Perfiles de las Ciencias Sociales, Año 3, No. 6, Enero – Junio 2016, 336-346 pp.
Http://revistas.ujat.mx/index.php/perfiles, México, UJAT.

PELIGROS DEL CLOUD COMPUTING: POSTURA FRANCO-EUROPEA

Guy Mazet[1]
Artículo Científico Recibido: *26 de agosto de 2015* ***Aceptado:*** *26 de octubre de 2015*

INTRODUCCION

El medio rector para la difusión de la información es internet, además de las posibilidades de extensión que tiene más allá de las computadoras y los dispositivos móviles permite la interacción con un número cada vez más creciente de objetos y de personas que interactúan entre ellos. Dicha evolución plantea numerosas interrogantes relativas a las libertades individuales pero también a la soberanía nacional. Los objetos calificados como conectados, comunicados o inteligentes podrían alcanzar entre 50 y 80 mil millones en el mundo en 2020. Los objetos conectados empiezan a insertarse dentro de la vida cotidiana e individual que llegan a estar dentro de la intimidad personal, su utilidad va desde la medición de parámetros de salud, hasta gadgets que miden la temperatura, el tráfico, el depósito bancario entre otros disponibles en relojes inteligentes, tabletas electrónicas y celulares.

De este manejo de la información, surge el hecho de que los datos constituyen una fuente de creación de valor. Cada que se accede a diferentes sitios de interés particular, el cliente/usuario deja una huella digital que permite a los publicistas analizar sus necesidades y promover un servicio personalizado, adaptado al cliente. Esto permite conocer mediante los objetos conectados proporcionar información sobre gustos, hábitos, relaciones, ya que las grandes empresas digitales obtienen y controlan las huellas de los usuarios y la multiplican en cantidades.

La capacidad de colectar los datos de los usuarios a través de estos objetos conectados aumenta los riesgos de atentar contra la vida privada mediante una lectura constante de actuaciones individuales; el temor de asistir al deterioro de la protección de datos personales ha tenido su paroxismo con la develación del sistema de vigilancia establecido por parte de la agencia norteamericana NSA.

[1] Guy MAZET. Doctor en Derecho. Instituto de Altos Estudios sobre América Latina. Universidad Paris 3 Sorbona Nueva Paris.
mail: kgm@noos.fr

Lo cierto es que la multiplicación de objetos conectados heterogéneos implica una potenza de cálculo más y más importante para manejar todos los datos involucrados en el proceso pero también recursos a servicios alejados de almacenamiento y análisis de contenidos: ahí encontramos el « Cloud » herramienta del « Big Data » ; dicha solución es un imperativo para los operadores de la conexión de objetos ya que se debe garantizar un tiempo de respuesta mínimo dentro el intercambio entre objetos y plataformas de gestión para evitar todo congestión.

Entonces se llama a las supuestas bondades del Cloud computing quien reúne para las empresas los beneficios económicos de la externalización de los procesamientos y servicios con los de arquitecturas de fuertes seguridad tecnológicas.

En efecto, el cloud puede caracterizarse como un modelo para habilitar el acceso a un conjunto de servicios computacionales (redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, rápidamente aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor de servicios ; entonces, el computo en la nube ofrece varias soluciones a las empresas y administraciones , pues permite el almacenamiento masivo de datos sin necesidad de contar centrales enormes de equipos físicos y su personal técnico, lo cual redunda en ahorros de costos significativos para los corporativos y servicios públicos.

Dicha nube opera en la red e integra diversos elementos que funcionan como uno solo a través de tecnologías basadas en distintos programas para crear máquinas virtuales más estables que el computo basado en servidores y en equipos como discos duros o memorias USB.

Este modelo se expande mediante contratos que firmen empresas o administraciones públicas con un tercero que provee servicios de cloud con la garantía que se maneja la información sin arriesgar los contenidos y los derechos de los eventuales titulares de los datos personales, o sea en el tramo en el internet, o sea en el sitio mismo del tratamiento con el requisito que este último queda conocido ; por eso se necesita tomar medidas jurídicas y tecnológicas para asegurar la seguridad contractual en el uso del cloud; el objeto de esta contribución es de exponer la postura francesa-europea al respecto.

En lugar de presentar un debate sobre las ventajas y peligros del cloud, hemos optado por un planteamiento de las problemáticas más recurrentes tratando de estas nuevas tecnologías.

De manera preliminar debemos presentar las modalidades de servicios ofrecidos mediante el cloud; dichos servicios distinguen:

El **SaaS** o Software as a Service es decir proveer programas on line

El **PaaS** o Platform as a Service o sea proveer una plataforma de desarrollo de aplicaciones on line

El **IaaS** o Infraestructura as a Service o sea proveer infraestructura de cómputo y de almacenamiento on line.

Estos varias servicios pueden declinarse según modos distintos: el « **Cloud público** » para un servicio compartido con muchos clientes, el « **Cloud privado** » para un servicio dedicado a un solo cliente y el « **Cloud Hibrido** » para una combinación de los dos. Lo más frecuentemente encontrado será el Cloud Publico para las empresas y sobre todo las ofertas SaaS (programas on line).

CALIFICACIÓN DE LOS ACTORES DEL CLOUD COMPUTING

Hay que recordar que el **responsable** del tratamiento es la persona física o jurídica quien define las finalidades y los recursos del procesamiento de los datos personales; el **incargado** ello, maneja los datos personales por cuenta del responsable según sus directivas.

Eso significa que el **cliente** siempre será responsable del tratamiento; en efecto, recolectando los datos y decidiendo de externaliza su manejo mediante un proveedor de servicios de cloud, esta responsable del tratamiento por determinar las finalidades y los medios de tratamiento.

El **proveedor** actúa por cuenta y bajo instrucciones del cliente responsable del tratamiento; entonces, parece posible de establecer una presunción de sub contratación en la relación entre cliente y proveedor de servicio cloud.

Tal presunción será particularmente efectiva cuando llama a un cloud privado, o sea especifico al cliente, que implica un gran dominio en la realización de la prestación por parte del proveedor . Al revés, cuando un cliente llama a un cloud público en

donde, por esencia, el proveedor define el funcionamiento y los objetivos de una aplicación on line accesible a varios clientes, los papeles respectivos del cliente y del proveedor pueden ser difíciles en determinar. Por eso, dicha presunción puede caer aplicando un conjunto de criterios que permiten definir el margen de maniobra cuyo proveedor dispone para realizar el servicio.
Estos criterios serían:

- El nivel de las instrucciones o directivas dadas por parte del cliente al proveedor: este criterio puede permitir evaluar en cual medida el proveedor queda comprometido por las órdenes del cliente responsable; entonces, si el cliente deja una grande libertad y autonomía al proveedor en la realización del servicio, el proveedor actuara también como responsable del tratamiento.
- El grado de control en la ejecución del servicio por del proveedor de parte del cliente responsable; eso permite medir la manera con la cual el proveedor respecta las instrucciones del cliente; conviene entonces preguntarse sobre el grado de vigilancia ejercitado por el cliente en su calidad de responsable.
- El valor agregada provista por el proveedor sobre el tratamiento de datos del cliente ; eso permite saber en cual medida el proveedor tiene el dominio del manejo de los datos; es cierto que cuando presenciamos un proveedor experto en la rama ello podrá con razón decidir de los recursos necesarios y , por ende, susceptible de ser calificado igualmente de responsable
- El grado de transparencia sobre la llamada a un proveedor, eso puede indicar en cuanto la calificación o expertos del proveedor; si la identidad o fama del proveedor está muy conocida en el ámbito del cliente, el proveedor podrá también ser considerado como actuando en calidad de responsable.

De todo esto, resulta que cuando un cliente llama un proveedor de servicios cloud, queda generalmente admitido que el primero esta responsable y el segundo sub contratante.

Sin embargo, en ciertos casos de PaaS y SaaS públicos, los clientes, a pesar de ser responsables de la elección de sus proveedor no pueden , en realidad, darle órdenes e

instrucciones y tampoco no pueden controlar la eficiencia de las garantías de seguridad y confidencialidad llevadas por el proveedor ; dicha ausencia de directivas y medios de control se debe sobre todo al carácter estandarizado de las ofertas de servicios, sin posibilidades de modificación por parte del cliente y la existencia de verdaderos contratos de adhesión que no posibilitan cualquiera negociación.

En dicha situación, el proveedor podría a priori ser considerado como conjuntamente responsable en aplicación de la definición del responsable del tratamiento según el artículo 2 de la Directiva 95/46/CE, ya que el proveedor participe a la determinación de las finalidades y de los recursos de los tratamientos de los datos personales.

Por eso, para prevenir todo riesgos de dilución de las responsabilidades siempre será conveniente precisar expresa y claramente cómo van compartirse las responsabilidades entre las partes del contrato.

En este sentido, debemos llamar la atención sobre algunas posibles fuentes de problemas que deben ser dilucidados previamente en el contrato tales: ¿ quién del cliente o del proveedor queda supeditado a las obligaciones de declaración antes las autoridades de protección competentes o si se encuentren conjuntamente responsables? ¿Quién debe informar el titular de los datos personales de las modalidades del tratamiento? Misma pregunta en lo relativa a las obligaciones de confidencialidad y de seguridad; una dificultad atañe el ejercicio de los derechos del titular cuando la diseminación posible de los datos en varios servidores ubicados en país diferentes hace muy complicado dicho ejercicio ; en este caso, se debe asegurar que tanto el cliente como el proveedor garanticen el ejercicio de los derechos « ARCO » del titular de los datos personales.

En este contexto, debemos recordar que el proveedor no puede usar los datos personales llevados por sus clientes nada más que con instrucciones de estos últimos; en consecuencia, un proveedor quien quería manejar datos para otras finalidades (por ejemplo en vista de uso publicitario) rebasaría los órdenes de su cliente cuando no informara su cliente de sus intenciones y no tendrá una previa autorización ; si obtiene dicha autorización, entonces el proveedor será responsable del tratamiento hecho por una finalidad distinta de la del cliente. En tale situación, cada uno, el cliente y proveedor será responsable del tratamiento operado.

Hay que saber que la Comisión europea ha publicado en 2012 un proyecto de reglamento – más alta norma en la jerarquía jurídica de normas europeas – relativo a la protección de los datos personales creando un verdadero régimen legal del proveedor

cuando prevé un listado no exhaustivo de los elementos debidamente presentes en el contrato de servicio de computo en la nube. El proyecto submite el proveedor a varias obligaciones comunes con el cliente responsable del tratamiento; así, el proveedor será supeditado a obligaciones de documentación, de cooperación con las autoridades de control, de seguridad de los tratamientos, de notificación al responsable en caso de violación de datos personales, de análisis de impacto, de autorización o previa consulta de las autoridades de control, del nombramiento de un representante en materia de protección de datos y enmarcamiento de las transferencia de datos.

Tal estatuto legal supeditando el proveedor a numerosas obligaciones importantes parece ser una interesante solución reequilibrando el balance de los poderes en el espacio de las responsabilidades.

Pero, por el momento dicho proyecto se encuentra estancado por dos razones: el impacto del asunto NSA quien ha trastocado las susceptibilidades europeas y las negociaciones del Tratado Transatlántico en donde las cuestiones de los datos personales se encuentran muy debatidas.

DETERMINACION DE LA LEY APLICABLE

Una de las grandes dificultades consiste en la definición de la ley aplicable a los actores del cloud computing.

Una regla satisfactoria Sicilia podría ser que la ley del responsable del tratamiento seria la ley aplicable; sin embargo, este propuesta aleja el criterio salido de los medios del tratamiento encarado por la legislación francesa según la cual esta última será aplicable cuando el tratamiento esta realizado por parte de un responsable del tratamiento no establecido en la Unión Europea pero quien llama a recursos de tratamiento ubicados en el territorio francés ; así, se restringe el campo de aplicación de la ley francesa y aumenta el fenómeno del dicho »fórum shopping ».

Este « fórum shopping »está constituido por el hecho que una empresa escoge de implementarse en un país más que otro considerando los ventajas nacidos de su legislación; (por ejemplo la ausencia de previa autorización de las autoridades inglesa respecto las transferencias hacia los países ubicados fuera de la Unión Europea podrá incitar una empresa norteamericana querando abrir una substituta en Europa en elegir el Reino Unido). Entonces tal solución no presenta tantos beneficios. En contrario, tomando en cuenta la dificultad del escoger del responsable del tratamiento para definir la ley aplicable, el criterio del « blancaje » puede ser interesante; este criterio queda previsto en

el proyecto del reglamento europeo para los responsables de tratamiento no establecidos en la Unión europea pero quienes ofrecen bienes y servicios a personas teniendo su residencia en el territorio de la Unión. En este sentido, hay que notar que el concepto de servicios se entiende como medios de tratamiento y eso de manera extensiva y que los *cookies* y las banderas *JavaScript* están consideradas como medios de tratamiento...
Por fin, otra solución consiste en que sea aplicable la ley del Estado miembro del lugar de ejecución principal de la prestación.

REGULACION DE LAS TRANSFERENCIAS

Ahí se trata de las transferencias de datos fuera de la Unión Europea ; de un punto de vista jurídico, la multiplicación de los lugares potenciales de almacenamiento de los datos hace difícil la concepción de herramientas jurídicos que pueden garantizar un nivel de protección adecuado como previsto en la legislación europea.

Frente a estas dificultades, podemos pensar en una solución en donde los proveedores insertan dentro sus contratos, cláusulas contractuales tipos que se acercan del sistema de los **BCR** o sea **Binding Corporates Rules** es decir reglas vinculantes entre empresas ; las BCR son un verdadero código de conducta definiendo la política de una empresa en materia de transferencia de datos; les BCR permiten ofrecer una « protección adecuada » a los datos transferidas desde la UE hacia países terceros dentro una misma empresa o grupo de empresas. Dichas BCR para proveedores permitirían al cliente del proveedor dejar los datos personales transferidos con la seguranza que, en el seno del grupo al cual pertenezca el proveedor, dichas datos van beneficiar de un nivel de protección adecuado.
El enmarcamiento de las transferencias de los datos puede también descansar sobre soluciones técnicas como por ejemplo el uso de « metadatos » para definir o describir otras datos cualquiera que sea su soporte o bien soluciones de cifra miento. Tal tecnología podrá ser una solución satisfactoria en caso de transferencia hacia ciertos países únicamente; entonces, en este caso el cliente podrá verdaderamente jugar su papel de responsable del tratamiento determinando, con precisión, antes la realización de la prestación, los países destinatarios de los datos.

Pero hay que decir que actualmente los mecanismos de transferencia no se encuentran adaptados al contexto del Cloud computing. En general, se considera que los BCR quedan la herramienta más adaptada y, por eso, la propuesta de creación de BCR para proveedores sus encarada parece acogida con mucho éxito dentro los operadores del mercado.

Hay que notar que el proyecto de reglamento europeo en sus artículos 42 y 43 prevé que las transferencias de datos hacia países terceros sean posibles cuando el responsable del tratamiento o el proveedor han puestos en marcha herramientas que permiten ofrecer garantías de protección de los datos adecuadas con la reserva de una previa autorización de parte de las autoridades nacionales cuando dichas herramientas no presentan un carácter vinculante. El reglamento impulse también el concepto de BCR proveedor.

Entonces, en la espera de la publicación del reglamento europeo, podemos recomendar un marco regulatorio de las transferencias de datos llamando a la firma de cláusulas contractuales tipo publicadas por la Comisión europea; en este caso las soluciones van diferir según la calificación y la ubicación del proveedor:

- Si el cliente transfiere los datos a un proveedor de cloud ubicado fuera de la UE actuando en calidad de subcontratarte: firma de cláusulas contractuales tipo del año 2010 quienes prevén la cadena de subcontratación.
- Si el cliente transfiere los datos hacia un proveedor ubicado dentro la UE actuando en calidad de subcontratarte quien va, a su turno, transferir por asimismo, los datos a otro sub contratante ubicado fuera de la UE: se puede encarar varias opciones: firma de cláusulas contractuales tipo 2010 entre el responsable y el subcontratarte fuera de la UE, mandato o contrato tripartes.
- Si el cliente transfiere los datos a un proveedor ubicado fuera de la UE actuando en calidad de responsable del tratamiento : firma de cláusulas contractuales tipo de 2001 o 2004; si el proveedor transfiere posteriormente los datos de su cliente a un sub contratante fuera, entonces vamos encontrar dos posibilidades :o sea , el cliente firme directamente las clausulas 2010 con este proveedor, o bien, el proveedor del cloud firme un contrato retomando las obligaciones de las clausulas 2010 con el requisito que sea previsto dentro el contrato entre cliente y proveedor de cloud la obligación para este ultimo de firmar un contrato equivalente a las clausulas contractuales tipo con todo proveedor.

SEGURIDAD DEL CLOUD COMPUTING

La cuestión de la seguridad de los datos es céntrica para los clientes llamando al Cloud computing y es cierto que ella constituye sus preocupaciones prioritarias.

En efecto, usando el Cloud, la empresa va externalizar los datos personales que ella maneja pero también los datos patrimoniales y estratégicas así como los procesos mismos; entonces, cualquiera parada , apagón o falla puede desembocar en una suspensión de actividades con consecuencias desastrosas respecto al cliente y la competencia.

El reforzamiento del contrato de Cloud y los compromisos de nivel de servicios para la protección de datos constituye un avance en la aproximación de la seguridad.

Si la contractualizacion de las condiciones de seguridad del tratamiento queda percibida como una necesidad primera, muchos de los operadores del mercado del Cloud subrayan las limitas debidas al carácter estandarizado de las ofertas de Cloud computing y al hecho que muchas veces, el proveedor define de manera unilateral las medidas que le parecen asimismo, pertinentes. Entonces, a veces, parece necesario llamar a los medios clásicos para enmarcar la seguridad de los tratamientos en el Cloud, como la certificación del proveedor. Por eso, existe disposiciones mínima que deben ser insertadas dentro el contrato (por ejemplo la responsabilidad en caso de pérdida de los datos) y se deben también promover o facilitar la creación de **SLAs** y **PLAs** asociados al texto mismo del contrato ; los SLA por Service Level Agreement, son compromisos del nivel de servicio por parte del proveedor y represente práctica usual en el marco de las prestaciones de servicios ; los PLA por Privacy Level Agreement es una forma de SLA para la protección de los datos personales ; este concepto queda en desarrollo dentro la Cloud Security Alliance.
Definitivamente, es verdaderamente importante que los contratos estandarizados incluyen dichos SLAs y PLAs.

OTRAS MEDIDAS DE PREVENCIÓN

La análisis de riesgos, reconocida como esencial no puede encararse sino como complementaria de la toma en cuenta de una debida protección de los datos persónales sobre todos en los casos de las pequeñas y medianas empresas (pymes) quienes muchas veces no tienen los recursos financiarías y técnicos para realizar dicha análisis de manera completa. Tratando de las medidas de seguridad, hay que subrayar las

medidas a veces impuestas, como la ISO 27001, la SAS70 o ISAE402. Estas normas proveen un marco que facilitan la evaluación de la seguridad ofrecida por el proveedor sin, no obstante, dar una absoluta garantía; cada vez se debe recomendar estudiar los requisitos exactos de la aplicación de la norma, sobre todo el « perímetro » de actividades de cada operadores sabiendo que se puede identificar tanto factores de riesgos del lado del cliente que del lado del proveedor....

El cifra miento parece ser la más segura de las medidas para el cliente de controlar el uso de los datos personales ; pero esta solución , todavía, no se encuentra, actualmente, técnicamente operatoria para la mayoría de los servicios de Cloud ; únicamente los servicios de almacenamiento de datos, tipo IaaS, parecen ser , hoy día, adaptados a la encriptación de datos del lado cliente pero tratándose de las aplicaciones más requeridas como SaaS se esperan avances más positivas ; al revés, otras opciones tal la « ofuscación » o sea proceso de padecimiento de los datos hasta rendir su comprensión imposible , parecen representar un provenir cierto.

El riesgo de acceso de los datos por parte de autoridades extranjeras, por ejemplo en el caso de la aplicación del *Patriot Act* en Estados Unidos debe ser encarado dentro el análisis de riesgos; (hay que recordar que el Patriot Act , puesto en marcha por las autoridades norteamericana del Homeland Security permite a estas últimas el acceso a los datos que se encuentran en los servidores con la consecuencia de la total ineficiencia de las cláusulas de protección de datos personales y otras reduciendo también los efectos del Safe Harbour elaborado entre los USA y la UE); en efecto , a pesar de ser transferidos mediante lazos cifrados (https o VPN), los datos quedan , en la mayoría de los casos, procesados « en claro » por el proveedor de cloud; una solución, cuando el cliente tiene recursos, será de poner en marcha una gestión de llaves adecuada y usar un algoritmo reconocido para, enseguida, cifrar los datos sobre las terminales del cliente antes de transferirles mediante un canal segurisado ; entonces, solo el servidor involucrado o sea el del proveedor de cloud, podrá leer los datos mandatos; sin embargo, esta tecnología, inspirada de la de la firma electrónica avanzada no se encuentra adaptada a numerosos servicios SaaS del cloud como, por ejemplo, los servicios de gestión de documentos en línea ya que en este caso, el proveedor necesita un acceso in claro a los datos para proveer el servicio . Mas allá, la imposibilidad de reducir suficientemente el riesgo de acceso a los datos por parte de autoridades extranjeras, ya, ha incitado algunas autoridades encargadas de la protección de datos en limitar o prohibir el uso de ciertos servicios SAAs; tal es el caso de Noruega quien prohíbe el uso de Google Docs. En muchos casos.

En definitivo se confirme la necesidad de definir las referencias técnicas de la protección de datos en el Cloud; la norma ISO 27001 queda la más citada como ejemplo para los problemas relacionados con la seguridad de los sistemas de información; pero se trata de una norma genérica quien esta leja de encarar todas las especificidades del planteamiento de protección de la vida privada; no corresponda totalmente a las necesidades en dicha rama.

CONCLUSION

De un punto de vista jurídico, el Cloud computing plantea muchas dificultades respecto las reglas de protección de los datos personales, particularmente en caso del Cloud público.

Esta problemática se amplía con el carácter estandarizado de los contratos de adhesión quienes dejan a los clientes que poca margen de negociación ; los clientes sufren una insuficiencia de transparencia por parte de los proveedores de servicios cloud en cuanto a las condiciones de realizaciones de las prestaciones sobre todo en los aspectos de la seguridad y sobre la cuestión de la eventual transferencia en el extranjero para asumir el tratamiento. Frente a esta situación se puede aconsejar una estrategia de personalización del contrato aliada a una constante llamada a la normalización ya que norma tal la ISO 27001constituye una verdadera norma de gobernanza y de seguridad de los sistemas de información. Entonces, la seguridad optima salida de la normalización, la disponibilidad del proveedor antes el cliente y la personalización de los servicios deben ser las llaves quienes permitieron luchar en contra del temor de pérdida del dominio del sistema de información o del peritaje de los datos.