanos puedan beneficiarse de la misma. Por lo tanto, un diálogo con todos, lo que significa que todos puedan participar tanto por lo que se refiere a la adopción y uso de las TIC así como la forma en la que ésta sea regulada o esté basada en esquemas de autorregulación, es fundamental para conseguir el máximo beneficio.

Por último, estas propuestas de acción deben ponerse en relación con otras medidas que tienen por objeto impulsar la competitividad en México, de manera que el país pueda beneficiarse, tanto a nivel nacional como internacional, del cómputo en la nube en los sectores público y privado. Y entre dichas medidas, se trata también de evitar situaciones que impidan el desarrollo del cómputo en la nube, tales como la soberanía de datos, y garanticen el máximo respeto de los derechos de los usuarios y consumidores, tales como la prohibición de tratar de datos personales con fines no previstos inicialmente a menos de que se cuente con el consentimiento necesario.

9. Conclusiones

Como principales conclusiones que derivan del estudio realizado, es posible señalar que:

1. ***El cómputo en la nube es una oportunidad para un México más innovador y competitivo:*** ya que hacer uso de una tecnología innovadora como ésta se concreta en la posibilidad de que las entidades y dependencias del sector pública puedan proporcionar servicios más eficientes a los ciudadanos, beneficiándose también de un importante ahorro de recursos públicos, y en el caso de las empresas que puedan competir tanto a nivel nacional como internacional.

   Además de que el cómputo en la nube pueda ser un detonador para la competencia en México, en todos los sectores de actividad, es también una oportunidad específicamente para el desarrollo del expediente clínico electrónico (ECE) y en el sector educativo. En el primer caso, es clave para hacer posible una mejor atención sanitaria y garantizar los derechos a la protección de datos personales, a la transparencia y a la salud. Y en el segundo caso, facilita el acceso a más y mejores contenidos educativos y constituye una oportunidad para los jóvenes mexicanos.

   Por último, gracias al cómputo en la nube desaparece un diferencial tecnológico que hasta la fecha daba lugar a una brecha entre las pequeñas y las grandes empresas. Es así que el cómputo en la nube ofrece a las pequeñas empresas la posibilidad de competir con grandes empresas.

2. ***Es necesario tomar en consideración cómo se desarrolla el cómputo en la nube:*** lo que supone que se deba analizar qué normatividad es aplicable al mismo, prestando especial atención a posibles o potenciales barreras y garantizando un alto nivel de protección de los derechos de los usuarios.

   Es decir, se trata de garantizar la seguridad jurídica en armonía con la normatividad internacional sobre un fenómeno transfronterizo, que sirva como base para el desarrollo tecnológico del país y, al mismo tiempo, identificar si hay barreras u obstáculos que impidan ser competitivos, tomando en consideración que el desarrollo tecnológico es imparable en un mercado digital global. Por lo tanto, normatividad y tecnología tienen que estar alineadas y responder también a los retos sociales y económicos.

   Asociado a la seguridad jurídica está la confianza, que debe generarla el modelo de prácticas del país, y por supuesto los proveedores de servicios. La confianza es necesaria para que permita a las organizaciones plantearse el uso del cómputo en la nube, diseñar servicios en la nube y por supuesto hacer uso de la nube con la confianza necesaria para clientes y accionistas.

3. ***Hay que garantizar la protección de datos personales, la privacidad y la seguridad:*** de manera que sean detonadores del cómputo en la nube y no inhibidores. Ser un detonador significa también que la protección de datos personales, la privacidad y la seguridad tienen que ser claves a la hora de generar confianza en los clientes de servicios de cómputo en la nube y en los titulares de los datos personales, ya sean estos último mexicanos o de cualquier otro país.

Garantizar el cumplimiento en materia de protección de datos personales y seguridad debe ser el resultado de medidas tecnológicas, legislativas y auto-regulatorias, además certificables. Y para garantizar dicho cumplimiento el proveedor de servicios de cómputo en la nube y el cliente deben cooperar, en su papel y obligaciones respectivas.

Es necesario desincentivar incumplimientos ya que de lo contrario no se genera la confianza que hace falta para el despegue de tecnologías como el cómputo en la nube. Por lo tanto, prever la graduación de las sanciones ante incumplimientos en determinados casos es esencial para que el incumplimiento no sea una "opción a considerar".

4. ***En particular, la seguridad es clave para el desarrollo del cómputo en la nube:*** ya que el modelo de negocio al que da lugar el cómputo en la nube implica que el proveedor de servicios tenga que adoptar también medidas que eviten desde accesos no autorizados hasta la pérdida de datos personales. De no ser así, el cliente estaría dejando un activo estratégico y exponiendo el derecho fundamental a la protección de datos personales de sus clientes a riesgos que podrían dar lugar a la pérdida de confianza en el uso de una tecnología todavía emergente.

   Además, es necesario poner foco en la necesidad de que los proveedores de servicios de cómputo en la nube garanticen la seguridad de los datos personales que tratan ante situaciones en las que se pueda producir un acceso no autorizado o hacer uso de los datos personales sin los debidos controles y/o procedimientos, tales como el control de acceso basado en roles (*Role Based Access Control*, RBAC), sistemas de detección de intrusiones (*Intrusive Detection System*, IDS) o procedimientos de notificación de brechas de seguridad. Y también es necesario que el modelo de negocio en el que se sustenta el proveedor de servicios de cómputo en la nube no tenga como objetivo hacer un uso en beneficio propio de la información que el responsable del tratamiento le ha encomendado para su custodia y gestión en los servicios que éste ha contratado y respecto de los que tiene una expectativa de cumplimiento por parte de aquél.

5. ***El proveedor de servicios de cómputo es un socio estratégico:*** Y, por lo tanto, un actor clave para que cualquier empresa, con independencia de su tamaño y sector de actividad, pueda ser competitiva. Por ello, a la hora de contratar servicios de cómputo en la nube, el cliente tiene que cumplir también con un deber de diligencia a la hora de analizar la información sobre los servicios de cómputo en la nube que le proporcionará el proveedor, qué y cómo cumple con sus obligaciones, así como otros aspectos relevantes, tales como comprender su modelo de negocio, sus prácticas y las funcionalidades de los productos en temas claves como seguridad y privacidad.

   En este sentido, un proveedor de servicios de cómputo en la nube que está certificado y que ha implementado medidas para guiar a sus clientes, siendo transparente, debe ser un estándar para la industria y una garantía para dichos clientes.

   Además, los terceros de confianza pueden desempeñar un papel relevante al dinamizar la adopción del cómputo en la nube, siendo también una oportunidad de negocio en relación con el mismo.

6. ***Es necesario que todas las partes interesadas colaboren:*** con la finalidad de que México pueda aprovechar al máximo esta tecnología, todavía en buena medida emergente, pero que permitirá al país seguir compitiendo a nivel internacional y posicionarse, en su caso, en los primeros lugares de los diferentes rankings.

   Por lo tanto, desarrolladores de políticas públicas, autoridades reguladoras y legisladores, entre otros, interactuando con la industria, la sociedad civil y los usuarios, deben tomar en consideración el cómputo en la nube como una oportunidad, analizando en profundidad todos los aspectos y cuestiones que se plantean. Cada uno de estos actores pueden adoptar diversas medidas en su ámbito competencial y, en su caso, aportar soluciones que ayuden a una rápida adopción del cómputo en la nube en México.

10. Bibliografía

BSA | The Software Alliance (2013), *2013 BSA Global Cloud Computing Scorecard*, Estados Unidos. Disponible en http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf

Butarelli, Giovanni (2012), *Security and privacy regulatory challenges in the Cloud*, Bruselas. Disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2012/12-03-21_Cloud_computing_EN.pdf

Cisco (2013), *Cisco Global Cloud Index Supplement: Cloud Readiness Regional Details*, Estados Unidos. Disponible en http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/CloudIndex_Supplement.pdf

Comisión Europea (2012), *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa*, COM(2012) 529 final, adoptada el 27 de septiembre de 2012. Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF

Grupo de Protección de Datos del Artículo 29 (2012), *Dictamen 5/2012 sobre la computación en la nube*, adoptado el 1 de julio de 2012. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

Foro Económico Mundial (2011), *Advancing cloud computing: What to do now? Priorities for industry and Governments*, Suiza.

Instituto Mexicano para la Competitividad (2012), *Cómputo en la nube: nuevo detonador para la competitividad de México*, México. Disponible en http://imco.org.mx/wp-content/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

International Working Group on Data Protection in Telecommunications (2012), *Working Paper on Cloud Computing – Privacy and data protection issues -"Sopot Memorandum"-*, Polonia. Disponible en http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083

Kaplan, James; Rezek, Chris y Kara Sprague (2013), *Protecting information in the cloud*, Estados Unidos, McKinsey. Disponible en http://www.mckinsey.com/insights/business_technology/protecting_information_in_the_cloud

Mariscal, Judith y J. Ramón Gil, "El Cómputo en la Nube en México: Alcances y Desafíos para los Sectores Público y Privado", Documento de Trabajo de la División de Administración Pública del Centro de Investigación y Docencia Económicas, núm. 280, octubre 2013. Disponible en: http://www.cide.edu.mx/publicaciones/status/dts/DTAP-280.pdf

Mather, Tim; Kumaraswamy, Subra y Shahed Latif (2009), *Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance*, Estados Unidos, O´Reilly.

McKinsey Global Institute (2013), *Disruptive technologies: Advances that will transform life, business and global economy*, Estados Unidos. Disponible en http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx

Mell, Peter y Timothy Grance (2011), *The NIST Definition of Cloud Computing, Special Publication 800-145*, Estados Unidos, National Institute of Standards and Technology. Disponible en http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Microsoft (2013), *Policymaker Guide to Security, Privacy, and Safety, Building Global Trust Online, volume 3*, Estados Unidos. Disponible en http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/policy_maker_guide.pdf

Microsoft (2011), *Privacy in the Public Cloud: The Office 365 Approach*, Estados Unidos. Disponible en http://download.microsoft.com/download/F/6/9/F6981E42-DEA6-4B14-B578-4DC19007D553/Privacy%20in%20the%20Public%20Cloud%20-%2012-12-11%20final%20standard.pdf

Millard, Christopher (2013), *Cloud computing Law*, Reino Unido, Oxford University Press.

Parlamento Europeo (2012), *Cloud Computing Study*, Directorate General for Internal Policies, Bruselas. Disponible en http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf

Presidencia de la República (2013), *Estrategia Digital Nacional*, México. Disponible en http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf

Quintanilla, Gabriela y J. Ramón Gil-García, "E-Gobernanza y sitios web en la administración pública federal en Canadá y México", Documento de Trabajo de la División de Administración Pública del Centro de Investigación y Docencia Económicas, núm. 282, enero 2014. Disponible en: http://www.cide.edu.mx/publicaciones/status/dts/DTAP%20282.pdf

Recio Gayo, Miguel (2014), *Esquemas de Derecho de las TIC*, España, Tirant lo Blanch.

Recio Gayo, Miguel (2013), *Esquemas de la Ley de Protección de Datos Personales y su Reglamento*, México, Tirant lo Blanch.

Secretaría de la Función Pública (2013), *Cloud Computing*, México. Disponible en http://cidge.gob.mx/wp-content/uploads/2013/03/Cloud-Computing.pdf

Secretaría de Salud, *Manual del Expediente Clínico Electrónico*. Dirección de Información en Salud. México, 2011.

Supervisor Europeo de Protección de Datos (2012), *Opinion of the European Data Protection Supervisor on the Commission´s Communication on "Unleashing the potential of Cloud Computing in Europe"*, Bruselas. Disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

Téllez Valdés, Julio (2013), *Lex Cloud Computing*, *Estudio jurídico del cómputo en la nube en México,* México, Universidad Nacional Autónoma de México.

Documento elaborado con la participación de: