RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

GOBIERNO ELECTRÓNICO Y TELECOMUNICACIONES

INDICE

I. INTRODUCCIÓN

La Sociedad de la Información y del Conocimiento está produciendo profundos cambios en el mundo. Esta transformación está impulsada principalmente por la aparición de nuevos medios disponibles para crear y divulgar información y conocimiento mediante las tecnologías de la información y la comunicación (en adelante TIC). Así, progresivamente han surgido nuevas formas de organización social y productiva, y una nueva cultura. Han cambiado las formas de comunicarse, de trabajar, de constituir nuestras organizaciones y comunidades. Todos asistimos a este proceso de globalización en el que se contraen los conceptos de espacio y tiempo y caen las fronteras, pero vivimos estas transformaciones de distintas maneras según sea el desarrollo económico, el tipo de inserción, la cultura, las fortalezas y las debilidades de las instituciones de las distintas comunidades nacionales. Para todos nuestros países resulta de gran importancia determinar cómo puede este paradigma contribuir al logro de objetivos de desarrollo más amplio que incluya un crecimiento económico sustentable, mayores grados de equidad y profundización democrática, y cómo también propicia la cabal integración de la Región en la sociedad mundial de la información.

Avanzar hacia una sociedad de la información que beneficie a todos los habitantes de la Región, junto con fomentar el desarrollo de los objetivos arriba indicados, requiere de un diálogo permanente para adoptar una agenda que acelere el proceso y reduzca los costos económicos y sociales. De este modo, es necesario diseñar estrategias para el desarrollo de la sociedad de la información que superen las fronteras nacionales y que hagan que la cooperación entre los países sea indispensable.

Atendida la similitud de los desafíos en materia de TICs y de protección de datos tenemos una oportunidad para adoptar medidas concertadas para potenciar las estrategias nacionales encaminadas a acelerar el proceso y contribuir a un desarrollo orientado a la cohesión social y a la inclusión.

En este marco abordaremos temas tales como el gobierno electrónico, el tratamiento de las informaciones personales en los servicios de telecomunicaciones y, en particular, fenómenos relativamente recientes como el "*spam*".

En este contexto, las garantías vinculadas al derecho fundamental a la protección de datos personales ante el uso de las tecnologías adquieren una enorme relevancia y llevan a la necesidad de procurar alternativas que permitan evitar la vulneración de este derecho, dadas las múltiples formas en que se puede hacer uso de las informaciones de los ciudadanos.

El concepto de seguridad ha alcanzado gran relevancia y se le ubica junto al de finalidad y consentimiento. Es así que como un apropiado grado de seguridad -comprensivo de políticas, protocolos procedimentales y planes de contingencia- coadyuva para lograr los grados de fiabilidad que contribuirán a favorecer los emprendimientos de gobierno electrónico y a un adecuado respeto a la protección de los datos personales en el sector de las telecomunicaciones.

II. GOBIERNO ELECTRÓNICO

Una de las definiciones que nos parece consistente acerca de todos los aspectos que contempla el gobierno electrónico es la que lo identifica como: "El uso de las tecnologías de información y comunicaciones (TIC) que realizan los órganos de la administración para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público, así como la participación de los ciudadanos".

La implantación del gobierno electrónico se desarrolla gradualmente y transcurre en un proceso que se diferencia en cuatro fases identificadas como: presencial; informacional; interactiva y transaccional.

Un buen desarrollo de gobierno electrónico permite avanzar en una triple finalidad, a saber: atención al ciudadano, buen gobierno y de desarrollo de la democracia. Estos ámbitos pueden analizarse de la siguiente manera:

La atención al ciudadano considera el establecimiento de nuevas formas de relación gobierno-ciudadanos-empresa-inversionista, mediante el uso de las tecnologías de la información y comunicaciones, que permitan al Estado brindar sus servicios en forma eficiente, eficaz y con independencia del lugar físico.

En buen gobierno se busca el establecimiento e introducción de nuevas formas y procesos internos en la Administración del Estado, que permitan la integración de los sistemas de los diferentes servicios, compartir recursos y mejorar la gestión interna de los mismos.

En cuanto al desarrollo de la democracia se considera la creación de mecanismos que, usando las tecnologías de la información y comunicaciones, permitan al ciudadano jugar un rol proactivo en el quehacer del país, permitiendo abrir nuevos espacios y formas de participación.

La importancia de las finalidades descritas y la circunstancia que el Estado se relaciona con todos los ciudadanos hace necesario promover proyectos de gobierno electrónico por cuanto estas iniciativas tienen un efecto catalizador y promotor de la economía digital y de la sociedad de la información.

Por otra parte, los ámbitos ya referidos -atención al ciudadano, buen gobierno, desarrollo de la democracia- tienen como condición elementos normativos, organizativos y tecnológicos.

Es así como toda incorporación de TIC debe hacer sentido a un proyecto estratégico que considere los aspectos jurídicos y tecnológicos, en una perspectiva interdisciplinaria, con el objeto de facilitar su implementación y promover una cultura de la seguridad.

La existencia de un marco normativo previamente definido se precisa para habilitar y dar garantías, dentro de los parámetros de la neutralidad tecnológica, al inicio de los procesos citados.

Atendidos los procesos de modernización y los avances alcanzados en materia de gobierno electrónico se va haciendo cada vez más necesario compartir información dentro del ámbito de las administraciones públicas, y desarrollar la interoperabilidad que permite evitar requerimientos reiterados de información a los ciudadanos tratando la información ya disponible de carácter no reservado, siempre dentro de las facultades y competencias de las instituciones públicas. El acceso a la información debe tener restricciones específicas para el caso de los datos sensibles, lo que será definido según las condiciones de cada país. Al respecto debe reafirmarse que el derecho fundamental a la protección de datos, exige que la administración pública actúe de manera acorde con las garantías propias del Estado de Derecho.

Como exigencias tecnológicas cabe destacar el problema de la identificación y autenticación de los ciudadanos, donde es útil el desarrollo de sistemas que promuevan, con garantías adecuadas, la incorporación de servicios tales como la firma electrónica. Además es necesario que se produzcan políticas que fijen directrices generales sobre seguridad, y confidencialidad de la información, lo que

incluye garantía del suministro eléctrico, adecuada ubicación de equipos y sistemas, el control de accesos que permita auditar que el servicio responde a las finalidades habilitadas, así como buenas prácticas para evitar riesgos, respaldo de información periódica, selección adecuada de contraseñas y privilegios de acceso, y planes de contingencias y de recuperación en caso de desastres.

La confianza es un elemento indispensable para garantizar el éxito de este tipo de proyectos, ya que en doble vía permite que haya uso de las herramientas dispuestas y, al mismo tiempo, estimula que el ciudadano continúe aceptando y usando proactivamente dichos servicios. En este sentido, ha de resaltarse el impulso a la educación y la capacitación y reiterarse las exigencias sobre seguridad y protección de los datos personales.

Asimismo, el tema de la cultura de los funcionarios incide en el éxito de estos proyectos, provocando un cambio en los servicios, donde se administra la información de una forma diferente.

Es necesario considerar en el diseño e implementación de los proyectos de gobierno electrónico la adecuada información al ciudadano sobre el alcance y las finalidades de estas iniciativas.

III. TELECOMUNICACIONES

Los servicios de telecomunicaciones constituyen un ámbito específico para la protección de los datos personales por dos razones, principalmente: La primera, porque las crecientes interoperatividad y extensión de estos servicios constituyen, por sí mismas, un factor de riesgo para la seguridad de la gestión de la información, en general, y de los datos relacionados con la intimidad, en particular. La segunda, porque el proceso de telecomunicación requiere determinar e identificar los puntos de terminación de la red entre los que se produce la comunicación que, por su eventual identificación con personas pueden alcanzar la consideración de datos personales.

La Declaración de Cartagena de Indias, con ocasión del III Encuentro Iberoamericano de Protección de Datos advirtió sobre los riesgos existentes respecto del tratamiento de los datos personales y la privacidad en el sector de las telecomunicaciones, incluyendo una enumeración de aquellos.

La Declaración presupone la necesidad de adaptar garantías que equilibren el tratamiento de datos personales en los servicios de comunicaciones electrónicas

disponibles al público con el respeto al derecho fundamental del individuo al tratamiento de sus datos personales.

La delimitación de estas garantías debe partir de un concepto básico como es el de la neutralidad tecnológica que trae ínsito el hecho de que estas garantías pueden resultar efectivas con independencia de las tecnologías utilizadas.

Los datos de tráfico relativos a los abonados que son tratados en las redes de comunicación electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas y los intereses legítimos de las personas jurídicas.

En particular, esta información puede ser tratada para elaborar perfiles de abonados y usuarios dirigidos a la promoción comercial de dichos servicios, tanto para la definición de los mismos como para la realización de acciones publicitarias. Asimismo, puede ser utilizada para la prestación de servicios con valor añadido, la cual se produce en ocasiones incluso con exigencia de una contraprestación, sin mediar el consentimiento informado del usuario.

Una situación similar se plantea respecto del tratamiento de los datos de localización que proporcionan información sobre la ubicación física del equipo terminal.

El adecuado equilibrio en el tratamiento de los datos de tráfico y localización para finalidades distintas de las relacionadas con la prestación de los servicios de comunicaciones electrónicas ha de requerir la obtención de un consentimiento previo e informado por parte de los abonados sobre los tratamientos que van a realizarse y sobre su finalidad específica. Esta exigencia debe reiterarse, particularmente, respecto de la prestación de servicios con valor añadido.

La introducción de facturas desglosadas permite que el abonado pueda comprobar las tarifas aplicadas pero, también, puede afectar a la intimidad de los usuarios de servicios de telecomunicaciones. Por ello deben fomentarse modalidades de pago alternativas que garanticen la privacidad y la posibilidad de optar por facturas en las que se omitan algunas cifras del número llamado.

Los servicios avanzados de telefonía en redes digitales ofrecen la posibilidad de identificar la línea desde la que se llama y la línea conectada. Para proteger a los interlocutores de la comunicación resulta aconsejable permitir la no identificación de la línea desde la que se efectúa las llamadas y rechazar las llamadas

procedentes de líneas no identificadas. Estas exclusiones no deberían de ser operativas cuando afecten a la seguridad pública o a los servicios de emergencias.

Las guías de abonados a servicios de comunicaciones electrónicas alcanzan gran difusión y tienen carácter público. El derecho a la intimidad de las personas físicas exige que puedan decidir sobre si sus datos han de figurar o no en dichas guías, así como sobre la inclusión en ellas de más datos de los necesarios para su identificación como abonados o sobre la utilización de las guías para usos distintos de esta finalidad.

Ante la frecuente utilización de los datos de las guías con fines de publicidad o de promoción comercial los abonados han de tener la opción de que se incluya en las guías una marca indicativa que excluya dicho uso.

El desarrollo de los servicios de comunicaciones electrónicas y de la sociedad de la información se apoya entre otros aspectos en la existencia de medidas de seguridad efectivas. Por ello los proveedores de servicios deberían adoptar las medidas necesarias para salvaguardar la seguridad e informar gratuitamente a los abonados y usuarios de los riesgos particulares existentes y de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones.

Finalmente, un fenómeno cada vez más frecuente es el de la instalación de dispositivos en los equipos terminales que permiten el almacenamiento y la recuperación de la información sin el conocimiento del usuario.

Los usuarios han de tener derecho a conocer la instalación de tales dispositivos y a que se les ofrezca un procedimiento sencillo y gratuito para proceder a su desactivación, excepto en aquellos casos en que sean necesarios para la prestación de los servicios.

IV. SPAM

El desarrollo tecnológico ha ampliado extraordinariamente la posibilidad de efectuar comunicaciones comerciales no solicitadas a través de llamadores automáticos, faxes y mensajes de correo electrónico incluidos los “*sms*”.

Algunas de estas modalidades como la remisión de comunicaciones comerciales no solicitadas a través de medios electrónicos (“*spam*”) han alcanzado proporciones inquietantes dado su carácter masivo.

El "*spam*" constituye un problema desde el punto de vista del individuo porque, además de suponer una intromisión en su intimidad, puede inducir a error o engaño, o responder a una voluntad de estafar. También implica una ocupación de su tiempo y gastos adicionales si se ve en la necesidad de adquirir programas de filtrado u otros programas.

Igualmente implica costes considerables para las empresas, tanto directos (reducción del rendimiento y de la productividad de los empleados e inversiones en tiempo y dinero para paliar el problema) como indirectos (falsos positivos, difusión de virus). Para los proveedores de servicios en Internet (ISP) y de servicios de correo electrónico (ESP) puede suponer la necesidad de adquirir más ancho de banda y mayor capacidad de almacenamiento.

Por otra parte, el "*spam*" es una actividad de tan bajo coste, que su rentabilidad es muy alta, máxime en los casos ("*phishing*" u otros) en los que se puede producir un fraude.

Finalmente el "*spam*" ha adquirido dimensiones globales y requiere respuestas a nivel internacional.

Por todo ello, el "*spam*" puede socavar la confianza de los usuarios, condición indispensable para el avance del comercio electrónico de la sociedad de la información en su conjunto.

Para hacer frente a este fenómeno ha de considerarse un amplio abanico de medidas normativas, técnicas, de sensibilización y de cooperación internacional.

En el ámbito normativo surge como primera cuestión a considerar la de alcanzar una definición homogénea del "*spam*" por cuanto la concurrencia de acepciones diversas dificultará la eficacia del resto de medidas y especialmente, la cooperación internacional.

En este sentido, la licitud o ilicitud del "*spam*" debería estar vinculada a la exigencia del consentimiento informado del usuario, bien en forma de consentimiento previo (*opt in*) bien, al menos, como posibilidad de oponerse a su recepción (*opt out*).

Asimismo, es relevante considerar que existe "*spam*" ilícito cuando no se ofrece un procedimiento efectivo para oponerse a la recepción de correo basura o "*spam*".

Las normas deberían prever sanciones adecuadas a la gravedad del fenómeno incluida la posibilidad del bloqueo de los sitios WEB implicados, facilitar los mecanismos de denuncia del *spam* y procedimientos de reparación de los daños originados. Para ello debería atribuirse competencias para su aplicación a autoridades específicas y elaborarse instrumentos legales efectivos. En este sentido, resulta procedente estimular mecanismos extrajudiciales alternativos para la resolución de conflictos.

Las soluciones técnicas para acabar con el "*spam*" pueden comprender el bloqueo de mensajes procedentes de servidores identificados como fuente del mismo y el empleo de programas de filtrado, por los usuarios en el propio equipo terminal y, por los prestadores de los servicios de comunicación electrónica en sus propios servidores.

En este ámbito debe prestarse especial atención a los servidores que funcionan en el modo abierto y a los "*proxy*" abiertos, que pueden ser utilizados para retransmitir mensajes que son enviados por los "*spammers*", por lo que deberían preverse exigencias para que adopten medidas de seguridad que lo eviten.

Sin embargo, las técnicas de filtrado pueden plantear problemas relacionados con el bloqueo de correos electrónicos importantes (falsos positivos) o con el no bloqueo de "*spam*" (falsos negativos) que pueden dar lugar a litigios judiciales. Por ello deberían adaptarse las condiciones de los contratos de abono para que los ISP/ESP y los proveedores de servicios móviles ofrezcan a sus clientes información sobre opciones de filtrado y cláusulas relativas a la prohibición de enviar correo no solicitado.

Las medidas de sensibilización y educativas son esenciales para que los ciudadanos adquieran el debido conocimiento de los riesgos que les puede ocasionar el "*spam*" y las medidas para evitarlo.

El tratamiento eficaz de las denuncias transfronterizas es uno de los elementos esenciales para hacer posible la protección de los usuarios lo que hace imprescindible la cooperación internacional.

Esta cooperación debería abarcar dos objetivos: uno, promover una normativa eficaz en los países de la región y, dos, cooperar entre las autoridades competentes para garantizar que las normas aprobadas se apliquen adecuadamente.

V. CONCLUSIONES

Finalmente, para impulsar el desarrollo del gobierno electrónico y de los sistemas de protección de datos personales en las telecomunicaciones proponemos la generación de una instancia de encuentro en el sitio WEB definido en el documento de estrategia de la RED, que permita conocer y aplicar buenas prácticas de gestión e identificar sistemáticamente experiencias relevantes que se difundan y permitan su replicabilidad y el aprendizaje conjunto.

Los componentes de esta iniciativa deberían incluir, entre otros, un banco de casos replicables, productos de gobierno electrónico (sitios WEB, servicios en línea, etc.), comparaciones de *bench marking* y bibliografía.

Huixquilucan (Estado de México), 4 de noviembre de 2005