

Guía de Recomendaciones Legales y Técnicas para la protección de Datos en Cloud Computing y Redes Sociales

Bibiana Luz Clara 1, Ana Haydée Di Dorio 2 ,
Verónica Uriarte 3, Juan Martin Brun 4, Fernanda Giaccaglia 5.

- 1.- Abogada, Profesora e Investigadora de la Universidad FASTA, Presidente del Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata. Miembro del Tribunal Arbitral del Colegio de Abogados de Mar del Plata, luzclarabb@infovia.com.ar
- 2.- Ingeniera en Informática, Instructor Informático en el Ministerio Público de la Provincia de Buenos Aires, Docente e Investigadora en Universidad FASTA, diana@ufasta.edu.ar
- 3.- Ingeniera en Informática, Analista Funcional en la Municipalidad de General Pueyrredón, Provincia de Buenos Aires, Investigadora en Universidad FASTA, yuriarte@live.com
- 4.- Alumno de abogacía e Investigador en Universidad FASTA, juanbrun@ufasta.edu.ar
- 5.- Abogada, Profesora e Investigadora de la Universidad FASTA, fernandag@ufasta.edu.ar

Abstract. El tema que nos ocupa en este trabajo es el uso de Redes Sociales y Cloud Computing en un nuevo modelo de sociedad, donde es necesario contar con principios universales claros, legislación uniforme a nivel internacional, y un marco de contención y seguridad para el bien más cotizado en la era actual: la información. **Como objetivo nos proponemos el análisis de las nuevas figuras jurídicas que utilizan los usuarios de redes sociales y computación en la nube, y las consecuencias que como consumidores pueden sufrir en dichas contrataciones, buscando aconsejar en el uso responsable y cuidado de la privacidad y datos que en las mismas se brindan.** Este estudio surge de una investigación realizada por profesionales de las facultades de Ingeniería y Derecho de la Universidad FASTA, con la finalidad de redactar una guía de recomendaciones que sirva a los usuarios de las redes sociales y cloud computing, conociendo las circunstancias que lo rodean y los derechos que los asisten.

Palabras Clave: Derechos del Consumidor – Redes Sociales – Cloud Computing- Usuario – Proveedor- Recomendaciones

1 Introducción

Con el correr del tiempo, las comunicaciones realizadas vía Internet, han ido evolucionando vertiginosamente. Así, desde los tradicionales programas de mensajería instantánea, como el ICQ o el MSN Messenger, hemos llegado en la actualidad a las “redes sociales”. En ellas, los usuarios ponen en común aficiones, gustos y vivencias, con la única finalidad de que toda su red de contactos, que se encuentra en constante crecimiento, tenga acceso a dicha información.

El concepto de *red social* en Internet supone una nueva forma de relación humana, y es un fenómeno que se encuentra en constante crecimiento.

Las redes sociales son importantes canales de comunicación e interacción. La información personal suministrada a través de las redes sociales y, en la mayoría de los casos, con el consentimiento de sus titulares, parece no conocer límites. Por ello, la actual protección jurídica se revela insuficiente.

Los usuarios de las redes sociales revelan tranquila y concientemente su privacidad y la de sus conocidos. Hoy en día la gente muestra sus emociones e imágenes por Internet, sin ningún tipo de control. Y una vez que la información personal se publica en Internet, el peligro de que se haga accesible a todo el mundo es incontrolable y el daño que se puede generar es irreversible.

No se trata de una tarea sencilla. Dar protección eficiente a la vida privada en el ámbito de las redes sociales conlleva la necesidad de reinterpretar, adecuar y fortalecer el concepto de protección existente hasta el momento.

Por otro lado, se está viviendo un cambio de paradigma con el cloud computing, donde debemos pensar en computación distribuida, o “clusters” desde el punto de vista técnico.

Si nos remontamos a los años 80s, cuando aparecieron las computadoras personales, parte de su atractivo era la promesa de liberar los programas y los datos del centro computacional principal. Pero las PCs aisladas tienen una debilidad obvia: en muchos casos la red fue el principal medio de colaboración e intercambio. Para el individuo, el control total viene con un precio. El software tiene que ser instalado y configurado. Luego, actualizado en cada nuevo lanzamiento.

La computación se está transformando en un modelo que consiste en servicios que son de consumo masivo y son entregados de manera similar a los servicios tradicionales como el agua, la electricidad, el gas y el teléfono. En este modelo, los usuarios pueden acceder a los servicios basados en sus necesidades sin tener en cuenta cómo los servicios están alojados o la forma en que se entregan.

De esta manera, los consumidores, como las empresas, son atraídos por la oportunidad de reducir o eliminar los costos asociados con la provisión “in – house” de estos servicios.

Sin embargo, desde que las aplicaciones en la nube pueden ser cruciales para las operaciones básicas del negocio de los usuarios, es esencial que los usuarios tengan garantías de los proveedores del servicio.

Los usuarios de los servicios informáticos deben pagar a los proveedores sólo cuando acceden a dichos servicios. Además, los usuarios ya no tienen que hacer grandes inversiones o encontrarse con las dificultades de construir y mantener infraestructura TIC compleja. Por lo tanto, los profesionales del software están enfrentando numerosos nuevos desafíos y cambios del modelo de negocio hacia la creación de software como servicio SaaS.

La creación de Internet, mediante la formación de un sistema mundial de redes informáticas que permite a computadoras individuales comunicarse con cualquier otra computadora en cualquier lugar del mundo, marcó el hito más importante para lograr esta visión del siglo XXI de “servicios informáticos”.

Los servicios informáticos se centran en la relación entre los procesos de negocios y las tecnologías de la información y comunicación, para automatizar los primeros utilizando estos últimos.

2. El Proyecto de Investigación

Este proyecto desarrollado durante el periodo 2011-2012 nace a partir de la necesidad de estudiar las nuevas figuras que han aparecido a partir de la irrupción del concepto de computación en la nube, y el auge, cada vez más preponderante de las redes sociales, como un nuevo modelo de negocio en la web. Se decide entonces, tratar ambos temas en conjunto ya que, si bien presentan características propias que los distinguen, ambos son servicios que se presentan como nuevos y tentadores a los consumidores, y no cuentan con un respaldo legal necesario para la protección de sus derechos.

Desde la óptica de los datos personales encontramos la problemática de la privacidad en las redes sociales, y desde la óptica de los datos comerciales, cuestiones propias del cloud computing.

Consideramos importante analizar y estudiar respecto a los riesgos en los distintos tipos de redes sociales y servicios de cloud computing para permitir al usuario evaluar en cada caso sus ventajas y desventajas.

En síntesis, el objetivo del proyecto es el análisis de las nuevas figuras jurídicas que utilizan los usuarios de redes sociales y computación en la nube, y las consecuencias que como consumidores pueden sufrir en dichas contrataciones, buscando elaborar recomendaciones de uso responsable y cuidado de la privacidad y datos que en a las mismas se brindan.

Para esta investigación se estudiaron las redes sociales más representativas del mercado, y se analizaron los términos y condiciones de prestación del servicio.

Además se completó el trabajo con una encuesta a los usuarios de las mismas, donde se buscó medir el conocimiento del usuario sobre los términos y condiciones aceptados, y la importancia que el usuario le da a estas cuestiones.

De la misma manera se procedió con los usuarios de cloud computing, respecto a la información comercial depositada en la nube.

3.- Las Redes Sociales

El fenómeno masivo del uso de redes sociales en la vida de las personas en la actualidad, y su consecuente exposición de la vida privada, es preocupante y abre las puertas al debate que se debe realizar sobre varios temas importantes, como lo es la protección de los derechos personalísimos, la responsabilidad de los proveedores de servicios de redes sociales y de hosting, el derecho a la libertad de expresión, las leyes de protección de datos y los delitos informáticos, entre otros.

Las redes sociales son estructuras sociales compuestas por grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como la amistad, el parentesco, intereses comunes o conocimientos.

Como concepto tecnológico de red social podríamos decir que se trata de una aplicación online que permite a los usuarios, de forma completamente descentralizada, generar un perfil público, compartir información, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión.

Los usuarios de redes sociales brindan datos personales sin ser conscientes de las consecuencias que ello provoca. Las condiciones legales a las que son sometidos, en la mayoría de los casos, ni siquiera son leídas y la mayoría de ellas son ambiguas y contienen cláusulas abusivas.

Las redes sociales presentan los siguientes aspectos que pueden ser considerados esenciales a la hora de realizar un análisis jurídico:

1. ***Protección de datos de carácter personal:*** El concepto de red social conlleva la puesta a disposición de toda la red de contactos de gran cantidad de datos personales; son los propios usuarios los que voluntariamente publican sus datos personales en la red.

Toda red social está firmada por tres elementos principales: software, datos personales e información sobre los usuarios, estas plataformas pueden presentar diversos riesgos en lo que respecta a la protección de datos personales:

- Los datos personales tratados por la red social pueden ser comunicados, cedidos o puestos a disposición de terceros.
- A pesar de que aparezcan publicados textos legales relativos a la protección de datos de los usuarios, es muy frecuente observar como dichos textos legales no son comprensibles para un ciudadano medio que no cuente con experiencia o formación jurídica. Los textos, además, suelen ser publicados en lugares de la plataforma de difícil localización y acceso. Todo ello ha llevado a la generalización ente los usuarios del hecho de que los avisos legales y políticas de privacidad no sean leídos en la gran mayoría de casos y, en aquellos casos en los que son revisados por los usuarios, no son realmente comprendidos, por lo que no cumplen su objetivo principal.

2. ***Protección de la privacidad, honor, intimidad, imagen:*** Se encuentra estrechamente relacionado con el derecho a la protección de datos personales.

Las redes sociales tienen gran parte de la responsabilidad en lo referido a la protección de la intimidad de sus usuarios. El adecuado diseño de la plataforma y de las herramientas puestas al servicio del usuario puede ser suficiente para evitar o minimizar los problemas relacionados con la privacidad.

Las redes sociales online son un ámbito susceptible donde se puede cometer gran cantidad de infracciones sobre el derecho a la imagen, simplemente si se piensa que una persona publica una fotografía, y ésta inmediatamente se empieza a distribuir por toda la red de usuarios, llegando a contactos o publicaciones no deseadas por el usuario.

Es dable destacar que en muchos casos hay actuaciones de los usuarios o de las propias redes, que realizan respecto de la imagen y otros datos que se escapan de la propia esfera de la protección de datos, como por ejemplo las cesiones ilegales de imágenes para finalidad comercial sin consentimiento previo e informado del titular.

Una foto “etiquetada” en las redes sociales, sin el consentimiento del afectado es una conducta ilícita que puede causar daño, y puede merecer una sanción penal y una indemnización civil.

Una de las cosas que en ocasiones olvidamos a la hora de utilizar estas redes sociales, es que el usuario tiene la posibilidad de consentir o no que su imagen o sus datos personales se hagan públicos. Pero no siempre disponemos de esta facultad ya que en algunas oportunidades no somos nosotros los que decidimos qué imagen o qué información nuestra es publicada, y es en este momento cuando se nos plantean los verdaderos problemas.

Las redes sociales son herramientas de mucho poder, y pueden poner en riesgo un matrimonio, una relación, un trabajo, una empresa. Estamos frente a un fenómeno de gran impacto y con un poder de influencia cada vez mayor, que mal utilizado puede ser muy dañino.

La red social debe informar a sus usuarios de la importancia de ser respetuoso con el resto de usuarios y de no llevar a cabo actos que puedan vulnerar la intimidad de los mismos.

De igual forma, deben sancionarse las acciones que vulneren la intimidad de cualquier tercero.

Toda red social debe establecer los canales necesarios de denuncia, que deben ser efectivos, garantizando la atención de las solicitudes en un plazo razonable.

3. **Protección de la propiedad intelectual:** Todos los usuarios deben atender a las condiciones de registro y especialmente a la regulación que en éstas se disponga en materia de propiedad intelectual e industrial, observando el tipo de cesiones de derechos que realizan y a favor de quién se realizan.
4. **Protección de los menores de edad:** Urge la necesidad de crear una ley que proteja a los menores de edad de los peligros que enfrentan en Internet, particularmente en las redes sociales. Frente a la vulnerabilidad de los menores en estas nuevas formas de convivencia social a través de las redes sociales en Internet, el derecho no puede quedarse atrás. No se trata de restringir el acceso de infantes y adolescentes a estos espacios de comunicación digital, pretenderlo sería ingenuo.

La exposición constante y pública de la información en las redes sociales implica ciertos peligros particularmente para los menores de edad porque pueden acceder a contenidos de información que no son pertinentes para su edad o entrar en contacto con personas que explotan su información.

La Constitución Nacional Argentina protege el derecho a la intimidad en los artículos 18°, 19° y 43°, y en los tratados con jerarquía constitucional, contemplados en el artículo 75°, inciso 22°. Además, la ley de Protección de Datos Personales N° 25.326, complementa nuestra Carta Magna.

Desde el punto de vista jurídico, muchos son los temas que conviene considerar. Uno de los principales riesgos es la vulneración de la intimidad de los participantes, puesto que es inherente a estos servicios la publicación de datos personales y otra información sensible de la persona. Por ello, es imprescindible que los proveedores de estos servicios implementen medidas de protección de esos datos.

Un interesante punto, desde la óptica jurídica, será determinar la naturaleza jurídica de los servicios de redes sociales. Muchos dicen que se trataría de un contrato por adhesión online.

Si se analiza la relación jurídica obligacional que surge de la prestación del servicio entre la empresa titular del sitio web y el usuario, estaríamos ante un contrato por adhesión. Estos contratos son aquellos en los cuales el contenido contractual ha sido determinado con prelación por uno sólo de los contratantes, al que se debe adherir el co – contratante que desee formalizar la relación jurídica obligatoria. El usuario, al realizar el proceso de registración en cualquier sitio web que preste este tipo de servicios (ejemplo: Facebook), debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente. En este orden, la naturaleza jurídica del contrato que rige la relación, llamados comúnmente “términos de uso”, “términos y condiciones”, “políticas de privacidad”, es la de un contrato por adhesión.

Una de las problemáticas jurídicas que se plantea de acuerdo a la naturaleza jurídica de los contratos por Internet, lo es en torno al verdadero consentimiento informado del usuario al aceptar las cláusulas en el momento de la registración, ya que la mayoría de los usuarios no suelen leer detenidamente los términos y condiciones del sitio web.

No se trata de restarle validez al consentimiento del usuario expresado por medios electrónicos, sino de plantear la problemática típica de los contratos por adhesión llevada al ámbito de Internet en relación a la información necesaria que debe tener el usuario para un verdadero consentimiento informado.

Una de las formas más utilizadas es prever la inclusión de las condiciones generales de contratación en el mismo proceso de registración, de manera tal que sea ineludible su exposición clara al usuario para su lectura y conformidad, y no mediante un link al final de la página.

La segunda cuestión central se plantea en cuanto a la jurisdicción pactada en los términos y condiciones del sitio web, que generalmente son en países extranjeros. Esta prórroga de competencia jurisdiccional puede resultar inaccesible para el contratante débil (usuario), que por lo general en virtud de la excesiva onerosidad devengada a partir de la distancia, derivada de litigar en una jurisdicción distinta a la natural, vuelve ilusoria cualquier pretensión de hacer valer sus derechos.

Otra cuestión importante, y que le preocupa a todos los usuarios de redes sociales, es la pérdida de control sobre la información personal. Hasta el momento, no existen fórmulas claras ni precisas que faciliten eliminar los datos en caso de decidir hacerlo. Algunos países están trabajando para sancionar una ley que garantice el “derecho al olvido”. Con ello, se obligaría a sitios como Facebook a que eliminen completamente la información personal de los usuarios, cuando éstos se den de baja. Este tipo de leyes también garantizarán la llamada “privacidad por defecto”. Gracias a ella, ninguna red o programa podrá hacer públicos los datos de una persona, sin su consentimiento expreso.

A modo de ejemplo, podemos mencionar un fallo de la justicia nacional, donde se obligó a Facebook a eliminar la foto de una persona. Lo anterior, encontró su fundamento en el derecho constitucional de intimidad y propia imagen, teniendo en cuenta que la foto publicada en contra de su voluntad, dañó el honor del menor. Dicho fallo fue: “*Bartomioli, Jorge Alberto C/ Facebook Inc. s/ Medida autosatisfactiva*”-*expte. n° 1385/09*¹. También podemos mencionar los siguientes fallos que resolvieron en forma similar a este tipo de cuestiones: “*Artero, Eduardo s/ Medida autosatisfactiva*”² y “*B. C. c/ Facebook Argentina S.A. s/ Medida autosatisfactiva*”³.

4.- La computación en la nube o “Cloud Computing”

Cloud Computing es un paradigma de computación distribuido que permite ofrecer servicios de computación a través de Internet. Mas comúnmente conocido entre los usuarios como “la nube”.

Para definirlo adecuadamente podemos utilizar los conceptos del NIST⁴ que lo define como “un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables⁵, que pueden ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios”.

De dicha definición resultan las cinco características principales a tener en cuenta:

- Autoservicio según necesidad.
- Amplio acceso a la red.
- Reservas de recursos en común.
- Rapidez y elasticidad.
- Servicio supervisado.

Es un paradigma de computación distribuido a gran escala, impulsado por las grandes economías, en el que un grupo abstracto, virtualizado y escalable dinámicamente de almacenamiento, plataformas y servicios es entregado por demanda a clientes externos a través de Internet.

Cloud computing ofrece a los usuarios finales ventajas en términos de movilidad y colaboración. Para los fabricantes de software, el software ofrecido como

1 <http://www.hfernandezdelpech.com.ar/JurisprudenciaMedidaAutosatisfactivaFacebook.html>

2 http://www.notiexpress.com.ar/index.cgi?mod=contentFront&_wf=true&accion=get&comando=article&articleId=138675.

3 <http://www.jusformosa.gob.ar/index.php/jurisprudenciaacercas/fallosdestacados/1209-b-c-c-facebook-argentina-sa-s-medida-autosatisfactiva>.

4 National Institute of Standards and Technology de USA.

5 Redes, servidores, almacenamiento, aplicaciones y servicios.

un servicio basado en Internet se puede desarrollar, testear y ejecutar en una plataforma informática elegida por el fabricante. Actualizaciones y correcciones de errores se despliegan en cuestión de minutos.

Los desarrolladores con ideas innovadoras para nuevos servicios de Internet ya no requieren grandes capitales económicos para desplegar su servicio o los costos humanos de operarlos. Ellos necesitan no preocuparse acerca del exceso de aprovisionamiento de un servicio cuya popularidad todavía no puede predecir. Por lo tanto, no malgastan costosos recursos, o se quedan por debajo de la demanda.

Como vemos, la nube hace que se reduzcan sustancialmente los costos incrementando a su vez la eficiencia de los recursos disponibles y de las soluciones tecnológicas, todo lo que se traduce en un notable servicio a la sociedad mediante la ayuda al cuidado del medio ambiente, cumpliendo así un importante objetivo de nuestra época, facilitando la reducción del consumo de energía, y provocando que múltiples recursos puedan ser usados al mismo tiempo por un gran número de usuarios, permitiendo la optimización de los recursos.

Facilita también el ámbito para la innovación, el uso de instalaciones inteligentes, y la desmaterialización de los procesos, todo lo que colabora en la creación y desarrollo de nuevas modalidades de trabajo, posibilitando un medio ambiente más sano y sustentable.

Cuando hablamos entonces de computación en la nube, hacemos referencia a un tipo de sistema distribuido y paralelo que consiste en una colección de computadoras virtuales interconectadas que están aprovisionadas dinámicamente y presentadas como uno o más de los recursos sobre la base de acuerdos establecidos mediante la negociación entre el proveedor del servicio y los consumidores.

El papel fundamental de la computación en la nube es evidente, pero la importancia del cliente no puede pasarse por alto debido a grandes razones:

- ✓ De seguridad: La gente puede no estar dispuesta a ejecutar aplicaciones críticas en la nube o enviar información sensible para ser procesada y guardada.
- ✓ Los usuarios quieren tener las cosas hechas incluso cuando Internet o la nube puedan estar caídas o los canales de comunicación estén funcionando lento.
- ✓ Con los avances de la tecnología multi – núcleo, la próxima década traerá las posibilidades de tener supercomputadores de escritorio.

Las nubes en general proveen servicios en tres niveles diferentes:

- ✓ Infraestructura como Servicio (IaaS, Infrastructure as a Service) provisiona hardware, software y equipamiento (mayormente en la capa unificada de recursos) para entregar ambientes de aplicación de software con un modelo de precio basado en el uso. La infraestructura puede escalar hacia arriba o abajo dinámicamente basado en la aplicación de las necesidades de recursos.
- ✓ Plataforma como Servicio (PaaS, Platform as a Service) ofrece un ambiente integrado de alto nivel para construir, probar y desplegar aplicaciones personalizadas. Generalmente los desarrolladores deben aceptar algunas restricciones en el tipo de software que puede escribir a cambio de

escalabilidad embebida de la aplicación. Un ejemplo es el motor de Google's App, el cual permite a los usuarios construir aplicaciones Web en los mismos sistemas escalables que subyacen en las aplicaciones de Google.

- ✓ Software como Servicio (SaaS, Software as a Service) consiste en software de propósito especial que es remotamente accesible por clientes a través de Internet con un modelo de precio basado en el uso. Como ejemplo, Salesforce es un líder mundial en proveer online CRM (Software para la administración de la relación con los clientes), o Mesh de Microsoft, que permite que las carpetas y los archivos estén compartidos y sincronizados a través de múltiples dispositivos.

En cuanto a su naturaleza jurídica, podemos encuadrar el cloud computing como una prestación de servicios, si bien comparte elementos con otras figuras jurídicas, como por ejemplo el de licenciamiento común de derechos de uso, de ciertos programas, recursos, y aplicaciones, basados en la infraestructura de red. La característica principal de esta contratación es que los recursos son proveídos a distancia, dependiendo solo de las posibilidades de acceso a Internet de los usuarios sea cual sea el lugar en donde se encuentren, lo que hace que sea muy común las contrataciones con proveedores de países extranjeros.

Pero lo que provoca muchos interrogantes es acerca de la privacidad, la seguridad y la confiabilidad. Permitiendo que un tercero tome custodia de documentos personales, se generan preguntas incómodas acerca del control y la propiedad: si uno se mueve a un proveedor de servicios competidor, ¿puede llevarse los datos consigo?, ¿puede perder acceso a todos los datos si no paga una factura?, ¿tiene el poder de borrar definitivamente documentos que ya no quiere?

Se deberá entonces, crear el marco jurídico regulatorio acorde para su desarrollo en el país, pero siempre teniendo en cuenta los principios de neutralidad tecnológica, flexibilidad, interoperabilidad, sin basarse en cuestiones excesivamente territoriales atento su modalidad de realizarse mediante proveedores de los mas diversos países, pero que permita brindar seguridad efectiva a la información, en especial cuando se involucran datos personales donde pudieran vulnerarse las previsiones de la ley 25326 en la materia de protección.

Los organismos internacionales tendrán que estudiar y tratar de favorecer la armonización de las normas locales para la adecuada inclusión de normas de privacidad según los standards internacionales de seguridad existentes.

Mientras la encriptación es efectiva para asegurar los datos antes de guardarlos en el proveedor, no puede ser aplicada en servicios en donde los datos sean computados. En Amazon EC2, el proveedor almacena máquinas virtuales en nombre de los clientes, quienes pueden hacer cómputos arbitrarios. En estos sistemas, cualquier con acceso privilegiado al host puede leer o manipular los datos del cliente. Hay una clara necesidad de buscar una solución técnica que garantice la confidencialidad e integridad de los cómputos, de una manera que sea verificable por el cliente del servicio.

Se plantean varios riesgos que un usuario de una nube debería consultar con el vendedor antes de comprometerse:

- ✓ *Acceso de usuarios privilegiados:* La información sensible que es procesada fuera de la empresa necesita la seguridad de que será accesible solamente por usuarios privilegiados.
- ✓ *Cumplimiento de la normativa:* El cliente necesita poder verificar si el proveedor tiene auditorías externas y certificados de seguridad, y si su infraestructura cumple con los requisitos regulatorios de seguridad.
- ✓ *Localización de los datos:* Ya que el cliente no conocerá donde sus datos serán almacenados, es importante que el proveedor cumpla con guardar y procesar los datos en jurisdicciones específicas y que se someta a las exigencias locales de la privacidad en nombre del cliente.
- ✓ *Aislamiento de datos:* Necesita asegurarse que la información de un cliente está completamente aislada de la de otro cliente.
- ✓ *Recuperación:* Es importante que el proveedor tenga un mecanismo eficiente de replicación y recuperación para restaurar los datos si ocurre un desastre.
- ✓ *Soporte:* Los servicios de la nube son especialmente difíciles de investigar, si esto es importante para el cliente, debe garantizarse el soporte por contrato.
- ✓ *Viabilidad a largo plazo:* Los datos deben ser viables incluso cuando el proveedor sea adquirido por otra compañía.

Cloud Computing en Argentina

Las grandes empresas internacionales, que tienen sus oficinas en Argentina ofrecen a través de sus sitios, servicios de cloud computing. Es así como, por ej. IBM Argentina⁶ presenta IBM Smart Cloud, como una nueva oferta de Cloud Pública Corporativa; la consultora Accenture⁷ también ofrece el desarrollo de servicios para la nube, tales como Solución de Procesamiento de Datos, Herramienta de evaluación de oportunidades en la nube, entre otras.

EMC Argentina, es una compañía multinacional que cuyas ofertas de Cloud Computing se basan en: “respaldo y recuperación, administración de contenido empresarial, almacenamiento unificado, grandes volúmenes de datos, almacenamiento empresarial, federación de datos, archivado, seguridad, y duplicación ayudan a los clientes a moverse a la próxima generación de administración de la información y a ofrecer TI como servicio como parte de su camino a la nube”⁸.

Ciertos servicios de Cloud Computing fueron adoptados masivamente tanto a nivel empresarial como a nivel hogareño, tales como Webmail, Dropbox o Edición de documentos en línea. Sin embargo, ciertos productos más vinculados a datos críticos de negocio generan alguna resistencia en las empresas a la hora de pensar en la migración a la nube, sobre todo por las dudas respecto a la seguridad de la información almacenada.

5.- Resultados de las encuestas

5.1.- Resultados de la Investigación en Redes Sociales

6 <http://www.ibm.com/ar/services/cloud.phtml> accedido el 10 de Enero de 2013.

7 <http://www.accenture.com/ar-es/Pages/service-technology-cloud-computing-overview-summary.aspx> accedido el 10 de Enero de 2013.

8 <http://argentina.emc.com> accedido el 13 de Enero de 2013.

Con el fin de obtener más fácilmente información de las encuestas, las mismas se administraron electrónicamente durante el año 2011.

Presentamos aquí un resumen de los datos obtenidos:

Consultados sobre la cantidad de redes sociales que utilizan, la mayoría indica utilizar más de una red social, resultando un promedio de 1.7 por persona.

Se observa esta ocurrencia en el sentido de los diferentes usos de cada una de las redes sociales, donde la preponderancia de Facebook está relacionada con el aspecto social, y el de LinkedIn con el aspecto Profesional, por ejemplo.

Redes más utilizadas:

- Facebook: 85%
- LinkedIn: 35%
- Twitter: 25%
- Google+: 10%
- Youtube: 10%
- Grooveshark: 3%

Consultados sobre si comparten cuestiones personales en las redes sociales, el 65% de las personas indican compartir información personal en alguna red, el 53% intereses personales, el 71% comparte fotos personales, el 25% comparte videos personales en alguna red.

Consultados sobre si comparten cuestiones laborales en alguna red, el 40% de las personas comparte información laboral en alguna red, el 43% personas comparten intereses laborales en alguna red, el 5% de personas comparten fotos laborales en alguna red y el 5% de personas comparten videos laborales en alguna red.

Resulta llamativo observar que se comparte más información personal que laboral, pero la mayoría de esa información se comparte en Facebook, red que está dedicada a las relaciones sociales. En cambio, de los que dijeron compartir información laboral, el 45% lo hizo en LinkedIn, red dedicada netamente a lo laboral, y sólo un 30% lo hace en Facebook.

Por otro lado, consultados sobre si creen que hay información que no compartirían en una red social, dejándola para su esfera privada, el 25% de los encuestados contestó que no tendría reparos, y considera que compartiría cualquier tipo de información. Son todas personas con estudios universitarios incompletos, entre 19 y 45 años y de diversas profesiones (entre las cuales se encuentra estudiantes de ingeniería y abogacía).

Surge de nuestro estudio, que sólo el 12 % de los usuarios leyó los términos y condiciones ofrecidas por su red social, el 23% leyó las políticas de privacidad. Son personas con estudios universitarios incompletos y en su mayoría son mayores de 45 años.

Es importante aclarar que también forma parte de esta investigación, el estudio de los términos y condiciones de las redes sociales mayormente utilizadas en Argentina, siendo seleccionadas: Facebook, LinkedIn, Twitter, Badoo, YouTube y Google+. Surge del análisis, que los términos y condiciones pueden ir variando a lo largo del tiempo y que el usuario puede ser notificado o no de dichos cambios.

También es importante el hecho de que, más allá de que es muy bajo el porcentaje de Usuarios que leyó los términos y condiciones, un 12%, un 11% de Usuarios dijo leer la política de privacidad sin haber leído los términos y condiciones, lo que implica, un conocimiento parcial de sus derechos y obligaciones. Estas son personas de variadas profesiones y sus edades abarcan entre los 26 y 45 años.

Sin embargo, a pesar del desconocimiento de las políticas de privacidad, se advierte que el 59% de los usuarios ha cambiado la privacidad de su perfil en algún momento.

Esta situación manifiesta una inquietud por la privacidad de la información volcada en la red.

Consultados sobre la actividad de los usuarios en las redes sociales, el 15% de los Usuarios manifestó acceder todo el tiempo, el 32% una o más veces al día, el 32% una o mas veces por semana, el 13% accede una o más veces al mes, el 7% accede menos de una vez al mes y el 1% no accede nunca.

Se puede concluir que el 79% de los usuarios accede al menos una vez por semana.

El 10% de los Usuarios consideran a la red social como un servicio “Esencial” en su vida y quehaceres cotidianos. Son usuarios de LinkedIn, Facebook y Twitter de entre 26 y 45 años.

Consultados sobre si se sienten “seguros” en el uso de la red social, el 45% manifestó que se sienten seguros y que no hay cuestiones de privacidad de sus datos que lo inquieten, mientras que de los que dijeron no sentirse seguros, solo el 9% de los usuarios manifestó haberse visto perjudicado por el uso de su red social.

5.2.- Resultados parciales de la investigación en Cloud Computing

Desde el punto de vista institucional, el 50% de las empresas encuestadas tienen como objeto de negocio Servicios Informáticos, como así también podemos decir que el 70% son empresas chicas, ya que tienen menos de 20 empleados. Con la utilización de estas nuevas herramientas tecnológicas y su facilidad de acceso, en muchos casos de modo gratuito, las empresas tienden a la reducción de costos en infraestructura, personal, software, entre otros. De nuestro estudio observamos que aunque Cloud Computing es un nuevo modelo de negocio tecnológico el 80 % de ellas utiliza el servicio desde hace mas de 1 año y menos de 5.

Consultados sobre los servicios que utiliza en la web el 90% utiliza el Software como servicio (Ej: GoogleApps: GoogleDocs o Similares, Office365, Dropbox, logme In, issu.com, Google). Cabe destacar que con estas aplicaciones se reduce a 0 el costo de licencia de software para el usuario de Cloud Computing.

En nuestra investigación, dividimos a los servicios de Cloud Computing como onerosos y gratuitos, y encontramos que el 90% de las empresas encuestadas utilizan ambos servicios.

Aunque las empresas entregan sus datos, basándose en la confianza que el proveedor del servicio les brinda, dado que se desconocen muchos de los mecanismos de seguridad y protección aplicados, el 100% de las empresas consultadas mostró conformidad con los servicios prestados y el nivel de seguridad otorgados por el proveedor del servicio. Los contratos a los cuales se adhieren para obtener el servicio

ya vienen impuestos, quedándoles solo una alternativa: aceptar o no disponer del servicio, opacando así el principio de la autonomía de la voluntad.

Resulta de nuestra investigación que aunque la empresa deba abonar por los servicios contratados, sólo el 60% de ellas leyeron los Términos y Condiciones.

Consultadas si han migrado de proveedor de servicio, el 30% contestó que sí, aunque solo el 10% lo atribuyó a una caída de servicio anterior que impidió la realización de una campaña comercial.

Consultadas si ha sufrido algún incidente de seguridad, el 10% contestó que sí, aunque el mismo fue solucionado y no lo atribuyó al proveedor del servicio.

Para los servicios gratuitos, la mitad de las empresas consultadas no leyeron los Términos y Condiciones.

Idénticamente con las empresas que utilizan servicios onerosos el 30% ha migrado de proveedor, aunque cuando se les consultó si habían sufrido algún incidente de seguridad el 20% indicó que sí.

6.- Recomendaciones a Usuarios de Redes Sociales

Es imprescindible leer los contratos de adhesión a las Redes Sociales antes de su aceptación, aunque en muchas de ellas las obligaciones de los usuarios se diluyen entre marañas de cláusulas contractuales.

Debemos promover y difundir las Redes Sociales que dispongan de Códigos Éticos que vayan más allá de la aplicación de lo dispuesto en las normas legales.

Si se ha vulnerado el derecho a la privacidad, lo recomendado es lo siguiente:

- Ponerse en contacto con los administradores del sistema a través de los sistemas de denuncia con los que cuente la Red Social para que el video o fotografía en los que aparezca el usuario sean eliminados, al no existir permiso expreso por parte del titular. De igual manera, deberá solicitar la retirada del comentario o texto que atente contra su intimidad.
- Ponerse en contacto con los buscadores que hayan indexado el contenido, para que procedan a su bloqueo o retirada, de tal forma que deje de aparecer dentro de los resultados en el momento de hacer las búsquedas.

En ambos supuestos las notificaciones deben hacerse sobre soportes fehacientes a fin de poder luego ser probadas en una eventual y futura acción judicial (carta documento, telegrama, acta notarial).

- Iniciar las actuaciones judiciales pertinentes ante los Tribunales.
- Emplear diferentes usuarios y contraseñas para entrar en las distintas redes.
- Las contraseñas deben ser seguras, con una extensión mínima de 8 caracteres, alfanuméricos y con uso de mayúsculas y minúsculas.
- Configurar el grado de privacidad del perfil del usuario de la Red Social, de tal forma que no sea completamente público.
- Aceptar como contacto únicamente personas conocidas o con las que mantiene alguna relación previa.

- No publicar en el perfil del usuario información de contacto físico, que permita a cualquier persona conocer dónde vive, dónde trabaja o estudia frecuentemente, o los lugares de ocio que suele frecuentar.

7.- Recomendaciones a Usuarios de Cloud Computing

Los Proveedores de Servicios de la Nube CSP (Cloud Service Provider) han estado buscando la manera de asegurar la integridad de los datos que son almacenados en la nube.

Debido al gran tamaño de los datos subidos a la nube, corroborar la integridad y veracidad de los datos es una tarea costosa y prácticamente irrealizable para los usuarios. Sin embargo, es importante que los usuarios puedan confiar y no deban preocuparse por verificar la veracidad de la información una vez volcada, es ahí donde se vuelve de crítica importancia la presencia de un tercero “de confianza” que pueda realizar auditorías periódicas a los datos cuando sea necesario⁹.

La idea de esta tercera parte es que deba tener la experiencia y habilidades en auditorías informáticas, que los usuarios pueden no tener, y que pueda chequear la integridad de los datos almacenados en la nube. De esta manera, puede ayudar a los usuarios también a evaluar los riesgos de suscribir estos servicios.

Surgió de nuestra investigación que las empresas entregan sus datos, basándose en la confianza que el proveedor del servicio les brinda, dado que se desconocen muchos de los mecanismos de seguridad y protección aplicados, el 100% de las empresas consultadas mostró conformidad con los servicios prestados y el nivel de seguridad otorgados por el proveedor del servicio. Los contratos a los cuales se adhieren para obtener el servicio ya vienen impuestos, quedándoles solo una alternativa: aceptar o no disponer del servicio, opacando así el principio de la autonomía de la voluntad.

En conclusión, habilitar las auditorías públicas podría jugar un papel importante para que el desarrollo de la economía naciente de la “nube” se establezca y permanezca, generando confianza en los usuarios, y asesorando respecto a los posibles riesgos existentes.

En este sentido la “Cloud Security Alliance” presenta instrumentos que favorecen la difusión y publicidad de documentos de control de empresas que ofrecen servicios cloud. Además la CSA (Cloud Security Alliance) ofrece online con un conjunto de documentos que pueden ayudar como guías de seguridad para detectar áreas críticas en los servicios de Cloud Computing.

CSA es una organización sin fines de lucro que promueve el uso de las buenas prácticas de tratamiento de la seguridad dentro del Cloud Computing.

CSA lanzó un programa denominado STAR (Registro de Garantía de Seguridad y Confianza). STAR es un registro gratuito, de acceso público, que documenta los controles de seguridad proporcionadas por las diversas ofertas de servicios en Cloud Computing, ayudando así a los usuarios a evaluar la seguridad de los proveedores de la nube.

9 Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, <http://www.cloudsecurityalliance.org>.

8.- Consideraciones Finales

Estamos obligados a aceptar las nuevas tecnologías de información así como el impacto y los cambios que ellas han producido en la sociedad y en el modo que esta tiene de comunicarse. Los cambios son vertiginosos y el Derecho siempre va tras ellos tratando de llenar los vacíos legales que se producen, por ello es importante investigar los fenómenos que se producen y considerar sus efectos, para poder entender y prever sus consecuencias.

Pretendemos que estas recomendaciones puedan ayudar a los usuarios a manejarse mejor en esta materia tan nueva por su contenido como por su desconocimiento.

La mayoría de los usuarios considera fácil, y conveniente estos sistemas lo cual hace que crezca rápidamente el número de personas y empresas que lo utilizan.

El poder compartir la información con otros usuarios le agrega valor a esta relación de consumo, pero a su vez este sistema multiusuario puede implicar accesos no autorizados a nuestros datos, situaciones que encuadren en figuras delictivas informáticas en nuestra ley, pero ¿qué pasa cuando otros países no penalizan dichas conductas?

Todas las facilidades apuntadas con anterioridad, se enfrentan aún a más problemas jurídicos sin resolver como la privacidad y protección de los datos, la jurisdicción y ley aplicable en caso de litigios, la protección de la propiedad intelectual, etc.

A esto se suman otros cuestionamientos, como por ejemplo, si sigo siendo yo quien tiene siempre el control de los datos que se suben a la nube. Si tiene el proveedor un plan de contingencia adecuado por imprevistos que pudieran producirse e impidan el acceso a los documentos allí ingresados. ¿Quién será el responsable por lo que allí ocurra y que tipo de responsabilidad le cabe? ¿Qué jurisdicción corresponde al ciberespacio donde se encuentra la nube? ¿Qué puede hacer el usuario frente a un daño concreto que se le produzca?

Estos y muchos otros son los cuestionamientos y desafíos que el Derecho tiene que resolver y contestar para evitar efectos no deseados.

Los usuarios individuales y empresas que utilicen estos servicios no tienen por qué rescindir sus habituales condiciones de seguridad, medidas de protección y confidencialidad porque ingresen al sistema de cloud computing, sino todo lo contrario. Deberán tratar de exigir dichas garantías en beneficio del colectivo de usuarios, en tanto los países terminen de definir el marco jurídico global que respetar al respecto.

Bibliografía

[1] <http://www.opencloudinitiative.org/> consultada el 17 de Julio de 2012.

- [2] M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at <http://www.techcrunch.com/2006/12/28/gmail-disaster-reports-of-mass-email-deletions/>, December 2006.
- [3] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," Online at <http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closes-its-doors/>, July 2008.
- [5] Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at <http://status.aws.amazon.com/s3-0080720.html> 2008.
- [6] S. Wilson, "Appengine outage," Online at <http://www.cio-weblog.com/50226711/appengine> outage.php, June 2008.
- [7] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at <http://voices.washingtonpost.com/securityfix/2009/01/payment-processor-breach-may-b.html>, Jan. 2009.
- [8] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage"
- [9] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, <http://www.cloudsecurityalliance.org>.
- [10] Elizalde, Francisco Martín "Prueba en la Cloud Computing: Cloud Computing & Service Level Agreements El modelo en los Estados Unidos de América y su proyección al ámbito legal argentino" *elDial.com* - DC15EE, Publicado el 08/06/2011