DECLARACIÓN DE CARTAGENA DE INDIAS - COLOMBIA

2004

III ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS

Los participantes en el III Encuentro Iberoamericano de Protección de Datos, celebrado en Cartagena de Indias (Colombia) durante los días 25 a 28 de mayo de 2004 para reflexionar sobre "La Protección de Datos Personales como garantía de calidad de los servicios: Nuevos retos y oportunidades para los Sectores Financiero, Comercial y de las Telecomunicaciones en Iberoamérica", desean hacer públicas las conclusiones que en el mismo se han alcanzado

Ponen de manifiesto su satisfacción por los desarrollos alcanzados tras el Encuentro de La Antigua (Guatemala), en junio de 2003, que se han concretado en el impulso de diversos proyectos regulatorios en el ámbito de la Protección de Datos Personales y en la consolidación de canales permanentes de colaboración e intercambio de experiencias, documentación y opiniones en materia de protección de datos.

En particular se congratulan de forma especial por el hecho de que los Jefes de Estado y de Gobierno de los países iberoamericanos, reunidos en la XIII Cumbre celebrada en Santa Cruz de la Sierra, Bolivia, los días 14 y 15 de noviembre de 2003 han reconocido de forma expresa la importancia del Derecho Fundamental a la Protección de Datos, al disponer en el punto 45 de la declaración Final de la Cumbre lo siguiente:

- "Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad."

La declaración de Santa Cruz de la Sierra, al reconocer la labor de la Red Iberoamericana de Protección de datos, nos impulsa a redoblar nuestros esfuerzos, en pro del derecho fundamental a la Protección de Datos, por lo que asumimos el compromiso de continuar por la vía ya iniciada, al objeto de conseguir la más amplia implantación posible de la cultura de la Protección de Datos, basada en marcos regulatorios nacionales que, como se señalaba ya en la Declaración de La Antigua, garantice una protección adecuada de este derecho fundamental en todos los países iberoamericanos.

En este sentido, consideran que resulta imprescindible dar a conocer la opinión de la Red a la Comunidad Iberoamericana, en la esperanza de que de esta manera se cuente con un punto de referencia objetivo e imparcial en la implantación efectiva del Derecho fundamental a la Protección de Datos Personales, convencidos de que el mismo influye de forma decisiva en el desarrollo social y económico de los Países Iberoamericanos.

En consecuencia, teniendo en cuenta las ponencias y trabajos presentados y el resultado de los enriquecedores debates mantenidos, hacen públicas las siguientes CONCLUSIONES:

I. LA PROTECCIÓN DE DATOS Y LA PERSPECTIVA DEL SECTOR FINANCIERO

- El tratamiento (1) leal, lícito, transparente y ético de datos personales constituye una garantía de la persona que debe ser respetada en la búsqueda de objetivos como velar por la estabilidad del sistema financiero y facilitar el acceso al crédito. La obtención y uso de información personal para mitigar y administrar los riesgos que implica el otorgamiento de crédito debe ir acompañada del respeto de los derechos de las personas en cuanto al tratamiento de sus datos personales. Una protección efectiva de datos financieros propicia que las personas estén más dispuestas a apoyar el flujo de su información. Para alcanzar estos objetivos es importante la actividad de las centrales de riesgos
- (1) A efectos del presente documento, esta expresión se entenderá como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción, públicas y las Centrales de Información Crediticia (2) privadas (CIC). Estas últimas facilitan a sus usuarios la medición del riesgo crediticio
- En adición a la incorporación de los principios esenciales de protección de datos reconocidos en instrumentos nacionales e internacionales, la regulación sobre protección de datos personales debería prever pautas que reconozcan las particularidades del dato financiero.
- Los desarrollos normativos deberán permitir el flujo de información a los intermediarios financieros para la evaluación de riesgos de su actividad, garantizando el derecho fundamental a la protección de datos personales de forma que exista un equilibrio entre ambos.
- La recolección y circulación de datos financieros de las personas se ha convertido en una herramienta valiosa en la solidez, modernidad y competitividad del sistema financiero.
- En este sentido, las Centrales de Riesgos Públicas (CRP) por su función de garantizar la estabilidad del sistema financiero deben estar habilitadas para el tratamiento de los datos necesarios para cumplir aquella finalidad.
- Las CIC contribuyen a solucionar las asimetrías de información en los mercados de crédito, fomentar una cultura de pago y, en general, al desarrollo de la actividad crediticia sobre bases sanas.
- Tanto los proveedores de servicios financieros como los consumidores obtienen beneficios al operar en un mercado con mayor calidad de información sobre las personas. La información que las CIC transmiten a terceros debe ser confiable y de calidad. Por lo tanto, ésta debe ser veraz, exacta, completa y actualizada.
- Pese a los avances y esfuerzos nacionales e internacionales que se han realizado sobre la materia, continúan presentándose situaciones en las que por diversas razones y circunstancias se ha dado un tratamiento indebido a los datos financieros de las personas. Por eso, todos los actores involucrados en el tratamiento de este tipo de información (las CRP y las CIC así como sus fuentes de información entre otros) deben impulsar y fortalecer medidas para garantizar en todo momento un nivel adecuado de protección de la información de los usuarios del sector financiero. Esto debería ir acompañado de servicios expeditos y efectivos de atención al cliente con miras a respetar sus derechos
- (2) Esta expresión comprende los burós de crédito, las centrales de riesgo, las protectoras de crédito y en general cualquier base de datos privada o empresa que realiza actividades de tratamiento de datos personales para la evaluación de riesgo. de acceso, actualización o rectificación de su información personal, que permiten, además de constituir una garantía para el ciudadano, incrementar la calidad de la información de las bases de datos. Adicionalmente, el fomento de una cultura organizacional de la protección de datos al interior de las CRP y las CIC y sus fuentes de información contribuirá a alcanzar el cometido citado.
- Todo lo anterior no sólo permitirá generar confianza en los ciudadanos respecto del tratamiento de sus datos crediticios sino que constituye un imperativo para respetar las obligaciones legales y éticas en el tratamiento de datos personales.

II. LA LUCHA CONTRA EL "SPAM"

- El creciente desarrollo de las autopistas de la información ha incorporado a la vida cotidiana instrumentos que facilitan la conexión electrónica entre los diferentes ámbitos en los que la persona desarrolla su actividad diaria. Las comunicaciones electrónicas suponen una vía inmediata, rápida y económica de contacto entre los usuarios de las diferentes redes públicas de telecomunicaciones.
- Al abrigo de un instrumento tan útil se ha desarrollado la práctica del envío de comunicaciones electrónicas o mensajes de datos no consentidos ni deseados, popularmente conocidas como "spam". Aunque no existe un concepto doctrinal unívoco para este fenómeno, normalmente se entiende como "spam" el proceso a través del cual se remite información no solicitada ni deseada. La progresión de este fenómeno ha sido exponencial en los últimos años, debido fundamentalmente al bajo coste de los servicios, a la facilidad de captar direcciones electrónicas y a la dificultad de identificar al "spammer" que, usualmente, puede servirse de medios técnicos que le permiten ocultar su verdadera identidad. Ello supone que se haya convertido en un problema global que afecta a la práctica totalidad de los sectores productivos y económicos, amén de bienes jurídicamente tutelables.
- La presencia del "spam" en la vida diaria de los usuarios de las redes públicas de telecomunicaciones ha producido una fuerte reacción contra su uso indiscriminado, dado que incide negativamente en la protección de otros bienes jurídicos y derechos de los usuarios, que son dignos de protección. La intromisión ilegítima que el "spam" realiza en la privacidad, el perjuicio económico que el mismo ocasiona a los ciudadanos y a las empresas, así como el envío a través del mismo de contenidos que en muchos casos resultan engañosos y fraudulentos, hacen que la sociedad exija medidas que combatan la realización de este tipo de prácticas.
- Deben adoptarse medidas técnicas que permitan controlar y establecer filtros al envío de "spam". Estas medidas resultan necesarias, aunque no suficientes para contrarrestar el crecimiento de estas prácticas. En este sentido deberían adoptarse medidas legislativas que disciplinen específicamente la lucha contra el "spam", garantizando los derechos de los usuarios y regulando, en lo que sea necesario, la actividad que desarrollan los diferentes agentes implicados en esta actividad. La colaboración internacional en esta materia permitirá establecer un marco homogéneo, que resulta imprescindible para combatir el "spam", dado el ámbito transnacional del propio fenómeno. Es preciso, además, propiciar e impulsar iniciativas de autorregulación sectorial que complementen y faciliten la aplicación del marco regulatorio sobre la materia.
- Por último, es imprescindible que se adopten medidas que potencien la concienciación de los usuarios en relación con los perjuicios que la práctica del "spam" les genera. De esta manera, los agentes que posibilitan la propagación de "spam" verán dificultada su actividad por una mayor formación de los usuarios, lo que contribuirá a prevenir activamente esta problemática que presenta múltiples interdependencias.

III. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS: PERSPECTIVAS EUROPEAS E IBEROAMERICANAS

- La transferencia internacional de datos personales debe estar sometida a un régimen de garantías para impedir que los principios que rigen el derecho fundamental a la protección de datos se vean vulnerados por el mero traslado de dichos datos a otro país.
- La Directiva de Protección de Datos de la Unión Europea ha consagrado este principio y ha otorgado a la Comisión Europea competencias para decidir que un país que ha establecido una legislación de protección de datos acorde con los estándares europeos y ha creado una autoridad de control independiente es un destino seguro para los datos personales provenientes de Estados miembros de la UE. Este reconocimiento equivale a la plena liberalización de los intercambios de datos personales entre la Unión Europea y el país de que se trate, lo que favorece en gran manera los intercambios comerciales y, específicamente, el desarrollo del comercio electrónico y el desarrollo de los servicios de la Sociedad de la Información.
- En el año 2000 la República Argentina promulgó la Ley Nacional de Protección de Datos Personales N 25.326 que, junto con el Decreto 1.558 del año 2001 que la reglamentó, introdujo un sólido régimen de protección de datos en su Derecho Nacional en el que se incluían todos los principios esenciales por los que debe regirse un tratamiento de datos personales para ser lícito y legítimo: proporcionalidad, finalidad, información al interesado, calidad, especial protección a

ciertas categorías de datos, confidencialidad, seguridad y derechos de acceso, rectificación y supresión para los interesados.

- Asimismo, estableció una autoridad de control independiente (la Dirección Nacional de Protección de Datos Personales) a través de la cual los interesados tienen la posibilidad de hacer valer sus derechos con rapidez y eficacia. Las garantías ofrecidas por este marco legislativo y de control fueron reconocidas por la Comisión Europea al considerar, en su Decisión 2003/490/CE de 30 de junio de 2003, que la legislación argentina ofrecía un nivel de protección de datos adecuado.
- En el caso que no exista este reconocimiento, es posible, entre otras opciones, la utilización de las cláusulas contractuales tipo aprobadas por la Comisión Europea. Su utilización permite establecer las garantías necesarias que suplan la carencia de una legislación adecuada en el país de destino al otorgar a los titulares cuyos datos se transfieren la posibilidad de exigir el cumplimiento de las cláusulas del contrato que les afectan así como una reparación en el caso de que se les causen perjuicios por no respetarse
- Por lo tanto, los participantes en el III Encuentro Iberoamericano de Protección de Datos hacen votos para que en los países iberoamericanos se promulguen regulaciones sobre protección de datos y se establezcan mecanismos de control independientes que promuevan una efectiva implantación del derecho fundamental a la protección de datos personales que, al mismo tiempo, faciliten el libre flujo de datos personales entre los países.

IV. EL SEC TOR DE LAS TELECOMUNICACIONES E INTERNET ANTE LOS ATAQUES DE LA PRIVACIDAD

- El desarrollo de la sociedad de la información ha supuesto la aparición de nuevos productos y servicios de comunicaciones electrónicas que han redundado en una sensible mejora en la capacidad de acceso a la información por parte de los usuarios.
- De este modo, han aparecido en los últimos años servicios de valor añadido o agregado que facilitan la calidad de vida de los ciudadanos y la actividad económica. Al propio tiempo, el crecimiento exponencial de Internet en los últimos diez años posibilita el acceso a una enorme cantidad de información, lo que permite disponer de un mayor conocimiento sobre las más diversas materias, y habilita asimismo la posibilidad de que el usuario pueda intercomunicarse con un número cada vez mayor de personas desde los lugares más remotos.
- El desarrollo de todos estos servicios de la sociedad de la información supone necesariamente el tratamiento de datos de carácter personal, que en ocasiones serán necesarios para lograr el acceso a la información o a los servicios requeridos por parte de los usuarios. No obstante el tratamiento de dichos datos puede generar riesgos para la privacidad de los usuarios y su derecho fundamental a la protección de datos de carácter personal. Estos riesgos se aprecian, en especial, en la utilización de Internet, mediante el uso de dispositivos que inciden directamente en la esfera más íntima del usuario. Igualmente, el tratamiento de los datos de facturación y tráfico de los abonados o usuarios, necesario para la propia realización de las comunicaciones electrónicas, debe someterse a todas las garantías necesarias para que el mismo no incida negativamente en la esfera de la privacidad.
- La realización de estos tratamientos supone un cambio en el marco regulador del derecho a la protección de datos, que debe tener en cuenta no sólo a las personas físicas, sino también, en ciertos supuestos, a las personas jurídicas o morales, así como a informaciones que tradicionalmente no habían sido suficientemente contempladas por las regulaciones nacionales e internacionales en materia de protección de datos de carácter personal.
- Desde el punto de vista de los agentes involucrados en el ámbito de las comunicaciones electrónicas la adopción de medidas que garanticen la utilización segura de las redes y el derecho a la protección de datos de los abonados y usuarios de los servicios reviste una especial importancia, no sólo desde el punto de vista del cumplimiento del marco regulatorio, sino como garantía de su propia imagen y solvencia frente a sus clientes y a la sociedad en general.
- En consecuencia, es preciso el establecimiento de un marco regulatorio que garantice la adecuada implantación de medidas de seguridad en las redes de comunicaciones electrónicas y, lo que resulta esencial, reconozca y enumere expresamente los derechos de los abonados y usuarios en relación con la protección de sus datos personales. Además, sería conveniente que los agentes ofrecieran productos o servicios que garantizasen, siempre que ello fuera posible, el anonimato en el uso de las comunicaciones electrónicas.

- Asimismo, el papel de los diversos agentes involucrados, a través de la adopción de sistemas de autorregulación, complementarios de los ya mencionados marcos regulatorios, así como el establecimiento de un marco internacional homogéneo en la protección de los derechos de los abonados y usuarios de los servicios de comunicaciones electrónicas, resulta también esencial para lograr una garantía integral de esos derechos.

V. EL SECTOR COMERCIAL Y EL USO DE LA INFORMACIÓN CON FINES DE MARKETING

- El marketing es y sigue siendo uno de los retos de la protección de datos personales en la actualidad. El desarrollo de esta área refleja los déficits que son constatables en los estándares de la protección de datos a nivel global. Para cambiar esto ayudaría mucho el establecimiento de marcos reguladores en esta materia que garanticen a las personas el uso adecuado de sus datos con fines de publicidad y de marketing, así como de autoridades de control que tutelen sus derechos.
- La evolución del marketing ha demostrado que la etapa actual se orienta a la generación de cada vez mejores servicios de valor agregado o añadido que pueden al mismo tiempo generar graves lesiones al derecho de protección de datos. Entre esos riesgos destaca la producción de perfiles de consumo a partir de la comparación e integración de diversos tipos de datos, ofrecidos de las más diversas fuentes sin transparencia e información para la persona. Frente al hecho descrito, surgió como reacción por parte de las personas el uso de técnicas de autoprotección como lo fue el resistirse a hacer uso del comercio electrónico, lo que tiene graves consecuencias económicas. Los problemas aumentan si se toma en cuenta la dificultad para distinguir entre los medios directamente relacionados con la red y los nuevos medios de comunicación por medio de telefonía que acceden también a servicios en línea.
- Para una protección adecuada de los datos personales en el ámbito del marketing podemos resaltar la necesidad de emplear herramientas de anonimización del usuario para usos ajenos a la gestión interna de los productos o servicios que la empresa ofrece, junto al consentimiento informado; transparencia y capacidad de decisión; los sellos de autenticidad y de calidad que puedan ir unidos a un proceso de auditaje informático de la calidad de los servicios prestados por una determinada empresa, a practicar de manera proactiva la protección de datos y especialmente el principio de proporcionalidad; así como la utilización de políticas de privacidad por las propias empresas que ofrecen los servicios.
- Resulta evidente que hoy el sector comercial y dentro de él el marketing es uno de los más necesitados de desarrollos normativos así como de la elaboración de códigos tipo o de conducta. Estos códigos tienen el carácter de códigos deontológicos o de buenas prácticas y constituyen un instrumento propicio para potenciar el adecuado tratamiento de los datos personales, complementando o desarrollando los marcos regulatorios existentes .
- Es propio de la naturaleza de los códigos tipo o de conducta el contribuir a la correcta aplicación del marco regulador general sobre protección de datos personales existente a las singularidades del sector correspondiente; asimismo es recomendable que se dé publicidad de los mismos para el conocimiento general, así como someterse a examen de las autoridades de control. Con todo lo señalado se evidenciaría el ajuste de los códigos referidos a las normas de protección de datos personales, asignándoles con ello un valor agregado o añadido de garantía, calidad y confianza, sin perjuicio de las obligaciones establecidas en la normativa vigente en materia de protección de datos.
- Dentro de la sociedad de la información y comercio electrónico, las comunicaciones comerciales o promocionales deberán cumplir con ciertos requisitos para enmarcarse dentro de un tratamiento adecuado de los datos personales. Dentro de estos, podemos mencionar el dejar constancia de la finalidad comercial de los mismos y la indicación de la persona física o jurídica en nombre de la cual se realiza el envío. La tendencia moderna parece enfocarse a propuestas "opt in" basadas en el previo consentimiento del usuario de los servicios.
- Otro factor indispensable dentro de las comunicaciones comerciales o promocionales es el dejar a salvo la posibilidad de la revocación del consentimiento en el momento que el titular de los datos considere oportuno. Cobra especial importancia en este punto el derecho de oposición, previa petición y sin gastos, al tratamiento de los datos que conciernen a su titular, en cuyo caso deberán ser dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.
- Dentro del sector comercial y el uso de la información con fines de marketing el marco jurídico de protección de datos personales, constituye y debe seguir siéndolo el marco dentro del cual se

incremente la seguridad de la información, la racionalización de recursos y el aumento de la confianza de los clientes a través de un tratamiento adecuado de sus datos.

VI. CONSIDERACIONES EN TORNO AL DESARROLLO DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

- Fruto de la Declaración de la Antigua, como corolario de los supuestos que la animaron tras la celebración del II Encuentro Iberoamericano de Protección de Datos, los participantes acordaron constituir la Red Iberoamericana de Protección de Datos
- La Red se creó así como un foro abierto a la incorporación de todos los países iberoamericanos, con el propósito de potenciar las iniciativas de intercambio de experiencias entre ellos y de reforzar su mutua y continua colaboración en materia de protección de datos.
- La coordinación de la Red se defirió a una Presidencia y una Secretaría Permanente, que transitoriamente se encargaron a la Agencia Española de Protección de Datos, con el propósito de adoptar una decisión al respecto durante la celebración de este III Encuentro.
- El compromiso asumido en la Declaración de La Antigua fue ratificado al más alto nivel por los Jefes de Estado y de Gobierno Iberoamericanos durante la celebración de la XIII Cumbre Iberoamericana celebrada en Santa Cruz de la Sierra (Bolivia), los días 14 y 15 de noviembre de 2003. En efecto, en el párrafo 45 de la Declaración de Santa Cruz de La Sierra, los participantes subrayan su reconocimiento de que la protección de datos personales es un derecho fundamental de las personas y destacan la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se creaba la Red Iberoamericana de Protección de Datos, abierta a todos los países de esta Comunidad.
- Este reconocimiento explícito e inequívoco constituye un importante apoyo al trabajo de colaboración mutua de la Red y a todas las iniciativas normativas sobre las que se está trabajando actualmente. Constituye, además, un impulso decisivo para la elaboración de nuevos proyectos que garanticen este derecho en Iberoamérica.
- En esta fase inicial, la Red Iberoamericana de Protección de Datos se ha caracterizado más porado másG una misi fundamentalmente informativa, una actividad común que ha sido en gran medida útil para conocer las realidades normativas de cada uno de los países y los problemas y desafíos que se nos plantean en materia de protección de datos de carácter personal, como se destacaba en la Declaración de Santa Cruz de la Sierra.
- Sin embargo, los cometidos de la Red, según su acta de constitución y el impulso ofrecido por la Cumbre de Jefes de Estado y de Gobierno, pueden ser mucho más ambiciosos, por lo que su estructura debe trascender a un estadio proactivo, que permita plasmar las iniciativas en realizaciones más concretas.
- Partiendo de esta idea, las reflexiones manifestadas en este III Encuentro han llevado a la adopción de las siguientes medidas en torno a la Red, más acordes con la importancia que la Cumbre le ha reconocido, y que se concretan en los siguientes nuevos cometidos y decisiones estratégicas:
    - a) Creación de subgrupos de trabajo, abiertos a la incorporación de los miembros de la Red que estén interesados. Durante el III Encuentro se han constituido los subgrupos para el estudio analítico de las siguientes materias:
        - Gobierno electrónico y telecomunicaciones, a iniciativa de la representación de Chile, que ejercerá su comunicación.
        - Accceso a la información pública y protección de datos, a iniciativa de la representación de México, que ejercerá así mismo su coordinación, habiendo manifestado ya su intención de participar los representantes de Costa Rica y del Perú.
        - Estrategia de la Red, a iniciativa de la representación de Colombia, coordinado por la representación de la Agencia Española de Protección de Datos. En este grupo han mostrado ya su intención de participar las representaciones de Costa Rica y El Salvador.
        - Viabilidad de creación de Autoridades de Control en el entorno iberoamericano, a iniciativa de El Salvador y coordinado por la representación de Argentina.

- Actualización periódica sobre los desarrollos normativos nacionales, incluyendo también las principales decisiones judiciales pertinentes y publicación de las ponencias y conclusiones del Encuentro en la página web de la Agencia Española de Protección de Datos, en la sección dedicada a la Red Iberoamericana.
- Constitución de una Secretaria "pro tempore" para la organización de los siguientes Encuentros, constituida por la Agencia Española de Protección de Datos y una representación de los países sede del encuentro a organizar y del anterior.
- Comenzar la preparación del IV Encuentro Iberoamericano de Protección de Datos, para cuya celebración los representantes de Costa Rica proponen este país como sede para 2005. La preparación se encarga a la Secretaría "pro tempore" que esta ocasión está constituida por la Agencia Española de Protección de Datos y la representaciones de Costa Rica y Colombia.
- Se acordó que la Secretaría de la Red y la Presidencia se mantengan durante los dos próximos años en la Agencia Española de Protección de Datos y se aprobó el siguiente logotipo para la Red.