Revista Digital de la Red Iberoamericana de Derecho Informático

ElDerechoInformático

Revista Nº 17 - Junio 2014

www.elderechoinformatico.com

En esta edición agradecemos la colaboración de:
Lic. Jorge Luis García Obregon, Abog. Javier Fernandez Moore, Marta Robles, Asociación de Derecho Informático de Argentina (ADIAr), Abog. Romina Florencia Cabrera

Una producción de:
Red Iberoamericana ElDerechoInformático.com
El Portal de Derecho Informático más grande de Iberoamérica

Noticias, Artículos, Doctrina, Jurisprudencia, Eventos,

Capacitación, Librería Digital, Foros, Comunidad... Derecho Informático

Todo en un solo lugar

RED IBEROAMERICANA

ElDERECHOInformático.com

EL PORTAL DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA

REVISTA Nº 17 - WWW.ELDERECHOINFORMATICO.COM

JUNIO 2014

REVISTA DIGITAL DE LA RED IBEROAMERICANA DE DERECHO INFORMÁTICO

RED IBEROAMERICANA
ElDERECHOInformático.com

Directores

Abog. Marcelo Temperini - mtemperini@elderechoinformatico.com

Abog. Guillermo Zamora - gmzamora@elderechoinformatico.com

Edición, Diseño y Maquetación

Abog. Marcelo Temperini - mtemperini@elderechoinformatico.com

Redacción y Edicion

Abog. Guillermo Zamora - gmzamora@elderechoinformatico.com

Contacto: info@elderechoinformatico.com

Colaboradores Junio 2014

Abog. Javier Fernandez Moore

Abog. Romina Florencia Cabrera

Marta Robles

ADIAr

Lic. Jorge Luis García Obregon

Esta edición se demoró más de lo esperado, el tiempo disponible, las cosas, la vida los etceteras se sumaron para que ello ocurra.-

A veces las cosas no se dan como uno desearía, y contra eso no podemos hacer nada, son las circunstancias que nos envuelven que hacen que ello ocurra.-

Hace unos 5 años cuando se largaba la Red antes de ser la Red, tuve la suerte de conocer a un tipo fantástico, buena gente, brillante por donde se lo mire y que en uno de los pocos rasgos de inteligencia que he tenido, tuve de socio, obvio que me refiero a Marcelo, el de la columna de al lado.-

Hoy, me cuesta más que de costumbre escribir estas lineas, nunca sabemos que dice el otro en sus editoriales, pero sospecho que el se estará despidiendo, con gran dolor en el alma para mi....-

Como dije, me cuesta sobremanera escribir esto, sólo darle las infinitas gracias a Marcelo por estos años de compartir cosas, sabiendo que vas a seguir estando, y que en este lado de la columna vas a encontrar a un amigo.-

Gracias

Abog. Guillermo Zamora

Escribi ya varias veces esta editorial, pero nunca quedaba conforme. En eso se puede ver parte de mí, de querer siempre intentar hacer las cosas lo mejor posible. En este caso no es capricho, sino que la importancia de esta editorial, por ser la última, me hace repasar una y varias veces mis pensamientos.

Una revista que nació de una de las tantas ideas de Guillermo, y que con trabajo y esfuerzo pudimos publicar ya 17 números... nada más ni nada menos. Una revista que siempre se hizo a pulmón, buscando ser una alternativa de publicación de doctrina internacional en materia de derecho informático, para aquellos autores que no tenían (o no querían) la posibilidad de publicar en otros lados.

El tiempo pasa para todos, y en mi caso el tiempo ha traído nuevas responsabilidades y otros caminos, que me obligan a dar un paso al costado de tan noble y osado emprendimiento como ha sido la Red Elderechoinformático.com.

Quiero aprovechar estas líneas para agradecer a Guillermo la oportunidad que me dio de recorrer este camino de la Red, que confió en mí cuando yo no era más que un pibe más de Santa Fe (que lo sigo siendo) con ganas de aportar y participar. Encontré en Guillermo una gran persona, con la cuál entablamos una amistad que va más allá de la Red, y uno de los genios más creativos, inquietos e innovadores que me ha tocado conocer.

Me despido, pero me llevo muchos amigos y muchos recuerdos buenos... al final de eso se trata no? Un abrazo grande y nos vemos donde el Derecho Informático nos lleve.

Abog. Marcelo Temperini

La necesidad de la protección de datos personales en Nicaragua. Parte 2

En la edición anterior les mencioné que tendríamos la segunda parte de la Protección de Datos Personales en Nicaragua, así que veamos;

FUNDAMENTACIÓN CONSTITUCIONAL

La base legal del acceso a la información pública, tienen su fundamento en la Constitución Política de la República de Nicaragua de 1987, así como las reformas parciales dictadas posteriormente.

Nuestra Carta Magna, en su Artículo 26, estable que: "Toda persona tiene derecho a, su vida privada, y la de su familia. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. Al respeto de su honra y reputación. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber porque y con que finalidad tiene esa información...

De conformidad con el Arto. 66, "Los nicaragüenses tienen derecho, a la información veraz, Este derecho comprende la libertad de buscar, recibir y difundir información e ideas, ya sea de manera oral o escrito, gráficamente o por cualquier otro procedimiento de su elección

De conformidad con el Arto. 67. El Derecho de informar es una responsabilidad, social y se ejerce con estricto respeto a los principios establecidos en la constitución. Este derecho no puede estar sujeto a censura, sino a responsabilidades ulteriores establecidas en la ley.

Por Llc. Jorge O. García
El autor es abogado y notario nicaragüense. Master en derecho empresarial y Maestrante en derecho tributario. University for International Cooperation (UCI) Costa Rica.
jgarcia@obregoncastroasociados.com

Según el Arto. 68,...los nicaragüenses tienen derecho de acceso a los medios de comunicación social y al ejercicio de aclaración cuando sean afectados en sus derechos y garantías.

Transcritas las anteriores normas constitucionales, queda demostrado la necesidad y obligación del estado de introducir el concepto autodeterminación informativa en el ordenamiento jurídico y que este no sólo sea un complemento al esquema de derechos fundamentales del ciudadano, sino que a las garantías adicionales que se requiere para dar al derecho de acceso a la información pública un adecuado contexto de funcionamiento.

Ley 787, Ley de Protección de Datos Personalesi

La referida ley fue publicada en La Gaceta, Diario Oficial del 29 de Marzo del 2012. Cuenta con 56 artículos, divididos en IX capítulos. Los abordaremos someramente sin entrar a fondo en ellos, pues no es el criterio de su servidor transcribirles la normativa sino más bien denotar las particularidades e importancias de la misma.

El Capitulo I aborda generalidades, como objeto y ámbito de aplicación de la norma, entendiéndose que es la protección de datos personales, automatizados o no, de toda persona natural o jurídica, y el manejo de esta información en ficheros públicos o privados. También, encontramos algunos conceptos propios de la materia donde resaltan los siguientes:

-Autodeterminación Informativa: Definiéndolo como el derecho que tiene toda persona a saber ¿quién?, ¿cuándo?, ¿con qué fines? y ¿en qué circunstancias? toman contacto con sus datos personales. A mi criterio este concepto esta muy reducido, pues la normativa lo ha limitado "a saber", cuando en realidad es un derecho fundamental derivado del derecho a la privacidad y por ende el individuo conserva la facultad de ejercer el control total y absoluto sobre su información personal.

-Bloqueo: entendiéndolo como la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

-Consentimiento del titular: Manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales. Este ítem amerita atención primordial, pues en la práctica no es así. Los comercios, bancos, financieras, etc, imponen al consumidor el firmar un formulario, de lo contrario no hay transacción económica. ¿Dónde esta la libre voluntad? ¿Se informa específicamente que es el documento a firmar? Tales presupuestos me despiertan leve sospecha que se estén cumpliendo a cabalidad. Esto demuestra que el camino para lograr una tutela jurídica efectiva, el camino es largo, ¡pero posible! Creo que es una situación de educación a los comerciantes…

-Clasificación de los datos personales: La norma los clasifica en Datos personales (puros y simples):

refiriéndose a la información sobre una persona natural o jurídica que la identifica o la hace identificable. Datos personales informáticos: Son los mismos datos personales pero tratados a través de medios electrónicos o automatizados. Datos personales sensibles: Concernientes a toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación. Datos personales relativos a la salud: sólo pueden ser los relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando el secreto profesional. Datos personales comerciales: son datos sensibles de las Empresas las bases de datos de clientes, proveedores y recursos humanos, para fines de publicidad y cualquier otros datos que se consideren información comercial o empresarial reservada fundamentalmente para el libre ejercicio de sus actividades económicas.

Disociación de datos: Se refiere al mecanismo para el tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada.

Ficheros de datos: Archivos, registros, bases o bancos de datos, públicos y privados, que contienen de manera organizada los datos personales, automatizados o no.

Fuentes de acceso público: Son aquellos ficheros cuya consulta puede ser realizada por cualquier persona, sin más exigencia que, el abono de una contraprestación.

-Responsable de ficheros de datos: Es toda persona natural o jurídica, pública o privada, que conforme Ley decide sobre la finalidad y contenida del tratamiento de los datos personales.

-Tercero: ¿Quién es considerado tercero en materia de protección de datos? Es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos personales, ya sea en ficheros de datos propios o a través de conexión con los mismos.

-Tratamiento de datos: Son las operaciones y procedimientos sistemáticos, automatizados o no, que permiten la recopilación, registro, grabación, conservación, ordenación, almacenamiento, modificación, actualización, evaluación, bloqueo, destrucción, supresión, utilización y cancelación, así como la cesión de datos personales que resulten de comunicaciones, consultas, interconexiones y transferencias.

¿Cómo opera el consentimiento del titular de datos? Cuales son las excepciones?

El titular de los datos deberá por sí o por medio de apoderado dar el consentimiento para la entrega de los datos. Siendo necesario otorgarlo por escrito o por otro medio idóneo, físico o electrónico. Se podrá revocar sin efecto retroactivo. No será necesario el consentimiento cuando: a) Exista orden judicial; b) Los datos personales se sometan a un procedimiento previo de disociación; c) Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; y d) Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento.

De esta pregunta me surge otra más, ¿Como se garantiza la validez de un consentimiento enviado por email? ¿Quién valida que el titular del email sea la misma persona? Con tantas facilidad que encuentras en la red para abrir cuentas comerciales de email (gmail, live, Outlook, yahoo, etc, etc,), pensaríamos que se puede desvirtuar fácilmente la garantía de credibilidad del titular de la cuenta. En otras legislaciones se han dado las soluciones acordes por medio de leyes específicas, pero en lo que respecta a Nicaragua se carece de normativas para este concreto, solo podemos tomar como referencia fiable las opciones que nos brinda la ley de Firma Digital, pero ese es otro tema.

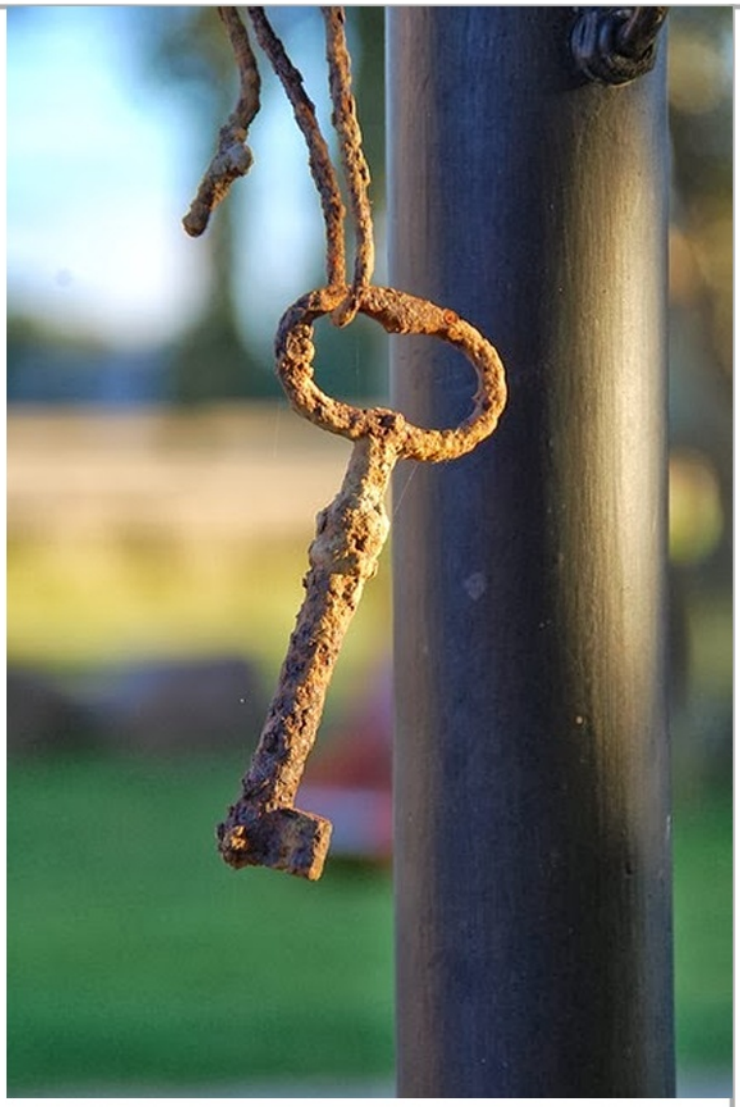
El capitulo II habla de los responsables de los ficheros de datos. Abordando la obligación principal de informar al obtener los datos personales del titular.

Se estipula la obligación de informar previamente a los titulares de datos personales de forma expresa y clara, de los siguientes aspectos: a) La finalidad para la que serán utilizados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del fichero de datos electrónicos o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga; d) Las consecuencias de proporcionar los datos personales, de la negativa a hacerlo o de la inexactitud de los mismos; e) La garantía de ejercer por parte del titular el derecho de acceso, rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales; f) Cuando los datos procedan de fuentes accesibles al público y se utilicen para hacer envíos publicitarios o promocionales, en cada comunicación que se dirija al titular de los mismos se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten; g) Que los datos sólo pueden ser utilizados para los fines que motivaron su tratamiento; y no podrán ser utilizados para otros fines; h) Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados, modificados, suprimidos, completados, incluidos, actualizados o cancelados según corresponda; i) La seguridad en el almacenamiento de datos y el derecho de acceso del titular a los mismos; j) La cancelación de los datos personales una vez que hayan dejado de ser necesarios a los fines para los cuales hubiesen sido tratados; k) Las condiciones técnicas mínimas de tratamiento de datos, tales como técnicas de

integridad, confidencialidad y seguridad; y l) La prohibición de la creación de ficheros de datos personales que almacenen información de datos sensibles.

Con respecto a las medidas de seguridad y confidencialidad en el tratamiento de datos, al igual que en otras legislaciones, el responsable del fichero de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la integridad, confidencialidad y seguridad de los datos personales, y evitar bajo su responsabilidad la adulteración, pérdida, consulta, tratamiento, revelación, transferencia o divulgación no autorizada, detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. En atención a la confidencialidad, las personas que intervengan en cualquier fase del tratamiento de datos personales están obligadas al secreto profesional respecto de los mismos. Subsistiendo aun después de finalizada su relación con el responsable del fichero de datos, pudiendo ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad nacional, defensa nacional, seguridad pública o la salud pública.

Los datos personales se podrán ceder y transferir cuando, previo consentimiento del titular de los datos, al que se le deberá informar sobre la finalidad de la cesión e identificar al cesionario. El consentimiento para la cesión es revocable, mediante notificación por escrito o por cualquier otra vía que se le equipare, según las circunstancias, al responsable del fichero de datos. Este no podrá ser exigido cuando lo disponga una ley, se realice entre instituciones del Estado en el ejercicio de sus atribuciones, se trate de razones de salud pública, de interés social, de seguridad nacional o se hubiere aplicado un procedimiento de disociación de datos, de modo que no se pueda atribuir a una persona determinada.



Será prohibida la cesión y transferencia de datos personales de cualquier tipo con países u organismos internacionales, que no proporcionen niveles de seguridad y protección adecuados. Se exceptúa en los supuestos de colaboración judicial internacional, intercambio de datos personales en materia de salud, cuando sea necesaria para una investigación epidemiológica, transferencias bancarias o bursátiles, conforme la legislación de la materia, cuando la transferencia se hubiere acordado en el marco de tratados internacionales ratificados por el Estado de Nicaragua (como los tratados de intercambio de información tributaria entre México y EEUU) y cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia.

Para la cesión y transferencia de datos personales que se encuentren en ficheros de datos públicos o privados, se hará a solicitud de una persona legalmente autorizada, debiendo detallar el objeto y la finalidad que se persigue con dicha información, asegurando el responsable del fichero de datos cumplir con las medidas de seguridad y confidencialidad de los mismos. Se debe verificar que el solicitante cumpla de igual manera con éstas medidas y sobre todo informar a la persona titular de los datos, la solicitud de transferencia y el propósito que se persigue, para su consentimiento; por ello se deben de tomar las previsiones necesarias para evitar que la información suministrada sea pasada a terceras personas. Toda esta transferencia de datos debe de contar con el aval de la Dirección de Protección de Datos Personales.

¿Qué es el derecho de olvido digital? La ley faculta que el titular de los datos pueda solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros. En los casos de ficheros de datos de instituciones públicas y privadas que ofrecen bienes y servicios y que por razones contractuales recopilan datos personales una vez terminada la relación contractual, el titular de los mismos puede solicitar que se suprima y cancele toda la información personal que se registró mientras era usuario de un servicio o comprador de un bien. Esto dará lugar a reclamos administrativos y judiciales, según sea el caso, contra de algunos monstruos, como google, facebook, youtube, etc, etc

Los derechos del titular de datos, se encuentras contenidos en el capitulo III. Sobresaliendo el Derecho a solicitar información, pues el titular podrá en todo momento solicitar información a la Dirección de Protección de Datos Personales, relativa a la existencia de archivos de él en de ficheros de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

También podrán solicitar que se le permita rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar sus datos personales y se podrán abstener de proporcionar datos personales de carácter sensible, pero como explique anteriormente, esto no se está cumpliendo a cabalidad, sobre todo en información financiera.

¿Cómo modifica el titular sus datos? Anteriormente se explicó que el titular podía solicitar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales, que estén incluidos en un fichero de datos. Pues, los datos de carácter personal, explicamos, se deben cancelar cuando dejen de ser necesarios o cumplan la finalidad que dio lugar a su tratamiento o cuando el responsable no cumple con la obligación de garantías mínimas. Esto deja abierta la acción de protección de datos consignada en la ley. Si los datos se modifican, también se le notificar al cesionario, en caso de cesión, para se cancele el tratamiento correspondiente. Cuando se siga un procedimiento de verificación y rectificación del error o falsedad de los datos personales que conciernen al titular, el responsable del fichero de datos debe bloquear los datos materia de la solicitud o consignar al proveer la información relativa que se tramita un procedimiento con determinado objeto. El obligado se puede negar a la rectificación ó modificación, según sea el caso, cuando exista una resolución judicial que determine la no modificación.

Con respecto a los ficheros y responsables de ficheros de datos personales, contemplados en el capitulo IV, es necesario aclarar que los responsables de estos deben inscribirse en el Registro de ficheros de datos que posee la Dirección de Protección de Datos Personales y esperar en el plazo de ley la resolución de su inscripción.

El registro de ficheros de datos debe recabar la siguiente información: a) Nombre y domicilio del responsable, entendiéndose como persona natural o jurídica con toda la descripción de la razón social, fecha de

constitución, objeto y representante legal; b) Naturaleza de los datos personales contenidos en cada fichero de datos; c) Forma, tiempo y lugar de recolección y actualización de datos; d) Destino de los datos y personas naturales o jurídicas a las que pueden ser transmitidos; e) Modo de interrelacionar la información registrada; f) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar nombre y domicilio de las personas que intervienen en la colecta y tratamiento de los datos; g) Tiempo de conservación de los datos; y h) Forma y procedimientos en que las personas pueden acceder a los ficheros de datos personales para realizar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los mismos según concierna. En los ficheros ninguna persona podrá poseer datos personales de naturaleza distinta a los declarados, cualquier modificación a la información contenida en los ficheros de datos personales debe ser comunicada por el responsable a la Dirección de Datos Personales.

Los ficheros de datos destinados al envío de publicidad, promociones, ofertas y venta directa de productos, bienes y servicios u otras actividades análogas sólo pueden incorporar datos personales con el consentimiento del titular de los mismos, cuando ésta los ha facilitado, o cuando los datos obren en fuentes accesibles al público. Este es uno de lo más polémicos bancos de datos de las personas, debido al irregular uso que se da hoy en día, saturando de marketing a las personas, tanto en la red como fuera de ella.

El envió de publicidad y promociones, a través de medios electrónicos (sms, email, redes sociales) debe de ser normado, existiendo la posibilidad para el destinatario de expresar su negativa a recibir spot publicitarios y promocionales de bienes y servicios o, en su caso, revocar su consentimiento de una forma clara y gratuita.

Es imperante mencionar que las empresas o instituciones que se dedican a actividades de marketing, envíos publicitarios y promocionales electrónicos deberán protegerse mediante un contrato que establezca que los datos personales que figuran en un fichero de datos han sido obtenidos con el consentimiento inequívoco e informado de los titulares o que estos han sido obtenidos de fuentes de acceso público. Se exceptúan las encuestas de opinión; investigaciones científicas o médicas, y a las actividades análogas, pero sólo serán cedidos previo consentimiento del titular.

El órgano regulador de la analizada ley, es la Dirección de protección de datos personales, cuyas facultades se encuentran contenidas en el capitulo V. Esta adscrita al Ministerio de Hacienda y Crédito Público, con una máxima autoridad administrativa, su función principal es el control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada y sus funciones accesorias son:

a) Asesorar a las personas naturales y jurídicas que lo requieran acerca del contenido y alcance de la presente Ley. Facultad, que a mí criterio, hay que observarla detenidamente pues en un proceso administrativo puede verse afectada de parcialidad, por ser Juez y parte. Aunque la Dirección, se aleja de mí criterio, considero que en caso concreto sería oportuno un pronunciamiento de la máxima instancia que aclare esta situación.

b) Dictar las normas y disposiciones administrativas necesarias para la realización de su objeto en el ámbito de su competencia. Quedando siempre a salvo la vía administrativa para el agraviado que se considere que se esta violentando algún derecho particular.

c) Dictar y vigilar que las normas sobre confidencialidad, integridad y seguridad de los datos personales se respeten y apliquen por los titulares de los ficheros de datos correspondientes.

d) Solicitar la información que requiera para el cumplimiento de su objeto a las entidades públicas y privadas titulares de los ficheros de datos, garantizando en todo caso la seguridad, la integridad y confidencialidad de la información. Dicha forma se regula en el respectivo reglamento.

e) Imponer las sanciones administrativas que correspondan a los infractores, quedando a salvo el recurso vertical.

f) Formular y presentar las denuncias por violaciones a la ley, ante la autoridad correspondiente;

g) Verificar que los ficheros de datos personales tengan los requisitos necesarios para que proceda su inscripción en el registro correspondiente.

h) Acreditar a los inspectores para la supervisión y vigilancia de los responsables de los referidos ficheros.

i) Fomentar y promover modelos de autorregulación, siempre y cuando sea posible, como mecanismo adicional para garantizar el derecho a la autodeterminación informativa de toda persona, estos modelos buscan un valor añadido en su contenido con respecto a lo dispuesto en la ley y el reglamento.

j) Emitir su criterio técnico en todo proyecto de ley y reglamento que pudieran tener incidencia en la validez y garantía del derecho a la autodeterminación informativa.

k) Divulgar el contenido y extensión del derecho a la autodeterminación informativa a la población y al resto de los Poderes e instituciones del Estado; y

l) Cooperar con otras autoridades de protección de datos a nivel internacional para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse el debido auxilio mutuo cuando se requiera; abordó un procedimiento (susceptible de mejora en un reglamento posterior) que consiste en visitas, de verificación y control, mediante las cuales los inspectores, revisan los ficheros de datos con el objetivo de establecer el grado de cumplimiento de las normas regulatorias de esta actividad o de brindar a las autoridades de la Dirección de Protección de Datos Personales mayores elementos de juicio para la adopción de una resolución con afectación a terceros o no.

Por su parte los inspeccionados están obligados a permitir el acceso a los ficheros de datos a los inspectores, facilitar y prestar la colaboración necesaria en la inspección, brindar la información y documentación solicitada, permitir la revisión de los equipos y cualquier otra actividad requerida por el inspector…

Si en la inspección se detectara y comprobara la existencia de infracciones graves o hechos que puedan constituir delitos, el inspector deberá tomar las medidas preventivas necesarias en presencia de la persona con quien se presentó para hacer la inspección y comunicarlo de inmediato a su superior inmediato para que proceda de conformidad a derecho.

¿Qué se considera infracciones?

La ley las clasifica en infracciones leves y graves, entendiendo como leves: tratar datos personales sin el consentimiento expreso ya sea por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos de su titular, cuanto la ley así lo exija; omitir la inclusión, complementación, rectificación, actualización, supresión o bloqueo, cancelación, de oficio o a petición del titular, de los datos personales que se encuentran en ficheros de datos públicos y privados; incumplir las instrucciones dictadas por la Dirección; obtener datos personales a través de formularios u otros impresos, sin que figure en los mismos, en forma claramente legible, las advertencias que se utilizarán para crear ficheros; y remitir publicidad a través de medios electrónicos, a titulares que han manifestado expresamente su negativa a recibirla.

Como graves se entiende el tratamiento de datos personales por medios fraudulentos o que infrinjan la ley; impedir u obstaculizar el ejercicio del derecho a

a autodeterminación informativa al titular de los datos personales, así como negar injustificadamente la información solicitada; violentar el secreto profesional; reincidir en las infracciones leves; mantener ficheros de datos, inmuebles, equipos o herramientas sin las condiciones mínimas de seguridad, integridad y confidencialidad requeridas; y obstruir las inspecciones que realice la Dirección.

Pero ¿Que tipo de sanciones se pueden imponer?

En materia administrativa operan el apercibimiento, suspensión de las operaciones relacionadas con el tratamiento de los datos personales y clausura o cancelación de los ficheros de datos personales de manera temporal o definitiva.

Es conveniente aclarar que siempre queda abierta la vía civil y penal para el titular de datos afectado por el actuar del responsable de ficheros de datos.

¿Qué es la acción de protección de datos?

Es cuando el titular de los datos busca la tutela jurídica ante el órgano administrativo, interponiendo la acción de protección de datos personales en esta sede. Se presenta ante la Dirección de Protección de Datos Personales, quien debe de conocer y resolver la denuncia presentada por el titular.

Esta particular acción procede para conocer de los datos personales que han sido objeto de tratamiento en ficheros de datos. Cuando se violenten las garantías de confidencialidad, integridad y seguridad en el tratamiento de los datos personales. En los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata. Para exigir su rectificación, actualización, modificación, inclusión, supresión o cancelación.

Cuando sean lesionados algunos de los principios que rigen la calidad del tratamiento de datos personales, en el ámbito público y privado. Para acceder a información que se encuentre en poder de cualquier entidad pública y privada de la que generen, produzcan, procesen o posean, información personal, en expedientes, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier documento que la administración pública o las entidades privadas tengan en su poder. Por último, para exigir la rectificación, actualización, modificación, inclusión, complementación, supresión, bloqueo o cancelación de datos personales tratados en ficheros de datos de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros, ya sea de forma manual, mecánica o informática, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate.

La Legitimación activa podrá ser ejercida por el titular, sus tutores y los sucesores de las personas naturales, por sí o por intermedio de un apoderado. Cuando la acción sea ejercida por personas jurídicas, deberá ser interpuesta por sus representantes legales o apoderados que éstas designen al efecto. La Legitimación pasiva procede respecto de los responsables y usuarios de los ficheros de datos personales públicos y privados.

Agotada la vía administrativa, mediante resolución emitida por la Dirección de Protección de Datos Personales, el titular de los datos puede hacer uso de la vía jurisdiccional, a través de Recurso de Amparo respectivo.

El reglamento de la ley ya fue publicado en Octubre del año pasado y aclaró las reglas del juego, estableciendo la dinámica de regulación que la ley calló.

Autor: Lic. Jorge García

Análisis comparativo del fallo del TJUE en el caso "Costeja Gonzalez" y el caso "Belén Rodríguez"

Por Abog. Javier Fernandez Moore

Luego de una charla brindada a raíz del fallo Costeja en España y el caso belén Rodríguez en Argentina, me permito sintetizar algunas reflexiones, basado en lo que dicen -u omiten- las propias sentencias. Las diferencias entre los casos son las siguientes:

En el caso "Rodríguez" se pidió: I. La reparación de los daños por : a) el uso comercial no autorizado de su imagen; b) la lesión de sus derechos personalísimos al honor, el nombre, la imagen y la intimidad, por haber sido vinculados e incluidos sus datos y su imagen en páginas de Internet de contenido sexual, erótico o pornográfico; II. Que se condenara a la Google y Yahoo: a) al cese del uso de su nombre y su imagen; b) a la eliminación de las vinculaciones de su nombre, imagen y fotografías con sitios de contenido sexual, erótico y pornográfico.

En el caso "Costeja": a) La Agencia Española de Protección de Datos ordenó a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a los mismos; b) Apelada la resolución ante la Audiencia Nacional, lo elevó en consulta el TJUE para que se pronuncie sobre la interpretación de los arts 2, letras b) y d), 4, apart 1, letras a) y c), 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24/10/1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la "Carta").

Lo que pretendía Costeja era que se obligara al periódico "La Vanguardia" a eliminar o modificar una publicación para que no apareciesen sus datos personales en dos avisos de subasta de un inmueble de su propiedad publicados el 19 de enero y del 9 de marzo de 1998, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Solicitaba también que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. Costeja afirmaba que el embargo al que se vio sometido estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente. La AEPD desestimó el reclamo contra La Vanguardia, al considerar que la publicación estaba legalmente justificada (lo había ordenado el Ministerio de Trabajo y Asuntos Sociales).

Así, tenemos claras diferencias en los presupuestos de fundabilidad de las demandas: mientras en el caso Rodríguez se invocó la ilicitud de los actos de las demandadas (violación a la intimidad y al honor) con apoyo en las normas de

responsabilidad del Código Civil (objetiva para la demandante, subjetiva según la sentencia de Cámara) y 31 de la ley de 11723 de propiedad intelectual (uso no autorizado de la imagen); en el caso "Costeja" se decidió el "retiro" de los vínculos no por la ilicitud del contenido (de hecho, se rechazó la demanda contra "La Vanguardia") sino por interpretación de la la Directiva sobre tratamiento de los datos.

En ese sentido, el TJUE declaró que "Los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que: "el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona,también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita".

Dijo también el Tribunal que "Se tendrá que examinar si el interesado tiene derecho a que la información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre sin que sea necesario que esa inclusión cause un perjuicio al interesado..." y que éste "puede, por derechos que le reconocen los arts 7 y 8 de la Carta, solicitar que la información ya no se ponga a disposición del público mediante su inclusión en tal lista de resultados. Tal derecho prevalece, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona".

Finalmente, el TJUE señaló que ese derecho cedería "...si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate".

Para llegar a esas conclusiones, el Tribunal declaró que el artículo 2, letras b) y d), de la Directiva 95/46/CE (24/101995), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que: "la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática almacenarla temporalmente y, ponerla a disposición de los internautas según un orden de preferencia determinado debe calificarse de "tratamiento de datos personales" y que "el gestor de un motor de búsqueda debe considerarse "responsable" de dicho tratamiento."

La pregunta sería: ¿son aplicables esas conclusiones bajo nuestra ley de protección de datos personales? ¿La aplicará la Corte Suprema "ex-oficio" a los casos pendientes?

CONCLUSIONES:

Si las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudican a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados (art. 19, CN), la libertad de expresión garantizada por otros Tratados de igual jerarquia a los que la Nación Argentina adhirió no puede ser el escudo de irresponsabilidad en el que se resguarden los que violan el derecho a la intimidad. No es cierto que el derecho a la intimidad y el de la libre expresión se encuentren en conflicto, de manera que uno excluya al otro. Por el contrario, la manera de asegurar la vigencia de ambos en el estado de derecho es admitir que su tensión los complementa, evitando el punto de ruptura.-

Autor: Dr. Javier Fernandez Moore

LOS SERVICIOS CLOUD Y SU ADAPTACIÓN A LA LEY ESPAÑOLA

La tecnología cloud ofrece servicios de computación a través de la Red. La reducción de costes, el acceso universal y remoto desde cualquier dispositivo o lugar, la flexibilidad y los indudables beneficios para el medio ambiente son las grandes ventajas que reporta el cloud computing. Los discos duros online, por ejemplo, están revolucionando la manera en la que guardamos la información y el modo de acceder a ella. Las legislaciones nacionales tratan de adaptarse a esta nueva realidad. En el presente artículo, nos centramos en el caso de España y damos recomendaciones a los usuarios, a la hora de elegir servicios que se acomoden plenamente a la ley de protección de datos de nuestro país.

LolaBits, Dropbox, Google Drive, SkyDrive, OpenDrive o Spider Oak son algunos de los discos duros online más populares. Todas ellas son plataformas basadas en el cloud computing, una tecnología que ha logrado prescindir de los soportes físicos, como instrumentos para el almacenaje de la información. Gracias a este nuevo sistema, Internet se ha convertido en el mayor depósito de datos del mundo, un lugar en el que se guarda información de millones de personas.

Esa ingente cantidad de contenidos personales en la nube hace necesaria la acomodación de estos servicios a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

¿Qué debemos tener en cuenta antes de contratar un disco duro virtual o cualquier otro servicio cloud?, ¿qué medidas de seguridad son exigibles?,¿cuáles son nuestras obligaciones como

Marta Robles, Departamento de Lolabits.

clientes?, ¿qué criterios debemos exigir al proveedor de cloud computing?, ¿es relevante la ubicación de los datos personales almacenados?. A éstas y a otras muchas cuestiones trata de dar respuesta la Guía para Clientes que Contraten Servicios de Cloud Computing, editada recientemente por la Agencia Española de Protección de Datos.

En primer lugar, hemos de tener presente que, si residimos en España, la legislación que se nos aplica, a nosotros y a los proveedores de los servicios cloud, es la LOPD y su reglamento de desarrollo (RLOPD, aprobado por R.D. 1720/2007). Ello, con independencia del país en el que se encuentre la empresa servidora o los archivos que ésta nos guarda. Es así, porque el responsable del tratamiento de la información es el cliente que contrata. Dicha responsabilidad no se desplaza al encargado del tratamiento (el prestador de los servicios en la nube).

Antes de elegir nuestro proveedor, debemos analizar y evaluar las características de los datos que manejamos y el grado de sensibilidad que éstos poseen.

Por supuesto, hemos de informarnos sobre los servicios que nos ofrecen y las garantías que los protegen. Hemos de estudiar con detenimiento los distintos tipos de nube (privada, pública o híbrida), para conocer la que mejor se adecue a nuestras necesidades. Con toda esa información en la mano, estaremos en disposición de saber para qué datos contrataremos el servicio y cuáles mantendremos almacenados en nuestros discos físicos.

Una vez seleccionados los datos a almacenar en la nube y la empresa servidora, hemos de solicitar a ésta información en torno a posibles terceros que intervengan en la relación. De existir, tenemos el derecho a conocerlos y a dar nuestro consentimiento a la participación. Por su parte, el proveedor debe responsabilizarse de que los subcontratistas dispongan de garantías jurídicas para el tratamiento de los datos, equivalentes a las que él mismo ofrece.

La localización del almacén de nuestra información en la nube no es una cuestión baladí, tiene su trascendencia. Si se halla en alguno de los estados del Espacio Económico Europeo (Unión Europea, Islandia, Liechtenstein y Noruega), no se precisan garantías jurídicas complementarias, porque las de estas áreas son suficientes y, además, no existe una transferencia internacional de datos propiamente dicha.

Otra cosa es que los ficheros se guarden en países ajenos al E.E.E. En este caso, sí estamos ante una transferencia internacional de datos y son precisas ciertas garantías jurídicas, que varían en función del estado de que se trate. Se consideran garantías adecuadas las que ofrecen una protección equivalente a las del Espacio Económico Europeo y las de empresas estadounidenses que han suscrito el principio de Puerto Seguro. Si no se dan tales requisitos, es necesaria una autorización de la Agencia Española de Protección de Datos.

En cuanto a las medidas a exigir a nuestro proveedor, hemos de preguntarle sobre el nivel de seguridad que nos ofrece. Debemos saber que las garantías varían, en función de la sensibilidad de los datos personales almacenados.

posibles incidencias y las medidas adoptadas para solventarlas.

Por otro lado, los proveedores cloud han de comprometerse a mantener la confidencialidad y a emplear los datos sólo para las actividades contratadas, además de devolverlos al responsable, en el formato acordado, una vez terminado el servicio o extinguido el contrato(portabilidad).

Por último, la empresa proveedora está obligada a articular mecanismos para el borrado automático de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato. Además, aquella ha de cooperar con los clientes, para que éstos, como responsables del tratamiento de los datos, puedan garantizar los derechos de acceso, rectificación, cancelación y oposición a las personas interesadas.

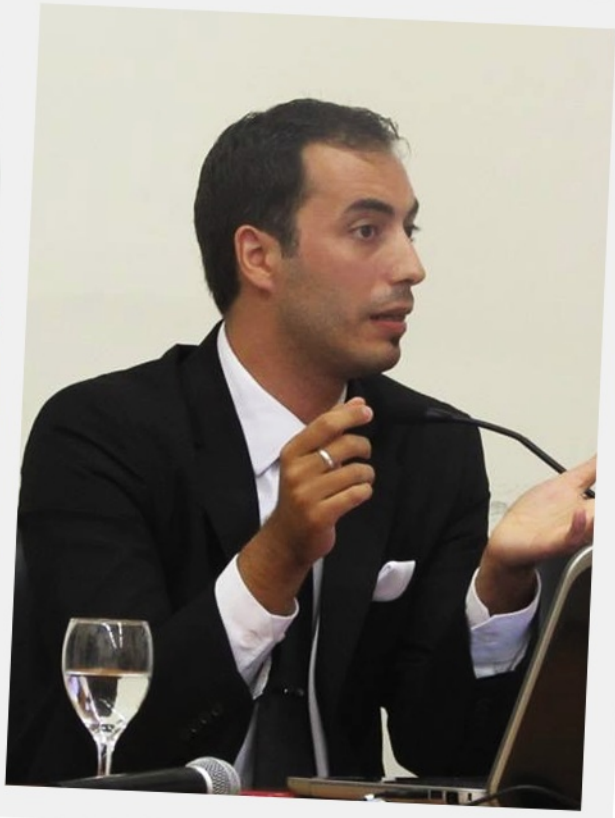
Teniendo presentes todos estos aspectos, los clientes estamos en disposición de contratar, de manera segura, con los proveedores de tecnología cloud que cumplen la legislación vigente. Para una información más completa, se puede consultar la publicación de la Agencia Española de Protección de Datos (http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf)

Autora: Marta Robles

El día 16 de Mayo de 2014, se llevó a cabo el VII Congreso de Derecho Informático, organizado por la Asociación de Derecho Informático de Argentina (ADIAr) y la Facultad de Ciencias Jurídicas y Sociales. El mismo fue realizado en el Aula Mariano Moreno de la FCJS de la Universidad Nacional del Litoral.

Al comenzar la jornada, se realizó la apertura a cargo del Abog. Guillermo Zamora, Presidente de ADIAr, junto al Abog. Alejandro Pivetta, Secretario General de la Facultad de Ciencias Jurídicas y Sociales. A continuación se llevó a cabo el primer panel del Congreso, destinado al Gobierno Electrónico y Gobernanza de Internet, en el cuál participaron la Mag. María Laura Spina (FCJS / UNL), el Dr. Eduardo Parodi (CSJN) y el Dr. Carlos Aguirre (UNC / AGEIA DENSI).

El segundo panel sobre Cibercrimen y Ciberespionaje, estuvo a cargo del Lic. Cristian Borghello (Segu-Info), quien expuso sobre distintos problemas de espionaje que hacen al estado actual de la ciberseguridad. En el mismo panel estuvo el Abog. Marcelo Temperini (UNL / CONICET / AsegurarTe), quien expuso sobre los distintos desafíos que deben asumirse para combatir el Cibercrimen en Argentina.



El tercer panel continuaba con la misma temática planteada, en las que expusieron los Abog. Miguel Sumer Elias (Informática Legal), desarrollando las diferencias entre crimen y delito cuando se habla sobre delitos informáticos. Posteriormente, el Abog. Fernando Barrio (UNRN), quien expuso sobre una visión del ciberespionaje a nivel global y sus distintas consecuencias.

El cuarto panel, dedicado a nuevas monedas digitales, en especial el Bitcoin, estuvo a cargo de la Mag.Corina Iuale (PGI-UNS; GECSI-FCJyS-UNLP), el Abog. Federico Daniel Arrue (PGI-UNS), Diego Bello y Martina Andrea Gutierrez Iuale. Por parte de La Plata, estuvieron la Abog. Noemí Olivera (GECSI-FCJyS-UNLP) y el abog. Gastón Deluchi (GECSI-FCJyS-UNLP), quienes han expuesto sobre los distintos aspectos legales a considerar en las nuevas monedas digitales.

Por último, el Dr. Horacio Fernandez Delpech ha disertado sobre un tema de indiscutible actualidad, como lo es la responsabilidad de los intermediarios en Internet, desarrollando las distintas teorías y posturas que existen sobre la materia.

A modo de cierre, estuvieron presentes el Decano de la FCJS, el Abog. Javier Aga, quien expresó algunas palabras de agradecimiento hacia ADIAr por el éxito del Congreso. Finalmente, el Abog. Guillermo Zamora (ADIAr), entregó una placa de reconocimiento y agradecimiento al decano


DERECHO INFORMÁTICO
#derinfotalle


LOTERIA DE SANTA FE
DERECHO INFORMÁTICO

Posgrado elderechoinformatico.com

POSGRADO DE ESPECIALIZACIÓN EN

DERECHO Informático

Inicio: Todo el año es posible comenzar.

Duración: 16/20 hs por cada Módulo

Módulos:

- Derecho Informático en la Sociedad de la Información
- Protección a las creaciones intelectuales
- Régimen Legal de los sitios web
- Comercio Electrónico - Contexto Latinoamericano
- Informática Forense: Problemática Jurídica de la Prueba Electrónica
- Reciclaje Electrónico, Cloud Computing y Nuevas tecnologías
- Relaciones Laborales y Tecnológicas
- Delitos Informaticos / CRIMES INFORMÁTICOS
- Certificación Digital – Contexto Latinoamericano
- Disputas de Nombres de Dominio y Marcas Registradas
- Protección de Datos Personales
- Gobierno Digital

Dirijido a: Profesionales que acrediten título de grado

Inversión: USD 300 por cada Módulo

Informes: info@elderechoinformatico.com
www.elderechoinformatico.com
www.fcj.unp.edu.ar

Docentes

- Carlos Dionisio Aguirre (Argentina)
- Fernando Barrio (Argentina)
- Horacio Fernandez Delpech (Argentina)
- Heidy Balanta (Colombia)
- Freddy Ossio Onofre (Bolivia)
- German Realpe Delgado (Colombia)
- Carlos Reusser (Chile)
- Laine Souza (Brasil)
- Natalia Enciso (Paraguay)
- Martín Horacio Barrandeguy (Argentina)

Organiza:

RED IBEROAMERICANA
ElDERECHOInformático.com
LA COMUNIDAD DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA

Certifica:

Facultad de Ciencias Jurídicas
UNIVERSIDAD NACIONAL DE LA PATAGONIA
SAN JUAN BOSCO
(Argentina)

DERECHOS HUMANOS, VIGILANCIA EN LAS COMUNICACIONES Y PROTECCIÓN DE DATOS

Romina Florencia Cabrera. Abogada, Investigadora, Docente. UNLP. Miembro del Observatorio Iberoamericano de Protección de Datos y otras instituciones científico-académicas.

Los Derechos Humanos deben estar siempre presentes en la vida jurídica; se basan en respeto a la dignidad y valor de la persona humana, como establece la Convención de Viena. Las Garantías Constitucionales, las llamadas seguridades jurídicas expresadas en la Ley Fundamental, la Carta Magna, ofrecen la real garantía de la libertad y de un estado de derecho, representativo, republicano y federal, como es el caso de nuestro país, Argentina. [1]

El gobierno electrónico, incorporando las Tecnologías de la Información y la Comunicación al procedimiento administrativo; y gobierno abierto, donde la transparencia en la información pública es esencial para promover la participación ciudadana y la confianza del electorado en sus representantes elegidos [2], deben incorporar conceptos de Derechos Humanos, regulados por los Tratados Internacionales. La E- democracia, es el resultado de incorporar la alta tecnología a la implementación de políticas públicas adecuadas con la protección de los derechos de los ciudadanos, como es el caso de la protección de los datos personales, el derecho a la intimidad, a la privacidad , el honor y a la libertad de expresión [3]. En nuestra Ley Fundamental, la ingeniería constitucional utilizada los ubica en el Art. 75 inciso 22, Atribuciones del Congreso, y no en las Declaraciones, Derechos y Garantías. [4]

En el Documento Internacional, suscripto el 10 de julio de 2013, llamado “Principios Internacionales sobre la aplicación de los Derechos Humanos en la vigilancia en las comunicaciones”,

los países firmantes, establecieron: “A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fracasando en garantizar que las leyes y regulaciones relacionadas con la vigilancia de las comunicaciones estén de acuerdo con el derecho internacional de los derechos humanos y protejan adecuadamente los derechos a la privacidad y a la libertad de expresión. Este documento intenta explicar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, particularmente a la luz del aumento de las tecnologías y técnicas de vigilancia de las comunicaciones, y los cambios en ellas. Estos principios pueden proporcionar a los grupos de la sociedad civil, a la industria y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, son consistentes con los derechos humanos.

Estos principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y con expertos internacionales en legislación sobre vigilancia de las comunicaciones, políticas públicas y tecnología”. [5]

Consta de un Preámbulo, donde se establece entre otras cosas que "La privacidad es un derecho humano fundamental y es primordial para el mantenimiento de sociedades democráticas".

Cambio de Tecnología y Definiciones. Los principios: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autoridad judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y sistemas, garantías para la cooperación internacional, garantías contra el acceso ilegítimo.

Describe la aplicación del Derecho Internacional Público en materia de DDHH (Derechos Humanos); el respeto a las Garantías Constitucionales (especialmente en defensa en juicio, como ser los Art. 8 y 9 del Pacto de San José de Costa Rica). La privacidad, intimidad, el honor, y la libertad de expresión quedan protegidos en el ámbito de la comunidad internacional, preservando los valores democráticos y el estado de derecho. Resalto, a mi humilde entender, la autoridad judicial competente, el debido proceso la transparencia y la cooperación internacional, como manera de garantizar las seguridades jurídicas y un equilibrado y razonable coexistir de las herramientas de prevención en materia de seguridad estatal, derecho a la intimidad, privacidad, honor, protección de datos personales (entre ellos los llamados sensibles por su delicada distinción) , el derecho de asociación y la libertad de expresión.

Los datos sensibles, son : "aquellos datos personales que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos. Estos datos están especialmente protegidos:

Los datos sensibles sólo pueden ser tratados cuando medien razones de interés general autorizadas por ley.

Queda prohibida la formación de archivos, registros, bases o bancos de datos que almacenen información que directa o indirectamente revele datos sensibles, salvo que la presente ley o cualquier otra expresamente dispongan lo contrario o medie el consentimiento libre, previo, expreso, informado y por escrito del titular de los datos.

Los datos relativos a antecedentes penales o contravencionales o infracciones administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectiva".[6]

La protección de estas garantías constitucionales y los Derechos Humanos consagrados especialmente en la Ley Fundamental, a través de los Tratados Internacionales suscriptos y ratificados por los Estados Parte, obteniendo jerarquía constitucional superior a las leyes, mientras no menoscaben los principios de la Carta Magna, deben estar por sobre toda norma o medida de carácter preventivo en materia de seguridad . Se debe hacer una aplicación razonable entre el interés público, y los derechos de la ciudadanía.

La protección de Datos debe estar presente en las agendas internacionales, siendo un tema de relevancia actual y especialmente en el futuro, dado la expansión del llamado entorno digital, principalmente del fenómeno Internet y dentro de ella, las llamadas Redes Sociales.

Autora: Abog. Romina Florencia Cabrera

REFERENCIAS:

1-Constitución Nacional, Art. 1: "La Nación Argentina adopta para su gobierno, la forma representativa, republicana federal, según lo establece la presente Constitución".

2-Antonio A. Martino. Ramón Gerónimo Brenna.

3-Observatorio Iberoamericano de Protección de Datos.

4-Giovanni Sartori. Aristóteles..

5-Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de

6- Centro de Protección de Datos Personales. Defensoría del Pueblo de la Ciudad de Buenos Aires. Habeas Data. Revista electrónica del Centro de Protección de Datos Personales.

Jorge Luis García Obregón

Es Licenciado en Derecho egresado de la Universidad Nacional Autónoma de Nicaragua (UNAN). Magister en Derecho Empresarial y Maestrante en Derecho Tributario en la Universidad para la Cooperación Internacional (UCI) de Costa Rica. Ha trabajado como abogado para diversas empresas y consultoras especializadas en Nicaragua y Costa Rica.

1 - ¿Como se definiría como abogado? y ¿como definiría su relación como letrado y el uso de las nuevas tecnologías?.-

Bueno, me definiría como un abogado inquieto, un inconformista de la abogacía tradicional, con una intensa curiosidad en los aspectos económico-legales. Considero que hay que ver más allá de las clásicas instituciones jurídico-romanas que perduran en la mayoría de los ordenamientos positivos vigentes de Latinoamérica, que aún son de gran utilidad, pero debemos entender, incorporar y analizar las figuras legales de otros países a fin de facilitar el intercambio de servicios y bienes dentro un marco de globalización.

Como fruto de mi especialización en Derecho Empresarial y Derecho Tributario en Costa Rica, país con un adelanto tecnológico notable en el istmo centroamericano, pude sentir, vivir y experimentar los nichos de negocios y nuevas oportunidades que se están abriendo para los empresarios y emprendedores en el ámbito informático. No hablo de programas prediseñados que nos venden de los EEUU o Europa, a los cuales se les agrega o mutan ciertas características para tropicalizarlos. No me refiero a la importación de producciones multimedias y audiovisuales. Tampoco me refiero a la representación de empresas extranjeras en el país; como Amazon, Open English, IBM, por decir algunas… Me refiero a ingenieros, empresarios y emprendedores nacionales que han engendrado sus propios productos, creado programas enfocados en satisfacer necesidades nacionales, en primera instancia e internacionalizar su modelo de negocio en un segundo plano. También artistas audiovisuales que han creado obras multimedias de gran valor y las apps que van creciendo en número y adaptándose a la vida cotidiana, entre otras…

Este intercambio de experiencias con el vecino país, me ha hecho interactuar con mis compatriotas nicaragüenses que están iniciando este nuevo y apasionante camino a las empresas informáticas.

Hoy en Nicaragua se ha visto un grupo de nuevos empresarios que están comenzando a estirar sus brazos y trabajar con sus semejantes que desean dar el brinco de la forma tradicional de hacer negocios al 2.0.

Mi relación con el derecho informático en el ámbito de mis especialidades se ha dado en temas de protección de datos, asesoría integral en páginas web, propiedad intelectual, contratos informáticos, por mencionar algunos. No es posible concebir un negocio sin presencia online. La prestación de servicios y venta de bienes se está trasladando a esta esfera ¡ahí esta el negocio!

Producto de esta experiencia y especialización es lo que ofertamos en una empresa de consultoría (www.itaxlegal.com), donde brindamos servicios especializados en temas de derecho de negocios, planificación fiscal y derecho de TICs. El aspecto informático esta presente en la mayor parte de los servicios que brindamos, por ejemplo; los servicios de planificación fiscal que abarcan la utilización de servicios off/shore se hace en el marco legal de la protección de datos; la asesoría empresarial y proyectos emprendedores esta enfocada a empresas que tienen que ver con temas informáticos… Todo en la medida que los proyectos de los clientes nos vayan guiando.

2 - ¿Cual es el estado de situación del derecho informático en Nicaragua?

El avance de esta materia en Nicaragua, no se ha consolidado desde el punto de vista doctrinal, pero sí desde el punto de vista legislativo, cumpliendo los acuerdos de la OMC. Pues, somos un país todavía en vías de desarrollo.

Contamos actualmente con una ley de protección de datos, firma electrónica, una fuerte regulación en materia de radiocomunicaciones y telecomunicaciones y delitos informáticos, ley de acceso a la información, facturación electrónica, impuestos a actividades comerciales relacionadas

con el Internet. Todavía no se entrado de lleno a conflictos sobre dominios y direcciones IP, pero es algo que esta muy cerca, por la creciente demanda de estos servicios.

Una de las cosas que más se reciente por el momento es una ley sobre comercio electrónico, pero a mí parecer esto no impide que se desarrolle la actividad. Al contrario, facilita el poder empezarlas, por ello se debe asesorar delicadamente en este particular, siempre con una tendencia a las legislaciones más predominantes en el mundo.

3 - ¿Como ve la situación del Derecho Informático en Latinoamérica?

Este es un campo muy nuevo para nosotros en Centroamérica pero con cierto camino recorrido en México y Suramérica, ya es notable ver el crecimiento de empresas latinoamericanas en este campo. Ello trae consigo que el derecho como un elemento regulador de las relaciones sociales, vaya creciendo a la medida que la sociedad lo requiera.

Colombia tiene un desarrollo acelerado en este aspecto con empresas como mercadolibre.com, startups, la sede de facebook, google, linkedin y otras que han establecido sedes también en Argentina y Brasil.

Veo que esta creciendo a pasos de gigante. El derecho esta evolucionando con la sociedad por ello, pronto estaremos en una era muy grata para los amantes de este tema y algo molesta para los que se resisten a los cambios.

4 - ¿Cual cree que es el tema en materia de derecho informático que más desarrollo va a tener a corto plazo?

En el caso de Nicaragua, creo que el tema de protección de datos, por que es obligatorio para todas las actividades comerciales que manejen datos sensibles. De las demás guardo mis reservas, pues por ejemplo en la ley de firma digital, no tenemos ninguna empresa que se haya atrevido tan siquiera a explorar el mercado.

En el caso de Centroamérica, creo que el e-commerce pues somos una región que tiende a crecer en las exportaciones. Las pymes que aprovecharán este mercado digital.

Suramérica, no tengo tanto conocimiento del contexto local, pero creo que los delitos informáticos están siendo un elemento de especial cuidado.

5 - ¿El delito informático existe? o se pretende regular un delito existente realizado con una herramienta informática?

No soy penalista. De hecho fue una de las ramas del derecho que poco me atrajo, por ello no te puedo contestar profundamente. Pero considero que el mismo existe con su independencia a las demás conductas atípicas. Pues reúne, a mi criterio, ciertas particularidades.

Es normal que algunos le nieguen la independencia de estas figuras queriendo siempre tenerlas al amparo de otras similares, pero ya hay algunas legislaciones que los tipifican como delitos especiales. Por ejemplo nosotros tenemos la tipificación de la destrucción de registros informáticos, el uso de programas destructivos, ¿Entonces? Creo que son conductas atípicas particulares…

6 - ¿Como visualiza la interacción e interrelación entre las dos ciencias, jurídica e informática?

Las veo completamente compenetradas. La informática es una ciencia como tal y por ello todas las actividades que se realicen en su ámbito deben ser normadas y reguladas. Veamos por ejemplo; la contabilidad y la ley, la contabilidad abarca los impuestos por ello debe tener pautas de normatividad, tener un marco de actuación conforme a la ley.

El mundo esta girando entorno a la informática, por ello tiende a regularse. Tal es el caso de los drones, hoy en día este tema esta siendo abordado muy ampliamente por personas de todo el mundo, debido a los bienes jurídicos tutelados que podrían afectarse con su uso, desde violaciones al derecho de la intimidad, seguridad ciudadana, soberanía, la estabilidad económica desde el punto de vista aduanero, etc, etc. Estoy seguro que el derecho informático cobrará una mayor importancia única en los próximos años.

7 - ¿Que consejos les darías a un empresario que está por comenzar a trabajar con su empresa en la nube?

Antes que nada, como empresario le diría que analice el mercado, que estudié; ¿Qué ofertará? ¿Qué será lo diferente de su negocio online respecto a la competencia? ¿Cómo marcará diferencia? su target de clientes, la estructura de su negocio y su ecosistema empresarial. Junto a ello le daría mi razonamiento legal, de acuerdo a su actividad, tales como; el tema de protección de datos, firma digital, que en base a los servicios que presta escoja una estructura societaria que no ponga en riesgo más de la cuenta, que escoja un régimen fiscal acorde y benefactor a su actividad… entre otros… Cada actividad llevaría una recomendación especifica, ya que hay empresas como un casino online, donde tenés que ver hasta temas relacionados con normativas de cumplimiento de la unidad de análisis financiera ó una empresa de firma digital donde el tema tiene matices mas administrativos y técnicos en cuanto a

en cuanto a registro de software se refiere. Creo que el mejor consejo sería que busque un especialista.

8 - ¿Como ve el trabajo o proyección de los gobiernos en materia de gobierno digital?

Bueno en Nicaragua el tema va lento, hay mucho por hacer…Por ejemplo, la digitalización del registro publico de la propiedad inmueble y mercantil, ha sido un proyecto de muchos años de estarse cocinando, que creo que se ha pasado un poco de fuego. En materia de impuestos va avanzando muy rápido en los últimos años, pues ya se esta orientando hacia una particular tributación online. La exigencia en base a los acuerdos internacionales, es que se avance rápido, pero a veces falta un poco de músculo económico.

Costa Rica, lleva buen camino, su gobierno digital se siente en tributación, municipalidades, registro civil, mercantil, de la propiedad, etc. La tendencia es migrar completamente a esa era digital que todos ansiamos, convertirnos en países con gobiernos digitales y ciudades digitales.

Hay un esfuerzo en conjunto en Centroamérica para avanzar en temas de este tipo, pero situaciones involuntarias e internas han frenado un poco.

9 - ¿Algo que desee agregar?

Creo que las legislaciones centroamericanas, tienen que evolucionar pronto para poder crear un ecosistema idóneo para la fertilidad del derecho informático, pues todavía persiste una tendencia centralista y protectora en cuanto a las existentes instituciones jurídicas. Hay que ceder un poco para tomar ese impulso que le hace falta a las empresas digitales.

Solo en la medida que se pierda ese temor a que ¡en Internet nada es seguro! Podemos ir poco a poco creando esa estabilidad económica. Lo único que detiene el crecer en estas actividades es la falta de condiciones optimas de los estados, pues talento hay y mucho…

Agradecemos la gentileza del Dr. Jorge Luis García Obregon.


Dejamos huellas.
Seguínos.
@elderechoinf
EDI
RED IBEROAMERICANA
ElDERECHOInformático.com
EL PORTAL DE DERECHO INFORMÁTICO MÁS GRANDE DE IBEROAMÉRICA