*Privacidad y seguridad en la nube: algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo**

Privacy and Security in the Cloud: Some Legal – Economic Implications from the Cross-Border E-Commerce

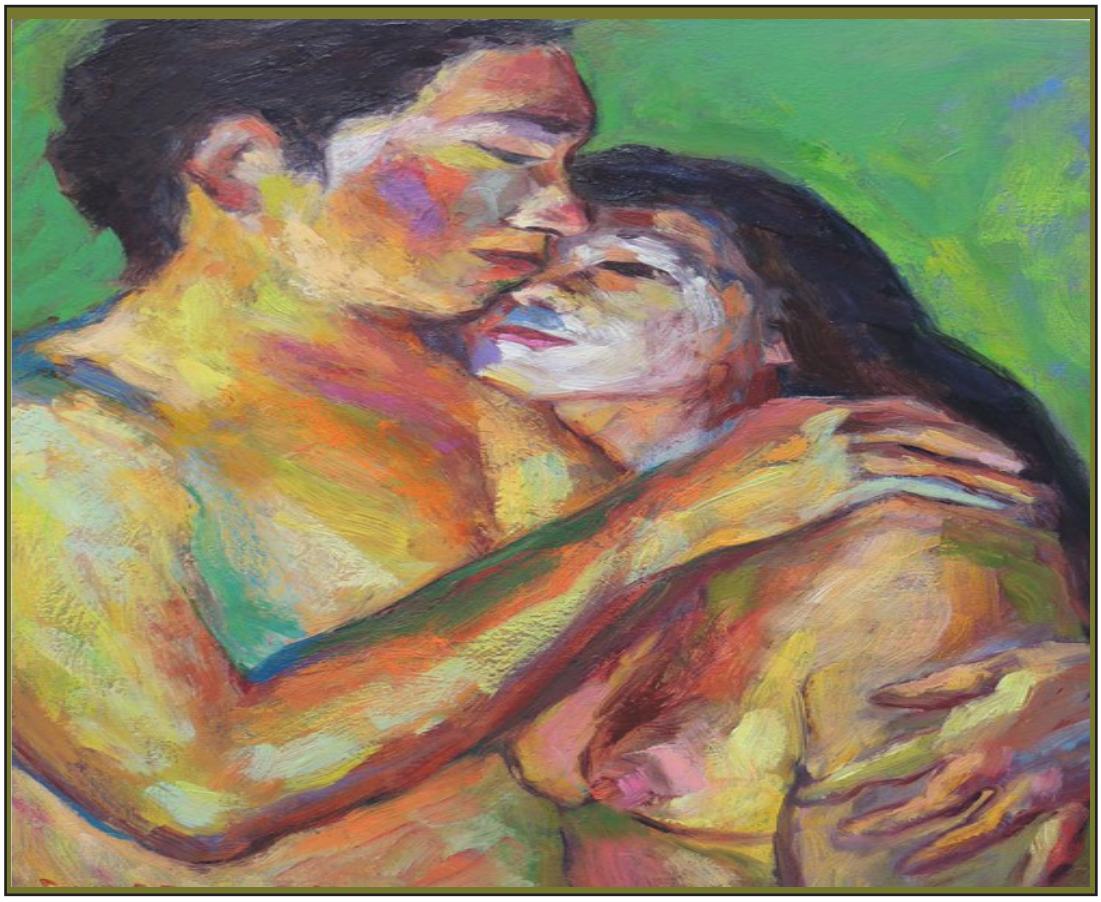
Gladys Stella Rodríguez (LUZ)** https://orcid.org/0000-0003-0063-1411

http://dx.doi.org/10.21503/lex.v18i25.2109

*Avance del proyecto de Investigación registrado ante el Consejo de Desarrollo Científico y Humanístico (CONDES) adscrito al Vicerrectorado Académico de la Universidad del Zulia, intitulado: Principios básicos de la contratación en la nube.

**Abogada, Magister en Planificación y Gerencia de Ciencia y Tecnología. Doctora en Derecho. Postdoctora en Gerencia en las Organizaciones. Profesora de pregrado y postgrado en materia Informática Jurídica y Derecho Informático e Investigadora del Instituto de Filosofía del Derecho de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Coordinadora del Programa de Postdoctorado en Derechos Humanos de LUZ. Investigadora acreditada en el Programa de Promoción para la Investigación e Innovación (PEII), Nivel C. Venezuela.
Correo electrónico: gr1970ve@gmail.com

Lex



Los amantes. Óleo sobre lienzo 61 x 46 cm.
Sonia Estrada Melgarejo (pintora peruana, Ancash)

RESUMEN

Hoy la sociedad del conocimiento demanda una tecnología avanzada. Por ello todo país y organización empresarial que desee ser desarrollada y competitiva ha de incorporar soluciones digitales disruptivas, como servicios completos basados en datos y soluciones de plataforma integrada, centrándose en generar ingresos digitales adicionales y optimizar la interacción y el acceso del cliente. Precisamente en este ecosistema digital único se desarrolla la contratación de servicios en la nube. Aunque son varios los beneficios, también son diversos los retos, uno de los principales en este modelo de acuerdo digital denominado cloud computing o computación en la nube, es la privacidad y seguridad de la información que se maneja. De manera que se expondrá primeramente la naturaleza de este modelo comercial digital, seguidamente se describen las obligaciones y responsabilidades de las partes contratantes; igualmente se destaca la postura de algunos proveedores de este servicio cloud en materia de privacidad y seguridad, ofreciéndose algunas alternativas de contratación para delimitar la responsabilidad de los participantes. De igual forma, se explican algunos aspectos sobre seguridad jurídica en estos contratos; se analizan algunos modelos de acuerdos preferenciales internacionales sobre protección de datos en el ámbito del comercio digital propio de la nube. Finalmente se desatacan los desafíos de América Latina frente a la computación en la nube. Se desarrolla una investigación no experimental de carácter descriptivo, basada en el análisis de contenidos emanados por autores y organismos especializados en TIC, así como se abordan los documentos de la OMC, CNUDMI y CEPAL.

Palabras Claves: *nube, privacidad, seguridad, información, acuerdos preferenciales internacionales, comercio digital.*

ABSTRACT

Today the knowledge society demands advanced technology. Therefore, every country and business organization that wishes to be developed and competitive has to incorporate disruptive digital solutions, such as complete data-based services and integrated platform solutions, focusing on generating additional digital revenue and optimizing customer interaction and access. Precisely in this unique digital ecosystem the contracting of cloud services is developed. Although there are several benefits, the challenges are also diverse, one of the main ones in this model of digital agreement called cloud computing or cloud computing, is the privacy and security of the information that is handled. So the nature of this digital business model will be explained first, then the obligations and responsibilities of the contracting parties are described; It also highlights the position of some providers of this cloud service in terms of privacy and security, offering some contracting alternatives to delimit the responsibility of the participants. Similarly, some aspects of legal certainty are explained in these contracts; some models of preferential agreements at international level on data protection in the field of the digital commerce of the cloud are analyzed. Finally, Latin America's challenges against cloud computing are unleashed. A descriptive non-experimental investigation is developed, based on the analysis of content emanating from authors and organizations specialized in ICT, as well as the documents of the WTO, UNCITRAL and ECLAC.

Key Words: *cloud, privacy, security, information, international preferential agreements, digital commerce.*

I. INTRODUCCIÓN

Con el paso del tiempo, la implementación de las Tecnologías de Información y Comunicación (TIC) en cualquier organización sea pública o privada ha generado el desarrollo de un nuevo paradigma organizacional, y es esto uno de sus principales atractivos y donde principalmente radica la importancia de estas herramientas, que cada vez inciden en un mejor funcionamiento de estas organizaciones al emplear prácticas de planificación y mejoramiento de procesos, los cuales sucesivamente afectan el rendimiento operativo organizacional.[1]

Según Gómez y Martínez[2] "toda organización o empresa que logre la internacionalización ha requerido herramientas entre otras de carácter tecnológico capaces de soportar eficientemente este tipo de procesos de intercambio comercial, dadas las diferencias significativas entre las partes, asociadas al idioma, distancias, marcos legales, culturas, monedas, geografía, entre otros aspectos". Las TIC permiten además aumentar la eficiencia a través del ahorro en tiempo totales del proceso y ahorros en gasto de desplazamiento, brinda soporte en la toma de decisiones, maneja diferentes niveles de formalismo y formas de contratar la contraparte. Adicional a esto, las TIC facilitan la construcción de relaciones, la gestión de información y el planeamiento de alternativas de negociación.[3]

Actualmente es natural encontrar acuerdos donde se contratan multiplicidad de servicios en línea donde estas herramientas tecnológicas resultan fundamentales para el desarrollo de cualquier emprendimiento comercial y lo cual ha dado origen al denominado comercio electrónico o comercio digital.

El comercio electrónico o *e-commerce* en inglés, puede ser definido como "la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos"[4]. Pese a que esta

1. E. Kleinschmidt, U. de Brentani, U y S. Salomo, "Performance of global new product development te programs: A resource – based view", J*ournal of Productin novation management*, 24, vol.5 (2007), 419-441.

2. Gómez y Martínez, *Negociación Internacional medios de cobro y pago,* (Madrid: 1 era edición, 2003).

3. José Jaime Baena y José Alejandro Cano, "Uso de Tecnologías de Información y Comunicación para la negociación" ¿Ventajas para las empresas colombianas? *Ciencias Estratégicas*, 22 (32).(2014), 1-29.

4. Véase https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm

definición es previa a la irrupción masiva del comercio electrónico, es lo suficientemente amplia para capturar sus distintas modalidades. El comercio electrónico puede realizarse entre agentes situados dentro de un mismo país o en distintos países. El presente trabajo por la naturaleza del negocio que involucra el *cloud computing*, se enfoca en la segunda modalidad, conocida como comercio electrónico transfronterizo, pues la naturaleza de esta forma de acuerdo involucra servicios prestados a través de la red de redes.

El comercio electrónico incluye tanto la adquisición de bienes físicos utilizando medios digitales (por ejemplo, la compra de un par de *jeans* en la plataforma Amazon) hasta el comercio de bienes y servicios digitales (por ejemplo, la adquisición en línea de un libro electrónico o de servicios financieros, de plataforma, software, infraestructura etc.), estos últimos ejemplos implican actividades propias de este modelo de negocios conocido como computación en la nube.

Para comprender las distintas formas que puede asumir este fenómeno del *e-commerce*, resulta útil el marco conceptual propuesto por López-González y Jouanjean.[5] Este se basa en tres elementos de cada transacción transfronteriza: i) la modalidad de entrega del bien o servicio (digital o física); ii) el tipo de flujo involucrado (bienes o servicios); y iii) los actores involucrados (empresas, consumidores o gobiernos). A los fines del presente documento la computación en la nube significa un negocio de entrega digital de servicios entre los proveedores de servicios de la nube y los usuarios de la misma.

Partiendo de lo anterior la computación en la nube, involucra comercio electrónico pues se trata de una nueva gestión de negocios digitales que comprende una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la misma Administración Pública.

La *cloud computing* como se le conoce en inglés, permite al usuario optimizar la asignación y el costo de los recursos asociados a sus necesidades de tratamiento de información.

Y es que probablemente el principal elemento común a las distintas modalidades del comercio electrónico es el valor estratégico de los datos. Para López-González y Jouanjean[6], dicho valor asume múltiples formas: los datos son un medio de producción, un activo transable, y el medio a través del cual se comercian diversos servicios y se organizan las cadenas globales de valor. En efecto, y coincidiendo con la irrupción del comercio electrónico transfronterizo, los flujos transfronterizos de datos han tenido un crecimiento exponencial en lo que va transcurrido de este siglo.

5. Javier López-González y Marie-Agnes Jouanjean, "Digital trade. Developing a framework for análisis", OECD *Trade Policy Papers*, No 205, (2017), 54-55, OCDE, París.

6. Javier López-González, y Marie-Agnes Jouanjean, op.cit., 59.

Entre 2002 y 2012, el tráfico transfronterizo en Internet aumentó 60% al año, y se estima que hacia 2025 podría multiplicarse por ocho con respecto a su nivel en 2015.[7]

En esta modalidad de comercio electrónico donde el usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecosto asociado a dichas situaciones; involucra beneficios, pero también significa riesgos, especialmente en materia de protección y seguridad de los datos personales.

Por ello en el presente trabajo se hará referencia a la naturaleza de la contratación en la computación o la nube, de igual forma se explicara las obligaciones y alcance de la responsabilidad por las partes contratantes, seguidamente se expone qué significado tiene la privacidad y seguridad en los contratos de servicios en la nube, algunas consideraciones de seguridad jurídica, así mismo que posturas acogen en los acuerdos comerciales los grandes bloques y Estados de la comunidad internacional en materia de protección de datos en el marco del comercio electrónico transfronterizo y, finalmente que proponen algunos organismos internacionales especializados en cuanto a alguna perspectiva de regulación jurídica, con especial referencia a la privacidad y seguridad en un ambiente de negocios de este grado de complejidad.

II. COMPUTACIÓN EN LA NUBE. NATURALEZA

En un entorno de *cloud computing* la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades. En función del modelo utilizado, los datos pueden no estar realmente en manos del contratista, toda vez que la propiedad, el mantenimiento y gestión del soporte físico de la información, los procesos y las comunicaciones pueden encontrarse en manos de terceros.

El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales.[8]

De esta forma, el *cloud computing* representa una nueva forma de utilizar las TIC, que se basa en emplear técnicas ya existentes de una forma innovadora y, sobre todo, a una nueva escala. Esto

7. Susan Lund y James Manyika, "How digital trade is transforming globalization". E15 Expert Group on the Digital Economy, ICTSD-World Economic Forum, (2016). Acceso el 10 de enero de 2019 desde, http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation/

8. "¿Qué es el *Cloud* Computing?" En: *Guía para clientes que contraten servicios de cloud computing*, ed. por. Agencia Española de protección de Datos, (Madrid: Agencia Española de protección de Datos, 2013), 5.

último es lo que la hace realmente distinta, ya que permite el uso de recursos de *hardware, software,* almacenamiento, servicios y comunicaciones que se encuentran distribuidos geográficamente y a los que se accede a través de redes públicas, de forma dinámica, cuando se necesita, mientras se necesita y abonando una tarifa (cuando no es gratuita) sobre lo que se consume; es decir, proporcionando a sus clientes un servicio de tecnologías de información bajo demanda.[9]

Este tipo de acuerdo posibilita el *outsourcing* de la computación y servicios sin externalizar su control y se basa en utilizar un modelo de pago por uso, con acceso *Web* a Internet con banda ancha. La industria del *cloud computing* representa un gran ecosistema con muchos modelos, fabricantes y nichos de mercado.

Se trata de una modalidad de servicios y aplicaciones que operan desde internet, bajo este esquema la información se almacena de manera permanente en servidores de internet.

La computación en la nube permite que los consumidores y las empresas gestionen archivos y utilicen aplicaciones sin necesidad de instalarlas. Esto genera múltiples beneficios para los usuarios, empezando por la posibilidad de acceder a la información y a las aplicaciones desde cualquier lugar, bien sea su casa, oficina, aeropuerto, etc., donde solamente requerirán de su dispositivo personal y una conexión a internet. .Los servicios de computación en la nube, pueden significar una o más prestaciones tales como infraestructura, plataforma y *software* y en términos de uno o más modelos de implementación como público, privado, híbrido y comunitario.

Herrera[10] **señala:**

> La "nube" o *cloud computing* es un modelo de gestión tecnológica basado en diversos servicios informáticos. Sus posibilidades son amplísimas, tanto para utilizar programas, plataformas, infraestructura y otras funcionalidades. Basta ver como surgen, además de las ya clásicas tipologías de *SaaS* (software como servicio), *IaaS* (infraestructura como servicio) y *PaaS* (plataforma como servicio), otras variantes como servicios de *big data,* de comunicaciones unificadas, de contenedores, de seguridad, de gestión y de almacenamiento, y nada impide que aparezcan más.
>
> Ejemplos cercanos hay muchos, como el almacenamiento de datos en *Google Drive, Dropbox, iCloud, Onedrive, Amazon Web Services*, entre otros; el hospedaje de sitios *web*; el back up de bases de datos; los site de contingencia para recuperación de desastres; el análisis de *big data;* la conexión de dispositivos de Internet de las cosas, por mencionar algunos *servicios cloud.*

9. "¿Qué es el *Cloud* Computing?" op. cit , 6.

10. Rodolfo Herrera, "¿La Nube es segura para los datos personales?" Revista Seguridad, 8 (2018). Acceso el 20 de septiembre de 2018 desde,
https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

Sin embargo, más allá de las innegables ventajas técnicas y de gestión que puede ofrecer la nube, el tema de la seguridad de la información es esencial y, dentro de éste, el de la protección de datos personales. Actualmente se percibe como la necesidad más urgente del paradigma en evolución *cloud computing,* la protección desde sus dos perspectivas: seguridad y privacidad.

Lo anterior es más urgente debido a que en la mayoría de los casos, sin embargo, lo que se oferta son contratos de adhesión, constituidos por cláusulas contractuales cerradas, en las que el proveedor de *cloud* fija las condiciones con un contrato tipo igual para todos sus clientes, sin que el usuario tenga ninguna opción para negociar sus términos. Este último caso es el más común, sobre todo cuando se encuentra el cliente en una situación de desequilibrio (p.ej.: una pyme frente a un gran proveedor), aunque hay que tener en cuenta que esto no eximirá, a ninguno de los dos, de las responsabilidades.

Los proveedores de infraestructuras como centros de supercomputación, grandes empresas de telecomunicaciones y empresas de *hosting*[11] disponen de las tecnologías, herramientas y modelos de gestión para optimizar la asignación de sus recursos ofreciendo nuevas oportunidades de negocio en los mercados emergentes del *cloud computing*. Pero resulta conveniente precisar el alcance de la privacidad y establecer las responsabilidades en el tratamiento de los datos bajo este innovador modelo de negocio que utiliza TIC en alto grado.

III. ACTORES EN LA CONTRATACIÓN DE SERVICIOS EN LA NUBE: OBLIGACIONES Y RESPONSABILIDADES

Los riesgos asociados con los niveles apropiados de seguridad de datos y privacidad en las diferentes capas de la computación en la nube son desafiantes para la organización del cliente. Esto se debe a la creciente importancia de los datos e información para las empresas y a las diferentes configuraciones de servicios de computación en la nube y modelos de implementación que son posibles.

La nube ofrece a las empresas y a los consumidores múltiples beneficios: el ahorro de costos, la flexibilidad y el acceso móvil a la información encabezan la lista. Sin embargo, por otro lado, plantea preocupaciones sobre la protección de datos y la privacidad; especialmente en torno a la información de identificación personal (PII), entendiendo por PII aquella que incluye cualquier tipo de información que pueda identificar a un usuario específico. Los ejemplos más obvios son los nombres y datos de contacto. Pero también se puede pensar fácilmente en registros médicos, las direcciones IP y los estados bancarios.

11. Servicio que ofrecen algunas compañías (los webhost) en Internet que consiste en ceder un espacio en sus servidores para subir (alojar, hostear) un sitio web para que pueda ser accedido en todo momento en forma *online*, Acceso el 21 de enero de 2019 desde www.alegsa.com.ar

En este sentido la Secretaria de las Naciones Unidas elaboro un Modelo de capítulos de un posible texto de orientación sobre los aspectos contractuales de la computación en la nube[12], en su propuesta de Guía de orientación señala que son varios los riesgos de este nuevo modelo de trabajo y particularmente se refiere a:

> …. d) la circulación de datos a través de fronteras. Proteger los datos personales y otra información delicada, al igual que respetar el derecho a la privacidad, es especialmente difícil en infraestructuras compartidas a las que los gobiernos pueden quizás acceder. La falta de información sobre la ubicación de los datos y el número de interesados directos que participan en el suministro de los servicios de computación en la nube acentúan los riesgos de violación de los datos;
>
> e) la pérdida o alteración de las credenciales de acceso a los servicios de computación en la nube, que es una de las causas más comunes de pérdida de datos o de divulgación de datos a personas no autorizadas;….[13]

Debido a las diferentes configuraciones y modelos de implementación de computación en la nube se puede afirmar que no es solo una de las partes la responsable de la seguridad y privacidad de datos en un servicio de computación en la nube. Además es muy probable que muchas organizaciones de clientes no sean del todo conscientes y no tengan estrategias adecuadas de gestión de riesgos y mitigación para enfrentar temas de seguridad de los datos y la privacidad.

Por otra parte en el documento de la Secretaria de la ONU (A/CN.9/WG.IV/WP.142)[14] se señala que:

> Los interesados directos que participan en un modelo de solución en la nube son varios: el proveedor de servicios de nube, el cliente, los terceros cuya información tiene el cliente, etc. Cualquier ambigüedad en la definición de las funciones y responsabilidades relacionadas con la propiedad de los datos, el control del acceso, el mantenimiento de la infraestructura y demás elementos puede generar riesgos de seguridad y de otro tipo. No asignar con claridad

12. El presente modelo de capítulos no refleja las opiniones de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) ni de su Grupo de Trabajo. Es el resultado de la labor de investigación realizada por la Secretaría y de las consultas que esta mantuvo con expertos, y se basa también en los documentos A/CN.9/823 y A/CN.9/856. El modelo de capítulos se presenta en forma de proyecto para que el Grupo de Trabajo lo examine. A/CN.9/WG.IV/WP.142. Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional Grupo de Trabajo IV (Comercio Electrónico) 55º período de sesiones Nueva York, 24 a 28 de abril de 2017, 1-20.

13. A/CN.9/WG.IV/WP.142 Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional Grupo de Trabajo IV (Comercio Electrónico) 55º período de sesiones Nueva York, 24 a 28 de abril de 2017, 17.

14. Ídem.

las responsabilidades puede tener consecuencias más graves cuando se utilizan recursos informáticos de terceros.

Bajo lo anterior resulta fundamental en los servicios en la nube determinar las exigencias de seguridad que deben implementar dos tipos de sujetos: Por un lado, los "Responsables de los registros", es decir, quienes tienen autorización para utilizar los datos y toman las decisiones sobre lo que hacen con ellos y, por el otro, los 'Proveedores de servicios en la nube', contratados por los responsables para que realicen para ellos algún tratamiento sobre esos datos. Esos proveedores de servicios *cloud* asumen, en ese caso, el papel de "Encargados del tratamiento" o "Mandatarios".

A continuación algunos aspectos en cuanto a las obligaciones de estos actores a tener en cuenta, cuando realizan tratamiento de datos personales en servicios cloud.

a. Obligaciones para el responsable del registro

En algunas legislaciones como la chilena su ley N°19.628 define al "responsable del registro" como aquella persona natural, empresa u órgano público que tiene una base de datos con información de los titulares y toma decisiones sobre su utilización".

En este punto es importante referirse a las obligaciones legales que debe cumplir el responsable si desea contratar un servicio *cloud computing* como apoyo al tratamiento de los datos. Por ejemplo, si desea entregar la base de datos para que una empresa *cloud* la respalde o para que le proporcione análisis de dichos datos.

Si se parte del principio de buena fe, todos tenemos derecho a tratar datos personales de otros, para fines lícitos. Para ello, por regla general, necesitamos autorización del titular de forma previa.

Ahora bien puede suceder que el responsable del registro utilice los datos legítimamente y pueda estimar necesario acudir a un tercero, para que le preste algún servicio de apoyo a su tratamiento.

Esa posibilidad de externalizar tratamientos de datos, pudiese exigir una formalidad bien concreta: como la de suscribir un contrato de mandato específico.

Al parecer, se confían en que los contratos *cloud* incluyan alguna cláusula de confidencialidad y otra sobre responsabilidad por incumplimientos y daños, pero eso no es suficiente para cumplir la ley.[15]

Este mandato obligatorio que debe existir entre el responsable del registro y el proveedor de servicios en la nube no puede ser genérico. Tiene que describir con detalle qué tipo de datos personales se entregan, para qué serán utilizados, cuánto tiempo los procesará, de qué manera serán devueltos

15. Herrera, Rodolfo "¿La Nube es segura para los datos personales?", op. cit.

y cómo se eliminarán, junto con la prohibición de utilizarlos para otros fines distintos al servicio contratado y, por supuesto, el impedimento de comunicarlos a terceros. Todo ello en atención a lo establecido en materia de protección de datos a nivel internacional.

La existencia de este contrato por escrito busca dejar evidencia de que el tratamiento de datos que realice el proveedor de la nube es legítimo, pese a no contar con autorización previa del titular. Del mismo modo, protege al responsable del registro aclarando que no ha realizado una comunicación no autorizada de datos a un tercero y que, en ese sentido, no ha infringido sus obligaciones de cuidado sobre la información personal de los titulares.

No hay que olvidar que ese mandato explicita que los datos no los usa el mandatario para sí mismo, sino para prestar un servicio al responsable del registro (su mandante), que sí cuenta con autorización previa del titular de los datos para tratarlos.

Sin embargo, no siempre el Responsable del registro tiene clara esta obligación legal y suele limitarse a suscribir los contratos tipo o de adhesión que regulan muchos servicios *cloud computing*. Al parecer, se confían en que tales contratos incluyan alguna cláusula de confidencialidad que pese sobre el proveedor de la nube y otra sobre responsabilidad por incumplimientos y daños, pero eso no es suficiente para cumplir la obligación legal. Se requiere suscribir un contrato de mandato específico para el tratamiento de los datos.

Lo anterior implica que la eficacia de la protección de datos personales en servicios en la nube se puede apoyar en la autorregulación contractual.

b. Obligaciones para el proveedor de servicios cloud, como mandatario o encargado del tratamiento

La mayoría de los marcos regulatorios en materia de protección de datos, no regulan suficientemente la figura del Encargado del tratamiento. De hecho, ni siquiera lo menciona como tal. Aunque se trata de uno de los actores relevantes dentro de las obligaciones de cuidar los datos personales.

Sin perjuicio de ello, y ante la insuficiente normativa, se cree que la referencia de contar con un contrato de mandato escrito y específico sobre la labor que realizará el mandatario, puede ser un punto de inicio eficaz para la protección de los derechos de los titulares de datos, obviamente en la medida que dichos contratos estén bien construidos.

Para entender un poco más el rol del mandatario, éste recibe los datos personales sin una autorización directa del titular, sino que lo hace mediante un encargo específico del Responsable del registro. Además, los recibe para utilizarlos exclusivamente respecto del encargo, es decir, no los puede emplear para sus propios fines, ya que de lo contrario, junto con extralimitar el contrato de mandato, pasaría a ser un responsable de tratamiento sin autorización del titular, es decir, que estaría utilizando los datos infringiendo la ley.

Ahora bien, cuando todo está en regla, es decir, se cuenta con un contrato de mandato bien hecho, el Encargado o Mandatario asume las mismas obligaciones de cuidado que pesan sobre el Responsable del registro, por lo que es importante detenerse en esta obligación.

De acuerdo al tratamiento y protección de los datos personales a nivel de la doctrina y la legislación especial en la temática se tiene una obligación más bien genérica sobre cuidar los datos personales, a partir de la cual el responsable del registro y el proveedor de servicios de la nube deben adoptar medidas de seguridad.

No obstante, la legislación no indica qué medidas deben implementarse para proteger los datos, ni mucho menos qué controles corresponden según el tipo de dato personal de que se trate, por ejemplo, si son datos de mera identificación o si son datos sensibles.

En tales circunstancias, como la obligación existe, hay que cumplirla y para ello, se recomienda adoptar estándares técnicos internacionales de seguridad de la información.

Dentro de los estándares más adheridos se encuentran las normas de la serie ISO/IEC 27.000. De hecho, la norma ISO/IEC 27.018, de 2014[16], precisamente se refiere a requisitos para la protección de información de identificación personal en sistemas de computación en la nube.

La norma ISO/IEC 27.018 es muy cercana a la ISO/IEC 27.002, sobre buenas prácticas de seguridad de la información, aunque con ciertos énfasis en determinados controles e incluyendo algunos nuevos, a partir de los riesgos propios de los servicios en la nube.

Por ejemplo, en el dominio de seguridad en las operaciones pone el acento en separar los entornos de desarrollo, en realizar copias de seguridad y en los registros de eventos.

Además, se incluyen controles tales como no utilizar los datos para fines de *marketing* y publicidad; eliminar los archivos temporales; notificar al cliente cuando se divulgan y cuando se violan los datos; informar sobre subcontratistas; establecer políticas para el traslado y eliminación de los datos; establecer acuerdos de confidencialidad con quienes acceden a los datos; cifrado de los datos; destrucción de medios de comunicación impresos con datos; identificaciones únicas para los clientes *cloud*; entre otras.

Frente a estas medidas y normas de carácter internacional, proveedores importantes, como *Amazon, Google y Microsoft* ya han resaltado que la seguridad es una responsabilidad compartida donde ellos se hacen cargo de lo que está fuera de la nube y los usuarios son, en gran parte responsables, de

16. Utilizada conjuntamente con ISO/IEC 27001, ISO/IEC 27018 ha sido publicada para permitir que proveedores de servicios *cloud* cuya infraestructura está certificada con esta norma, le puedan decir a sus clientes actuales y potenciales que sus datos están garantizados y que no serán usados para ningún propósito para el cual no se dé expresamente su consentimiento.

la seguridad en la nube. Para mayor referencia.[17]

c. Responsabilidad en la nube desde la perspectiva de algunos proveedores de Servicios Cloud en materia de privacidad y seguridad

Claramente cuando se examina el Modelo de Responsabilidad Compartida de Servicios *Web* de Amazon (AWS en ingles), su enfoque de la responsabilidad es principalmente en Infraestructura como Servicio (IaaS).[18] Es evidente que hay una responsabilidad significativa en el cliente o consumidor de los servicios en la nube de AWS para realizar su evaluación debidamente y garantizar que los controles están en su lugar para asegurar el nivel apropiado de seguridad y privacidad de los datos, particularmente en Plataforma como Servicio (PaaS)[19] y más en Software como Servicio (SaaS)[20] y dependiendo del tipo de modelo (s) de implementación en la nube utilizado[21], bien sea de despliegue o de servicio, se complica aún más las cosas.

Microsoft también ve la seguridad de los servicios en la nube como una responsabilidad compartida entre el CSP, siglas del inglés Cloud Service Provider o Proveedor de Servicios en la Nube y el cliente, el cual se basa en gran medida en el estándar *PCI DSS 3.2.1*.[22]

Estas empresas prestadoras de servicios *cloud* que se ejemplifican, ven a la clasificación de datos como responsabilidad de la organización del cliente en los tres modelos de servicios en la nube. Los niveles más bajo de la red que son la seguridad física, la infraestructura del *host* y los controles de red, son principalmente responsabilidad del proveedor de servicios en la nube.

17. Ver https://aws.amazon.com/es/compliance/shared-responsibility-model/, https://cloudgoogle.com/security/ y https://gallery-technet.microsoft.com/shared-Responsabilities

18. El proveedor ofrece recursos como capacidad de procesamiento, de almacenamiento o comunicaciones, que el usuario o cliente puede utilizar para ejecutar cualquier software; desde sistemas operativos hasta aplicaciones.

19. Al usuario se le permite desplegar aplicaciones propias (adquiridas o desarrolladas por el propio usuario), el proveedor ofrece la plataforma de desarrollo y las herramientas de programación.

20. El proveedor proporciona la infraestructura de hardware, el producto de software, e interactúa con el usuario a través de un portal de acceso. El mercado de SaaS es muy amplio y comprende desde el email basado en la Web, hasta el control de inventarios y el procesamiento de bases de datos. Es común en el mercado sostener que los servicios en la nube, son aquellos en los que el proveedor garantiza el acceso a un disco rígido, independiente de los ordenadores de los usuarios, al cual se puede llegar desde cualquier lugar del mundo, conexión a la web mediante. PCs, tabletas y celulares están incluidos, gracias a Internet.

21. Ver http://dx.doi.org/10.21503/lex.v17i23.1674

22. El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment CardIndustry Data Security Standard – PCI DSS) es un estándar de seguridad publicado por el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) y orientado a la definición de controles para la protección de los datos del titular de la tarjeta y/o datos confidenciales de autenticación durante su procesamiento, almacenamiento y/o transmisión. Actualmente, se encuentra en la versión 3.2.1, publicada el 17 de mayo de 2018.

Sin embargo, claramente este modelo de responsabilidad compartida indica que la responsabilidad de los datos y la seguridad residen en gran parte con la organización del cliente.

En la plataforma *Google Cloud* puede verse el *Customer Responsibility Matrix*. Este también enfatiza que la seguridad es una responsabilidad compartida. Utilizando el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) *Google* detalla sus responsabilidades como proveedor de servicios en la nube y las de la organización del cliente que utiliza una Matriz de Responsabilidad PCI-DSS. *Google* se adhiere a los requisitos de PCI-DSS establecidos para un proveedor de servicios de nivel 1. En otras palabras, se requiere que *Google Cloud Plataforma* (GCP) cumpla con PCI DSS y todos los requisitos que se aplican directamente a un proveedor de servicios.

Google también deja muy claro su rol como proveedor de servicios en la nube, servicio en el que:

• Algunos de los requisitos de PCI DSS son responsabilidad exclusiva y deben ser implementados por la plataforma Google Cloud.

• Otros de los requerimientos de PCI DSS son de exclusiva responsabilidad y deben ser implementados por el cliente.

• Otros requisitos son responsabilidad compartida y deben ser implementados por ambas partes.

En este sentido, estas plataformas proponen que el principio de responsabilidad compartida para la seguridad de los datos y la privacidad en la computación en la nube es una perspectiva importante a considerar aplicando los principios clave del *Bright Internet Framework.*[23]

Lo anterior supone tener mayor cuidado por parte del responsable del registro, coincidiendo con Herrera[24] que la seguridad de los datos personales en la nube descansa principalmente en los contratos que se suscriban, tanto para la prestación del servicio *cloud* propiamente, como también, respecto del contrato de mandato que debe existir entre el responsable del registro y la empresa *cloud*.

Por su parte, vale indicar que en algunos países no existe una ley especial de protección de datos como es el caso de Venezuela o aun existiendo leyes como el caso de Chile, la misma no contiene normas especiales para el tratamiento de datos en la nube, ni siquiera cuando el servicio aloja los datos fuera del territorio nacional. Y aun existiendo normas, lo cierto es que cuestiones como la recolección,

23. Bright Internet tiene como objetivo establecer una plataforma segura de Internet que pueda identificar y eliminar de manera preventiva los orígenes anónimos maliciosos de los delitos informáticos y los terrores mundiales. No obstante, Bright Internet también tiene como objetivo mantener la libertad de expresión y la protección de la privacidad que pueden violar las medidas preventivas. La investigación para Bright Internet estudia la validez de los principios de Bright Internet y diseña sistemas y tecnologías que pueden cumplir los objetivos conflictivos de manera efectiva y eficiente. El espectro de diseño de Bright Internet abarca tecnologías y estándares, leyes y políticas, y colaboración internacional y estructura de gobernanza global. http://brightinternet.org

24. Rodolfo Herrera, "¿La Nube es segura para los datos personales?", op. cit.

el uso y publicidad de la data almacenada en la nube, sin dejar de mencionar la probabilidad que el proveedor contrate servicios de *outsourcing* en el extranjero, no están reguladas de una manera completa y coherente, especialmente en Latinoamérica. Distinto es el caso en la Comunidad Europea, donde se publicaron las *Cloud Service Level Agreement Guidelines Standardisation.*[25]

En este punto, se recomienda que los proveedores de servicios *cloud* implementen estándares técnicos internacionales de seguridad, incluso con mayor rigurosidad, como ocurre con la norma ISO/IEC 27.018, dado el mayor riesgo que puede representar el ambiente *cloud* para el titular de los datos.

d. Algunas recomendaciones de seguridad jurídica a considerar en los contratos de servicios en la nube

Resulta obvio que para celebrar un acuerdo donde ambos actores: Responsable de la Data o registro y el Proveedor de servicios en la nube, vean garantizados sus deberes y derechos, se tendrá que acudir a la asesoría de un experto en seguridad informática, algunos consejos ofrece Cobo[26], a continuación:

• "Formalización de cuerpos normativos, procesos y procedimientos internos de gestión de la seguridad, que permiten disponer de un modelo de control homogéneo y común a cualquier tipología de servicio."

• "Incorporación de cláusulas de seguridad en el contrato. Tradicionalmente, la seguridad ha estado presente en los contratos, principalmente, a través del establecimiento de cláusulas generales de confidencialidad y protección de datos de carácter personal. Los nuevos modelos de servicio requieren de una mayor especificación y nivel de detalle en materia de seguridad en los contratos y de una mayor participación de los responsables de seguridad en la confección de los mismos."

Este punto es realmente conveniente, propone la obligación por parte del proveedor, de auditar dichos mecanismos regularmente por medio de un auditor independiente y consensuado por las partes (contratantes). Se coincide en la necesidad de una auditoría independiente, que surja de una cláusula contractual es el remedio anticipado para un sin fin de conflictos. Pero, como al autor citado, también es conveniente reservar el derecho de su cliente a una auditoría propia, que incluya un test de penetración.[27]

25. Ver European Commission Issues Cloud Service level Agreement Standarization Guidelines, del 26 de Junio de 2014

26. Juan Cobo, "IT Seguridad en "la Nube": ¿Cómo controlar lo que no controlas?" *Red Global de Conocimientos en Auditoría y Control Interno Auditool*, ISSN ON LINE: 2665-3508, publicada el 07 de enero de 2011. Acceso el 23 de enero de 2020 desde,
https://www.auditool.org/blog/auditoria-de-ti/350-it-seguridad-en-la-nube-icomo-controlar-lo-que-no-controlas

27. Definidos como: "Las pruebas de penetración (también llamadas "pen testing") son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar", definición *online* de *Techtarget.*

En este caso, el de la auditoría de parte, debe pactarse el procedimiento, la identificación de responsables, y las notificaciones que dentro de plazos determinados, deben cursarse. Resulta claro que un uso abusivo de esta herramienta puede interrumpir la continuidad del encargo o mandato del proveedor de servicios.

> "Adicionalmente, dice el autor[28], al clausulado de seguridad, el contrato debería recoger acuerdos de nivel de servicio en materia de seguridad sobre determinados aspectos, cuya aplicación dependerá de la naturaleza del servicio prestado, tales como los siguientes: tiempos de respuesta en configuraciones y parametrizaciones de seguridad; idoneidad de las configuraciones y parametrizaciones de seguridad; nivel de infecciones, intrusiones y exposiciones de información; bastionado y nivel de actualización y parcheado de las plataformas; tiempo de respuesta en la identificación, notificación, mitigación y resolución de incidentes; nivel de incremento de incidentes de seguridad; nivel de cumplimiento en auditorías de seguridad, y nivel de pro actividad por parte del proveedor".

IV. PRIVACIDAD Y SEGURIDAD (CONFIANZA) EN LA CONTRATACIÓN DE SERVICIOS EN LA NUBE

Una de las principales formas de generar confianza, entre proveedores y usuarios (clientes), es ponerse de acuerdo sobre quién obtiene qué derechos, y quién asume responsabilidades de lo que pase con la información en la nube.

La novedad es la misma de siempre: la preocupación; ya que muchos de los asuntos de privacidad en la nube son objeto de constantes inquietudes acerca de:

• La información dispuesta a través de servidores y aplicaciones externas.

• La manera en cómo las personas y las organizaciones conforman su postura ante las políticas aplicables, regulaciones estándar, contratos y políticas de intercambio.

• La metodología con la que la información es puesta en la nube y cómo permanece en ella, así como también la certidumbre de que al borrarla, realmente sea así.

• Las palabras clave generadas para mostrar y acceder a la información para modificarla, copiarla u otros usos.[29]

Estas consideraciones deberían llevar a la difusión de mecanismos reguladores que orienten a los usuarios a un empleo más definido de estos servicios, así como de las ventajas y desventajas que pueden encontrar en las políticas de privacidad que los proveedores otorgan.[30]

28. Juan Cobo, "IT Seguridad en "la Nube": ¿Cómo controlar lo que no controlas?" *Red Global de Conocimientos en Auditoría y Control Interno Auditool*, op. cit.

29. Julio García y Galvy Cruz, "Privacidad de la información en la Nube". Revista Seguridad 8, (2018) 1, Acceso el 20 de septiembre de 2018 desde, https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

30. Julio García y Galvy Cruz, op. cit., 2.

La introducción de criterios de privacidad es esencial para resolver las preocupaciones de los usuarios. Algunas políticas de privacidad de estos sitios de almacenamiento son a la vez que explicitas, requirentes para los usuarios. Un ejemplo se encuentra en la Declaración de derechos y responsabilidades de Facebook, en la cual la empresa específica que la propiedad intelectual del contenido es del usuario, pero al aceptar las condiciones, se le otorga a la empresa un permiso extensible de uso del contenido, mismo que se cancela sólo con la desactivación o eliminación de la cuenta.

El correcto establecimiento de políticas de privacidad de la información en este tipo de servicios (sea SaaS, PaaS, IaaS) evita que datos como: nombre, tarjeta de crédito, registros biométricos, etc., puedan ser usados para distinguir o rastrear la identidad de un individuo; y éstos se utilicen para cometer fraudes, robos de identidad, envío de correo no deseado, entre otros.

No obstante, falta preocupación de los proveedores respecto a las consecuencias de no tener control adecuado sobre la privacidad de la información de sus clientes; un hecho concreto ocurre en la declaración de políticas de *Amazon o Facebook*, como se indico antes.

Los miedos de los usuarios están justificados, pues no existe una figura legal que establezca discernimientos sobre cuándo una información puede hacerse pública, cuándo debe estar asegurada, o bien, cuándo es robada.

El criterio de consentimiento aplicado a las políticas de uso de los servicios de cómputo en la nube podría servir para dar contexto y referencia sobre lo que usuarios podrían exigir en caso de presentarse una infiltración o violación a las sesiones privadas en este tipo de servicios, aunque se debe estar consciente que la amenaza siempre estará presente.

La computación en nube puede representar una mejora en la privacidad de información de aplicaciones no críticas. Sin embargo la transparencia es crucial, los usuarios deben poder evaluar y comparar las prácticas de seguridad de cada proveedor. Actualmente, la migración de información crítica continúa siendo muy riesgosa (incluso en nubes privadas).

Desde esta perspectiva, las Naciones Unidas[31] trabaja en un Acuerdo Marco que permita:

> "promover el comercio transfronterizo sin soporte de papel permitiendo para ello el intercambio y el reconocimiento mutuo de datos y documentos relacionados con el comercio y facilitando la interoperabilidad entre las ventanillas únicas nacionales y subregionales y otros sistemas de comercio sin soporte de papel, con la finalidad de que las operaciones comerciales internacionales sean más eficientes y transparentes y al mismo tiempo se mejore el cumplimiento de los reglamentos".
>
> "El artículo 5 del Acuerdo Marco establece "la mejora del entorno de confianza transfronterizo" (párrafo 1 g)) como uno de los principios generales por los que se guía el Acuerdo".

31. A/CN.9/WG.IV/WP.141 Asamblea General de las Naciones Unidas Comisión de las Naciones Unidas para el Derecho Mercantil Internacional Grupo de Trabajo IV (Comercio Electrónico) 55º, período de sesiones, Nueva York, 24 a 28 de abril de 2017. Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza.

En esta propuesta se plantea con respecto al comercio transfronterizo el tema de la seguridad y la confidencialidad de la información transmitida por Internet. Se utiliza un sistema de gestión de la identidad para resolver esa cuestión. En consecuencia se busca el establecimiento de un entorno de confianza transfronterizo (ECT) en la esfera del comercio electrónico que contribuya a la simplificación de los trámites y al desarrollo del comercio internacional, y permita a los países participantes simplificar el proceso de identificación y la gestión de la identidad. Por "confianza" en el contexto de la seguridad puede entenderse la certidumbre en relación con la fiabilidad y la veracidad de la información o en relación con la capacidad y la voluntad de una entidad de actuar de forma apropiada en una situación dada. Así pues, la creación de un entorno de confianza entre los Estados ayudará a armonizar la utilización de mecanismos de seguridad (por ejemplo, todos los países utilizarán un enfoque común de la selección de mecanismos como firmas electrónicas y protección mediante la verificación de contraseñas en dos pasos) y también permitirá aumentar el nivel de confianza (confianza continua y mensurable en la reputación, las capacidades, la validez o la autenticidad de alguien o de algo) entre los participantes en el comercio electrónico.

Se propone que por entorno de confianza transfronterizo se entienda una combinación de condiciones jurídicas, organizativas y técnicas recomendadas por los organismos especializados de las Naciones Unidas y las organizaciones internacionales competentes con miras a asegurar la confianza en el intercambio internacional de documentos y datos electrónicos entre partes (entidades) que interactúan electrónicamente al realizar operaciones de comercio electrónico

a. Principales cuestiones de Seguridad en Cloud Computing

Entre las principales cuestiones de acuerdo al proyecto LEFIS-APTICE (financiado por Sócrates. European Commission)[32], se tiene:

1) Desde la perspectiva de los individuos que se conectan a la nube: maximizar el control de usuario individual, crear servicios anónimos para usuarios individuales, crear mecanismos para el uso de identidades múltiples y limitar la información de identidad y autenticación para transacciones de alto nivel.

2) Desde la perspectiva de los proveedores de *cloud computing*: anonimato de la información personal, cifrar datos si contienen información personal, compartimentar-aislar el procesamiento y almacenamiento de datos, controlar los identificadores únicos, gestionar explícitamente los requisitos de seguridad y privacidad entre los proveedores de servicios *cloud computing*.

3) Desde una perspectiva global: proporcionar un aviso adecuado sobre la privacidad, soportar el desarrollo de PET (PrivacyEnhacing Technologies), utilizar la valoración del impacto de la privacidad y coordinar la aplicación de la privacidad y el cumplimiento a través de diferentes áreas jurisdiccionales (por ejemplo, cuando se pasa de un país europeo a un paraíso fiscal). Si los clientes emprenden procesos del tipo test de penetración no suele ser una buena opción en entornos *outsourcing* como

32. Javier Areitio, Protección de Cloud Computing en seguridad y privacidad. Facultad de Ingeniería. ESIDE. Grupo de Investigación Redes y Sistemas. Universidad de Deusto (2010).

cloud computing ya que el proveedor de la nube no puede distinguir nuestros test con un ataque real y además nuestros test de penetración pueden potencialmente impactar negativamente en otros usuarios de forma inaceptable.

V. ALGUNOS MODELOS DE ACUERDOS PREFERENCIALES A ESCALA INTERNACIONAL SOBRE PROTECCIÓN DE DATOS EN EL ÁMBITO DEL COMERCIO DIGITAL PROPIO DE LA NUBE.

En los últimos años, la creciente digitalización del comercio mundial ha imprimido un mayor sentido de urgencia al examen de la idoneidad de los acuerdos de la Organización Mundial de Comercio (OMC) frente a dicho fenómeno.

La aceleración de la revolución tecnológica, en particular la digital, es ampliamente reconocida. Sobre la base de regularidades empíricas como la ley de Moore (la capacidad de procesamiento se duplica cada dos años) y la ley de *Butter* (la capacidad de transmisión por fibra óptica se duplica cada nueve meses), se ha afirmado la existencia de tendencias exponenciales en el desarrollo de las tecnologías. Si bien tales tendencias son insostenibles en el largo plazo, sí es posible que caractericen el momento actual de creciente dinamismo en materia de *hardware,* plataformas y aplicaciones.

No cabe duda que la masificación de las tecnologías móviles y el uso de Internet han impulsado la ubicuidad de las tecnologías digitales, dando lugar a nuevos patrones de consumo, de relacionamiento y de producción. En ese proceso —que se traduce en bloques tecnológicos como los de computación en la nube, grandes datos e Internet de las cosas— cumplen un papel central las plataformas globales de agregación, tales como *Google o Facebook* en Occidente o *Baidu o Alibaba* en China. Las tecnologías más avanzadas en materia de robótica e inteligencia artificial se construyen sobre la base de esas plataformas, lo que tiene fuertes connotaciones geopolíticas en términos del equilibrio entre los grandes bloques del mundo.

Lo anterior configura un desafío para aquellos países o empresas que quieran insertarse con éxito en el comercio mundial, en este sentido la Comisión Económica para América Latina y el Caribe[33] considera que los países que basan su competitividad en la exportación de productos de alta intensidad tecnológica demandan capacidades científicas muy avanzadas y un alto nivel de inversión en I+D, al tiempo que mantienen una estrecha vinculación entre la base productiva y el sistema de ciencia y tecnología. Los sectores de alta intensidad tecnológica muestran una menor exposición a la entrada de competidores, mientras que los de baja intensidad tecnológica están mucho más expuestos a la competencia internacional, generando rentas más bajas.

Además, los países tecnológicamente avanzados mantienen un superávit en su balanza comercial de esta clase de bienes de media y alta tecnología, lo que no ocurre con las economías latinoameri-

33. Comisión Económica para América Latina y el Caribe (CEPAL) "Claves para un desarrollo productivo más inclusivo: el rol del conocimiento y la digitalización". La Unión Europea y América Latina y el Caribe. Estrategias Convergentes y sostenibles ante la coyuntura global" CEPAL, (LC/TS.2018/56/Rev.1), Santiago: Editado por CEPAL, (2018): 57-77.

canas. A diferencia de lo que ocurría hace algunos años, actualmente las empresas con mayor valor de mercado a nivel mundial corresponden a la industria digital. Esto se vincula con la capacidad de generar oferta de servicios digitales, como es el caso de la computación en la Nube, que en su mayoría se concentra en los Estados Unidos y, en menor medida, en Asia.

Ahora bien, se ha expuesto que en medio de estas negociaciones de uso intensivo de las TIC, la protección de los datos y la seguridad en su transferencia resulta altamente comprometida y, por ello desde organismos como la OMC se hacen esfuerzos para abordar la protección debida.

En este contexto, en la undécima Conferencia Ministerial (Buenos Aires, diciembre de 2017) un grupo de 43 miembros de la OMC[34] (incluyendo a la Unión Europea como uno) acordó iniciar el trabajo exploratorio conducente al lanzamiento de negociaciones sobre comercio electrónico. Esta declaración fue suscrita por todos los países desarrollados y por varios países de América Latina[35] y Asia, pero no por algunas de las principales economías en desarrollo (China, India e Indonesia), y tampoco incluyó a ningún país de África, excepto Nigeria. Ello da cuenta de las distintas visiones existentes sobre la necesidad y forma de adaptar las normas de la OMC a los desafíos que impone la digitalización, en particular dada la brecha digital entre países desarrollados y en desarrollo.

Dando seguimiento a lo anunciado en Buenos Aires en diciembre de 2017, en enero de 2019 un grupo de 49 miembros de la OMC[36] acordó iniciar negociaciones sobre comercio electrónico. Estas serán plurilaterales pero abiertas a la participación de todos los miembros interesados. La composición de este segundo grupo es muy similar a la del primero. Sin embargo, una diferencia fundamental es que incluye a China[37], cuya participación es crucial para que un eventual acuerdo plurilateral alcance la necesaria masa crítica.[38]

34. OMC (Organización Mundial del Comercio), Informe sobre el comercio mundial 2018. El futuro del comercio mundial: cómo las tecnologías digitales están transformando el comercio mundial. Ginebra. Acceso el 13 de abril de 2019 desde https://www.wto.org/spanish/res_s/publications_s/wtr18_s.htm.

35. Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, México, Panamá, Paraguay, Perú y Uruguay

36. OMC (Organización Mundial del Comercio), Informe sobre el comercio mundial 2018. El futuro del comercio mundial: cómo las tecnologías digitales están transformando el comercio mundial, op. cit.

37. En este contexto, China ha avanzado en la economía mundial, inicialmente sobre la base de su capacidad manufacturera y luego gracias a su creciente poder tecnológico y como inversionista en el exterior En particular, la combinación del peso del país asiático en manufacturas cada vez más avanzadas y de su desarrollo de plataformas digitales fortalece su capacidad de desarrollar iniciativas geopolíticas de amplio alcance, que alteran el equilibrio aceptado cuando se pensaba que China solo sería "la fábrica del mundo". En particular, el tamaño y el dinamismo de la base industrial preexistente, las condiciones comerciales y el desarrollo de la tecnología serán fundamentales para determinar quién dirigirá el juego. De acuerdo a una encuesta realizada recientemente por Infosys, por el momento, China parece ser quien tiene una ventaja sobre sus competidores más cercanos (Alemania, Estados Unidos y Reino Unido).

38. Sebastián Herreros, "¿Qué regulación internacional existe actualmente para el comercio electrónico?", en *La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe, serie Comercio Internacional,* Capitulo I. N° 142, (LC/TS.2019/42), (Santiago: Comisión Económica para América Latina y el Caribe (CEPAL), 2019).

Además de los acuerdos de la OMC, existen otros instrumentos multilaterales relevantes para el comercio electrónico. Uno de ellos es la Ley Modelo sobre Comercio Electrónico (LMCE) elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) en 1996, en la que se basan las leyes sobre la materia de 150 jurisdicciones en 71 países, incluidos 22 de la región latinoamericana.[39] Este instrumento (no vinculante) "fue el primer texto legislativo que adoptó los principios fundamentales de no discriminación, neutralidad tecnológica y equivalencia funcional, generalmente considerados como los pilares del derecho moderno de comercio electrónico" .[40] La LMCE contiene varias disposiciones de gran relevancia para el comercio electrónico transfronterizo, como el reconocimiento jurídico de los mensajes de datos y la validez de la firma electrónica. Estos conceptos fueron posteriormente incorporados en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, de 2007, también negociado en el seno de la CNUDMI.[41]

Otros instrumentos multilaterales relevantes para el comercio electrónico transfronterizo fueron negociados en el ámbito de la Organización Mundial de la Propiedad Intelectual (OMPI). Ellos son el Tratado sobre Derecho de Autor y el Tratado sobre Interpretaciones o Ejecuciones y Fonogramas, ambos de 1996, conjuntamente denominados los "tratados sobre Internet" de la OMPI. Ambos instrumentos tienen como principal objetivo adaptar los acuerdos ya existentes de la OMPI sobre esas materias (la Convención de Roma y el Convenio de Berna, respectivamente) a la revolución digital, y en particular a los desafíos que plantea distribución en Internet de material protegido por el derecho de autor como software, juegos y canciones (OMC, 2018).

Dado que los acuerdos de la OMC son tecnológicamente neutrales, se plantea la interrogante de si se requieren cambios en la gobernanza del comercio mundial para enfrentar de mejor modo los desafíos que plantea la revolución digital. Desde hace una década y media, esta pregunta viene siendo contestada empíricamente de modo afirmativo. Así lo demuestra la profusión de acuerdos comerciales preferenciales.[42]

39. Véase http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model_status.html (consultado el 20 de marzo de 2019).

40. CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) (2018), Situación actual – Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). Ginebra.

41. El texto en español de la Convención puede consultarse en:
https://www.uncitral.org/pdf/spanish/texts/electcom/0657455_Ebook.pdf
(consultado el 27 de marzo de 2019).

42. En este documento, la expresión "acuerdos comerciales preferenciales" se asume como equivalente a la de "acuerdos comerciales regionales", que la OMC define como "acuerdos comerciales recíprocos entre dos o más socios". Esta categoría incluye tratados de libre comercio (TLC), uniones aduaneras y otros tipos de acuerdos de menor alcance

A nivel mundial bajo esta premisa en estos acuerdos dominan tres actores principales: los Estados Unidos, la Unión Europea (UE) y China, con aproximaciones al tema claramente distinguibles y en ocasiones contrapuestas.[43]

Sin embargo, las áreas en las que se observa una (relativa) mayor similitud entre los acuerdos negociados por estos tres estados están en relación con el "entorno habilitante" del comercio electrónico en general, incluido el transfronterizo. En efecto, la mayoría de los acuerdos negociados por estos tres actores contiene disposiciones sobre la necesidad de que las partes cuenten con: a) un marco nacional para las transacciones electrónicas (en el USMCA[44] y el CPTPP[45] se dispone que éste debe ser compatible con los principios de la Ley Modelo de la CNUDMI); b) disposiciones sobre firma electrónica y autenticación electrónica; c) disposiciones sobre protección al consumidor en línea; y d) disposiciones sobre protección de la información personal.[46]

Entre los temas más mencionados se incluyen el apoyo a las pymes para utilizar el comercio electrónico, diversos temas regulatorios (protección de la información personal, protección del consumidor en línea, mensajes electrónicos comerciales no solicitados, seguridad y autenticación en las comunicaciones electrónicas) y el gobierno electrónico.

En el plano regulatorio Herreros[47] señala que, "las distintas aproximaciones de EEUU, UE y China son especialmente evidentes respecto de la protección de la información personal, la que se ha convertido en un activo estratégico en la economía digital". Los acuerdos del modelo estadounidense disponen que las partes deban contar con un marco legal que disponga la protección de la información personal de los usuarios del comercio electrónico, y que en su desarrollo deban tomar en consideración los principios y directrices de los organismos internacionales pertinentes.[48] No obstante, en ambos acuerdos se señala que esta obligación puede cumplirse incluso mediante compromisos

43. Ciuriak, Dan y Ptashkina, Maria (2018), "The digital transformation and the transformation of international trade". RTA Exchange. Ginebra, ICTSD y Banco Interamericano de Desarrollo, Acceso 20 de septiembre de 2018 desde: http://e15initiative.org/publications/the-digital-transformation-and-the-transformation-ofinternational-trade/

44. Tratado Comercial de Estados Unidos con el Canadá y México, suscrito en noviembre de 2018 (USMCA, por su sigla en inglés),

45. Tratado Integral y Progresista de Asociación Transpacífico (CPTPP), que entró en vigor entre seis de sus once signatarios en diciembre de 2018. Sus once miembros son: Australia, Brunéi, Canadá, Chile, Japón, Malasia, México, Nueva Zelandia, Perú, Singapur y Vietnam. Actualmente el acuerdo está vigente entre Australia, Canadá, Japón, México, Nueva Zelandia, Singapur y Vietnam

46. Negrita nuestro

47. Sebastián Herreros, "¿Qué regulación internacional existe actualmente para el comercio electrónico?", en La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe, serie Comercio Internacional, op. cit., 28.

48. El CPTPP no menciona ejemplos de esos principios y directrices. En cambio, el USMCA hace referencia al Marco de Privacidad del APEC y a la Recomendación del Consejo de la OCDE relativa a las directrices para la Protección de la Privacidad y Flujo Transfronterizo de Datos Personales, de 2013.

voluntarios de las empresas. Es decir, no se obliga a las partes a contar con una ley específica sobre protección de los datos.

Los acuerdos de China con Australia y la República de Corea también permiten un alto grado de discrecionalidad a las partes, ya que solo disponen que deberán adoptar medidas para proteger la información personal de los usuarios del comercio electrónico.[49] En el caso del acuerdo con Australia, se agrega que al desarrollar sus estándares de protección de datos, las partes deberán (en lo posible) tomar en cuenta los estándares internacionales y los criterios de los organismos internacionales relevantes.

En contraste con el enfoque relativamente homogéneo que caracteriza a los acuerdos correspondientes a los modelos estadounidenses y chino, no se observa un patrón consistente en los cinco acuerdos examinados suscritos por la UE. El estándar más alto se establece en el acuerdo con Canadá, en el que se dispone que las partes deberán adoptar o mantener disposiciones legales, reglamentarias y administrativas para la protección de la información personal de los usuarios del comercio electrónico, y que al hacerlo deberán tomar en consideración las normas internacionales.[50]

En los acuerdos con Japón y Singapur, en el primero se reconoce la importancia de que las partes adopten medidas para proteger la información personal de los usuarios, y en el segundo se menciona el entendimiento común de que el desarrollo del comercio electrónico debe ser plenamente compatible con los estándares internacionales de protección de datos (aunque sin señalar cuáles). Por último, los acuerdos con México y Vietnam, los socios de menor nivel de desarrollo, no abordan el tema. Paradójicamente de que la protección de los datos personales no ha figurado de modo consistente en los acuerdos comerciales de la UE, ésta es el actor que se ha dotado internamente de una legislación más completa y ambiciosa en la materia, pues cuenta con el Reglamento General de Protección de Datos (RGPD). Este eleva sustancialmente el estándar de protección de los datos personales en todo el territorio de la UE.[51] Según Wheeler[52] las empresas no comunitarias que manejan datos personales de ciudadanos de la UE también deben cumplir con las disposiciones del RGPD, por lo que éste

49. El acuerdo con Chile parece establecer un estándar más exigente, ya que dispone que las partes deberán "adoptar o mantener una normativa interna y otras medidas que garanticen la protección de la información personal de los usuarios (...)".

50. Sebastían Herreros, "¿Qué regulación internacional existe actualmente para el comercio electrónico?", en *La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe*, op. cit.

51. Para mayores antecedentes, véase Comisión Europea, "Reforma de 2018 de las normas de protección de datos de la UE", [en línea] , acceso el 10 de abril de 2019 desde , https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eudata-protection-rules_es#sobreelreglamentoylaproteccindedatos

52. Tom Wheeler, "The General Data Protection Regulation sets privacy by default", Brookings Institution, 23 de mayo de 2018, acceso el 20 de septiembre de 2018 desde, https://www.brookings.edu/blog/techtank/2018/05/23/thegeneral-data-protection-regulation-sets-privacy-by-default/.

podría convertirse de facto en una suerte de régimen mundial. De hecho, los mayores costos para las empresas extranjeras -y potencialmente también para los usuarios- asociados a su cumplimiento ya han generado críticas en los Estados Unidos.[53]

El RGPD entró en vigor en mayo de 2018, por lo que cabe esperar que los futuros acuerdos comerciales suscritos por la UE contengan disposiciones que reflejen de cerca sus contenidos.

En cuanto a la región de Latinoamérica vale señalar que exhibe una gran heterogeneidad en términos de su participación en acuerdos que contengan disposiciones sustantivas sobre comercio electrónico, pudiendo identificarse dos grupos de países. Un grupo está compuesto por los miembros de la Alianza del Pacífico (Chile, Colombia, México y Perú), los países centroamericanos (incluido Panamá) y la República Dominicana. Todos ellos han suscrito varios acuerdos —principalmente con socios desarrollados y entre sí— que contienen capítulos sobre comercio electrónico.[54] El otro grupo está integrado por los cuatro miembros originales del MERCOSUR (Argentina, Brasil, Paraguay y Uruguay), el Estado Plurinacional de Bolivia, Cuba, Ecuador, la República Bolivariana de Venezuela y los miembros de la Comunidad del Caribe (CARICOM). Algunos de estos países (Bolivia, Cuba, Paraguay y Venezuela) no han participado a la fecha en ningún acuerdo comercial o de integración económica que aborde expresamente el comercio electrónico, mientras que los restantes solo lo han hecho en un acuerdo cada uno.[55] Por otra parte, trece países de la región figuran entre los patrocinantes de las negociaciones plurilaterales sobre comercio electrónico lanzadas en enero de 2019 en la OMC.[56]

Existen 34 acuerdos preferenciales suscritos por países de la región hasta la fecha que contienen capítulos sobre comercio electrónico, de los cuales 31 se encuentran vigentes. De estos acuerdos, 25 son con socios extra regionales y los restantes 9 entre países o agrupaciones de la misma región.

Los tres grandes modelos regulatorios expuestos han sido desarrollados por actores que, más allá de sus grandes diferencias, tienen el elemento en común de estar mucho más avanzados que la región latinoamericana en la economía digital. Sin perjuicio de ello, probablemente el mercado único digital actualmente en construcción en la UE constituya la referencia más pertinente para avanzar en una

53. Niam Yaraghi, "A case againstthe General Data Protection Regulation", *Brookings Institution*, 11 de junio de 2018, acceso el 20 de septiembre de 2018 desde,
https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-thegeneral-data-protection-regulation/

54. Todos estos países, excepto Chile, son también signatarios del Acuerdo de Tecnología de la Información de la OMC.

55. Esta situación podría cambiar en caso de concluir exitosamente las negociaciones comerciales que el MERCOSUR lleva adelante desde hace casi dos décadas con la UE, o las que inició más recientemente con Canadá, la República de Corea y Singapur. Todos estos socios incluyen regularmente el comercio electrónico —con distintos niveles de profundidad— en sus acuerdos comerciales

56. Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Uruguay.

línea similar en América Latina y el Caribe, por tres motivos. En primer lugar, porque —a diferencia de los modelos estadounidense y chino—tiene por definición una visión regional. En segundo lugar, porque combina un grado importante de apertura —necesario para el desarrollo del comercio electrónico— con un énfasis marcado en regular los efectos disruptivos de la digitalización.[57] En tercer lugar, la posibilidad de avanzar hacia un marco regional utilizando elementos relevantes del modelo comunitario se acrecienta por el hecho de, entre los tres actores principales a nivel mundial, la UE es el que tiene acuerdos comerciales vigentes con el mayor número de países de la región. De hecho, en caso de concluir exitosamente las negociaciones con el MERCOSUR, la UE dispondría de acuerdos con todos los países de la región excepto el Estado Plurinacional de Bolivia, Cuba y la República Bolivariana de Venezuela.

Reconociendo las dificultades técnicas y políticas que supone crear una legislación de alcance supranacional al estilo de la existente en la UE, los esfuerzos hacia la constitución de un mercado digital regional podrían centrarse inicialmente en avanzar hacia una mayor interoperabilidad de las legislaciones nacionales. Con ello se lograría atenuar la incertidumbre y los costos de transacción en las operaciones transfronterizas que surge de la coexistencia de leyes nacionales distintas en materias como la protección del consumidor en línea y la privacidad de los datos personales, entre otras.

VI. ALGUNOS DESAFÍOS PARA AMÉRICA LATINA Y EL CARIBE EN ENTORNOS DE CONTRATACIÓN DE SERVICIOS EN LA NUBE

Como bien afirma la CEPAL[58] la nueva revolución industrial se genera a partir de la incorporación de tecnología avanzada en los procesos productivos; en sectores estratégicos, esta agregación permitiría incrementar los niveles de competitividad y productividad de la economía. Esta tecnología avanzada comprende, entre otros elementos, la contratación de servicios en la nube, la incorporación de sensores y el desarrollo de la Internet de las cosas, la generación y gestión de grandes datos y la incorporación de la robótica e inteligencia artificial.

En ese contexto, es necesario revisar las políticas orientadas a incentivar el acceso y uso de servicios digitales, principalmente de Internet, ya que la mayor parte de las medidas que se han adoptado en la región se han orientado a promover el uso de Internet residencial. Este paso de la Internet del consumo a la Internet de la producción no implica descuidar el cierre de brechas de acceso de los usuarios

57. Por el contrario, el modelo estadounidense privilegia la apertura, para preservar la posición dominante de los gigantes tecnológicos de ese país. Por su parte, el modelo chino corresponde a una experiencia sui géneris difícilmente replicable en otros países, ya que en él confluyen el enorme mercado interno de ese país con las particularidades de su sistema político y económico.

58. Comisión Económica para América Latina y el Caribe (CEPAL) "Claves para un desarrollo productivo más inclusivo: el rol del conocimiento y la digitalización". *La Unión Europea y América Latina y el Caribe. Estrategias Convergentes y sostenibles ante la coyuntura global*, CEPAL, (LC/TS.2018/56/Rev.1), Santiago: Editado por CEPAL, (2018), 57-77.

individuales, sino más bien complementarlas con acciones de masificación del uso de Internet en el ámbito productivo. De acuerdo a la información de las encuestas industriales, en general existe un alto grado de adopción de tecnologías maduras (Internet, banda ancha, informática) en las empresas, independientemente de su tamaño. Sin embargo, su asimilación o incorporación como parte de los procesos productivos todavía es muy escasa, concentrándose el uso en elementos tales como correo electrónico, búsqueda de información y uso de servicios financieros. Esta incorporación debe abarcar todos los estadios de la producción, desde la adquisición de insumos y procesamiento hasta la distribución.

De lo contrario se seguirá observando grandes diferencias entre los países que han incorporado estas tecnologías de avanzada y aquellos que solo la consumen, como es el caso principalmente de los países de la región de América Latina y el Caribe.

La Agenda Digital para América Latina y el Caribe (eLAC) ha tenido como misión fortalecer el proceso de integración regional en materia digital, atendiendo al dinamismo tecnológico y los cambios sociales provocados por la digitalización. Este proceso se inició en 2005 en Río de Janeiro, durante la Primera Conferencia Ministerial Regional de América Latina y el Caribe preparatoria de la segunda fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), donde se aprobó la primera versión del Plan de Acción sobre la Sociedad de la Información de América Latina y el Caribe (eLAC2007)[59]. Posteriormente, este proceso se mantuvo vigente con los planes eLAC2010, eLAC2015, eLAC2019 y el plan de trabajo con acciones específicas para el período 2013-2015 y 2018-2020.

Durante la Sexta Conferencia Ministerial sobre la Sociedad de la Información en América Latina y el Caribe, celebrada en abril de 2018 en Cartagena de Indias (Colombia), se aprobó la última versión de la Agenda Digital para América Latina y el Caribe (eLAC2020), renovando los acuerdos de la Conferencia con una visión hacia 2020 e incorporando en las prioridades de la Agenda un conjunto de desafíos emergentes vinculados a la digitalización.

En la Agenda Digital (eLAC2020), los Gobiernos de la región definieron 30 objetivos, interdependientes y complementarios, cuyos resultados se afectan mutuamente y se ordenan en un mapa de referencia de siete áreas de acción: i) infraestructura digital; ii) transformación y economía digital; iii) mercado digital regional; iv) gobierno digital; v) cultura, inclusión y habilidades digitales; vi) tecnologías emergentes para el desarrollo sostenible, y vii) gobernanza para la sociedad de la información.[60]

Lo anterior supone retos para la región en materia de fortalecer su actividad de comercio electrónico transfronterizo Parte de estos retos incluyen los ámbitos fiscales, normativos, de regulación,

59. Se hace referencia al inicio del proceso de aprobación de un plan de acción; sin embargo, las conferencias regionales se iniciaron en 2000 con la Declaración de Florianópolis, continuando en 2003 con la preparación regional de la Cumbre Mundial sobre la Sociedad de la Información y la Declaración de Bávaro.

60. Comisión Económica para América Latina y el Caribe (CEPAL) "Claves para un desarrollo productivo más inclusivo: el rol del conocimiento y la digitalización". *La Unión Europea y América Latina y el Caribe. Estrategias Convergentes y sostenibles ante la coyuntura global*, op. cit.

logísticos y de idioma. Las empresas se ven obligadas a cumplir con distintos marcos fiscales y legales, lo que puede ser un desincentivo para el comercio en línea. Asimismo, las diferentes leyes de derechos al consumidor que rigen los procedimientos para la resolución de reclamos y devoluciones difieren de un país a otro. Las normativas sobre privacidad y protección de datos pueden dificultar el intercambio de datos interregionales pero las similitudes idiomáticas pueden ser una ventaja competitiva para las empresas de la región.

Según estimaciones recientes, el comercio electrónico entre empresas y consumidores (B2C) en el ámbito transfronterizo alcanzará aproximadamente 1 billón de dólares por año para 2020, llegando a representar el 30% del comercio electrónico minorista. Si bien se debe ser cauteloso con estas estimaciones, es importante notar el creciente peso del comercio digital —especialmente de productos digitales— en los flujos comerciales en un escenario de pérdida de dinamismo del comercio mundial, la inversión extranjera directa y el financiamiento internacional.[61]

VII. CONCLUSIONES

La computación en la Nube configura una modalidad mas de negocio dentro del conjunto de Tecnologías de avanzada y, quienes participan en esta gestión digital encuentran altos beneficios, pero también se enfrentan a riesgos importantes y, uno de ellos ha sido en referido a la privacidad y seguridad de los datos y la información que dicho negocio de comercio electrónico involucra.

Son tres los actores o partes que participan en este tipo de contrato de servicios en la nube, por una parte, el responsable del registro, por otro el proveedor del servicio en la nube y el tercero que es el titular de los datos o información que se maneja. De igual forma, puede darse entre sujetos de comercio entre sí, o entre estados y comerciantes o entre comerciantes y el consumidor final o entre todos ellos.

Con base a la flexibilidad, ubicuidad y portabilidad de la información que involucra este negocio electrónico, resulta conveniente revisar los acuerdos o tratados que a nivel internacional se han aprobado por los estados a partir de los estudios de las organizaciones internacionales como OMC, CNUDMI, la CEPAL, la OMPI, entre otros. Ello porque estos instrumentos pueden facilitar la mejor delimitación de atribución de responsabilidades a cada parte contratante, lo cual se hace más complejo en escenarios transfronterizos. Pero sin duda también puede significar limitar o minimizar la participación en esta modalidad de comercio digital que implica competitividad si la misma se desarrolla de manera adecuada.

Los servicios de computación en la nube, pueden significar una o más prestaciones tales como infraestructura, plataforma y software y en términos de uno o más modelos de implementación como público, privado, híbrido y comunitario. Por lo cual es sumamente atractivo y cada vez más se expande su uso.

61. Ídem.

Debe reconocerse que las dificultades técnicas y políticas que supone crear una legislación de alcance supranacional, a fin de la constitución de un mercado digital regional podrían centrarse inicialmente en avanzar hacia una mayor interoperabilidad de las legislaciones nacionales. Con ello se lograría atenuar la incertidumbre y los costos de transacción en las operaciones transfronterizas que surge de la coexistencia de leyes nacionales distintas en materias como la protección del consumidor en línea y la privacidad de los datos personales, entre otras.

En el caso de América Latina y el Caribe las normativas sobre privacidad y protección de datos pueden dificultar el intercambio de datos interregionales pero las similitudes idiomáticas pueden ser una ventaja competitiva para las empresas de la región.

Para hacer frente a los elementos que afectan la expansión de la economía digital a nivel regional, es necesario que los países avancen en una agenda estratégica que permita definir un conjunto de principios, objetivos y acciones que guíen las decisiones de política para formar un mercado digital regional que contribuya a mejorar la conectividad y aumentar la eficiencia comercial, reduciendo las asimetrías normativas y los costos de transacción. La decisión de avanzar hacia la configuración de un mercado digital regional es un elemento que puede fortalecer los procesos de integración regional.

REFERENCIAS

_____ " ¿Qué es el Cloud Computing? " En: *Guía para clientes que contraten servicios de clod computing*, Madrid: Agencia Española de protección de Datos, 2013.

- A/CN.9/WG.IV/WP.141 Asamblea General de las Naciones Unidas Comisión de las Naciones Unidas para el Derecho Mercantil Internacional Grupo de Trabajo IV (Comercio Electrónico) 55º período de sesiones, Nueva York, 24 a 28 de abril de 2017. Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza.
- Areitio, Javier. "Protección de Cloud Computing en seguridad y privacidad". Proyecto Grupo de Investigación Redes y Sistemas LEFIS-APTICE (financiado por Sócrates. European Commission). Facultad de Ingeniería. ESIDE. Universidad de Deusto: 2010.
- Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional Grupo de Trabajo IV (Comercio Electrónico) 55º período de sesiones Nueva York, 24 a 28 de abril de 2017.
- Baena, José Jaime y Cano, José Alejandro "Uso de Tecnologías de Información y Comunicación para la negociación" ¿Ventajas para las empresas colombianas? En *Ciencias Estratégicas*, 22 (32), (2014):1-29.

- Ciuriak, Dan y Maria Ptashkina. "The digital transformation and the transformation of international trade". RTA Exchange. Ginebra, ICTSD y Banco Interamericano de Desarrollo. Acceso el 20 de septiembre de 2018 desde, http://e15initiative.org/publications/the-digital-transformation-and-the-transformation-ofinternational-trade/.

- CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) (2018), Situación actual – Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996). Ginebra.

- Cobo, Juan. "IT Seguridad en "la Nube": ¿Cómo controlar lo que no controlas?". En *Red Gobal de Conocimientos en Auditoría y Control Interno Auditool*, ISSN ONLINE: 2665-3508, publicado el 07 de enero de 2011. Acceso el 23 de enero de 2020 desde, https://www.auditool.org/blog/auditoria-de-ti/350-it-seguridad-en-la-nube-icomo-controlar-lo-que-no-controlas

- Comisión Económica para América Latina y el Caribe (CEPAL) "Claves para un desarrollo productivo más inclusivo: el rol del conocimiento y la digitalización". En *La Unión Europea y América Latina y el Caribe. Estrategias Convergentes y sostenibles ante la coyuntura global.* CEPAL, (LC/TS.2018/56/Rev.1). Santiago: Editado por CEPAL, (2018):57-77.

- García, Julio y Cruz, Galvy. "Privacidad de la información en la Nube". *Revista Seguridad*, 8, (2018). Acceso el 20 de septiembre de 2018 desde: https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

- Gómez y Martínez. *Negociación Internacional medios de cobro y pago*. Madrid: 1era edición, 2003.

- Herrera, Rodolfo "¿La Nube es segura para los datos personales?" *Revista Seguridad*, 8 (2018). Acceso el 20 de septiembre de 2018 desde: https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

- Herreros, Sebastián. "¿Qué regulación internacional existe actualmente para el comercio electrónico?". En *La regulación del comercio electrónico transfronterizo en los acuerdos comerciales: algunas implicaciones de política para América Latina y el Caribe*, serie Comercio Internacional, Capitulo I. N° 142 (LC/TS.2019/42). Santiago: Comisión Económica para América Latina y el Caribe (CEPAL), 2019.

- Kleinschmidt, E, de Brentani, U y Salomo, S. "Performance of global new product developmente programs: A resource – based view". *Journal of Product innovation management*, 24, vol.5 (2007): 419-441. https://doi.org/10.1111/j.1540-5885.2007.00261.x

- López-González, Javier y Jouanjean, Marie-Agnes "Digital trade. Developing a framework for análisis", OECD *Trade Policy Papers*, No 205, (2017): 50-64.OCDE, París.
- Lund, Susan y Manyika, James "How digital trade is transforming globalization". *E15 Expert Group on the Digital Economy*, ICTSD-World Economic Forum, (2016). Acceso el 10 de enero de 2019 desde, http://e15initiative.org/publications/how-digital-trade-is-transforming-globalisation/
- OMC (Organización Mundial del Comercio) (2018), Informe sobre el comercio mundial 2018. El futuro del comercio mundial: cómo las tecnologías digitales están transformando el comercio mundial. Ginebra. Acceso el 13 de abril de 2019 desde, https://www.wto.org/spanish/res_s/publications_s/wtr18_s.htm
- Wheeler, Tom "The General Data Protection Regulation sets privacy by default". En *Brookings Institution*, (23 de mayo de 2018). Acceso el 20 de septiembre de 2018 desde, https://www.brookings.edu/blog/techtank/2018/05/23/thegeneral-data-protection-regulation-sets-privacy-by-default/
- Yaraghi, Niam "A case againstthe General Data Protection Regulation", *Brookings Institution,* (11 de junio de 2018). Acceso el 20 de septiembre de 2018 desde, https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-thegeneral-data-protection-regulation/

RECIBIDO: 31/01/2020

APROBADO: 10/05/2020