DERECHO A LA INTIMIDAD EN LA SOCIEDAD DE LA INFORMACION

Ley Nº 18.331: impacto y reglamentación

Dra. Esc. María José Viega[(*)]

1. Derecho a la intimidad

Desde un punto de vista jurídico el derecho a la intimidad es el derecho a la reserva de la vida privada. En ese sentido dice la Declaración Universal del Derechos Humanos de 1948 que "Nadie será objeto de injerencias arbitrarias en su vida privada…" y que "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

El concepto inicial de intimidad evolucionó en un sentido positivo, afirmándose la "privacy" como un presupuesto del ejercicio de otros derechos de proyección social e incluso económica.

La privacidad es un tema que puede ser enfocado desde múltiples ópticas, desde el cruzamiento de ficheros en soporte papel y de ficheros electrónicos, la privacidad desde la óptica del consumidor y de las telecomunicaciones (sean por cable o inalámbricas) y por supuesto, no podemos dejar de considerar nuestros datos personales en el ámbito de Internet.

La manipulación informatizada de los datos da origen a la llamada "libertad informática", la cual aparece como un nuevo derecho de autotutela de la propia identidad informática, o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscriptos en un programa electrónico[1].

En este sentido, a Internet se la ha calificado como una amenaza en la difusión de elementos relativos a la persona, por ser un medio masivo y polifacético de comunicación. Tal es así, que se han analizado en otra oportunidad[2] las diferentes clases de comunicaciones a través de la Red y las han comparado con las comunicaciones "tradicionales", estudiando similitudes y diferencias con la correspondencia privada, la prensa escrita y la radiodifusión.

(*) **Directora de Derechos Ciudadanos de la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC)**. Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UR). Profesora de Informática Jurídica, Derecho Informático y Derecho Telemático en la Facultad de Derecho de dicha Universidad. Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro de la International Technology Law Association. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro del Instituto de Derecho Informático (UDELAR) y Coordinadora de su Grupo de Jurisprudencia. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

[1] ALTMARK Daniel y OLINA QUIROGA Eduardo. "Régimen jurídico de los bancos de datos", en Informática y Derecho (Depalma, Buenos Aires, 1998), vol. 6, página 146.

[2] VIEGA, María José. "Derechos Humanos en el Ciberespacio". Trabajo publicado en la Revista electrónica de Derecho Informático (REDI), Junio de 2002.

Para reflexionar sobre este tema es interesante respondernos las siguientes preguntas[3]: ¿hay alguien escuchando nuestras llamadas telefónicas?, ¿qué tan seguro es enviar un fax?, ¿alguien lee nuestros e-mails? ¿y nuestro chat?, ¿es posible que alguien recupere a través del proveedor de Internet lo que escribimos hace unos meses?, ¿es realmente importante la privacidad para cada uno de nosotros?

En los hechos, la mayor parte de las personas ceden sus datos a cambio de puntos, millas, etc. sin tener conciencia que nos estamos identificando, que estamos dando información sobre nuestros hábitos, consumo, en definitiva sobre nosotros mismos y no conocemos la utilización posterior que se dará a esos datos.

Ahora bien, ¿"alguien" nos espía?

Según el diccionario espía es una persona que con disimulo y secreto observa o escucha lo que pasa, para comunicarlo al que tiene interés en saberlo.

¿Quienes nos espían?, por ejemplo, a través de Internet.

Se suele responder que nos espía el gobierno, las empresas, los ciberdelincuentes.

¿Para qué nos espían?

Depende de la respuesta que demos a la pregunta anterior serán los motivos. Los gobiernos en aras de la seguridad nacional. Las empresas buscan crear perfiles de usuarios a los efectos de ofrecernos productos que sean de nuestro interés, lo que tendrá como resultado el spam. También existe el espionaje entre empresas, el cual podemos enmarcarlo en el ámbito de la competencia desleal. Y finalmente los ciberdelincuentes, quienes obviamente desean obtener nuestros datos para obtener un beneficio, normalmente económico, con su utilización.

¿Cómo nos espían?

"En el pasado, si el Gobierno quería violar la privacidad de los ciudadanos tenía que dedicar una cierta cantidad de esfuerzo para interceptar, abrir al vapor y leer el correo de papel. Esto es similar a pescar con una caña, un pez cada vez. Afortunadamente para la libertad, esta vigilancia que requiere tanto esfuerzo no es práctica a gran escala. Hoy en día, el e-mail está reemplazando al correo convencional y, a diferencia de éste, los mensajes electrónicos son facilísimos de interceptar y escudriñar buscando palabras clave. Esto se puede llevar a cabo de manera rutinaria, automática, indetectable y a gran escala. Es similar a la pesca con red de arrastre, lo que constituye una diferencia orweliana para la salud de la democracia"[4].

George Orwell escribió una novela en el año 1948 de ciencia ficción titulada "1984" en la cual nos presenta el mundo del futuro dividido en tres estados totalitarios. El protagonista es el símbolo de la rebelión contra el poder de un estado policíaco (bajo el control del Gran Hermano) que ha llegado a apoderarse de la vida y la conciencia de

[3] VIEGA, María José. "Privacidad & Espionaje en Internet". Derecho Informático. Tomo VI. Fundación de Cultura Universitaria. Página 237.

[4] ZIMMERMANN, autor del paquete criptográfico PGP, citado por García Mostazo Nacho en "Libertad Vigilada. El espionaje de las comunicaciones". Ediciones B. Barcelona, 2003.

todos sus súbditos, interviniendo en las esferas más íntimas de los sentimientos humanos[5].

Podemos decir entonces que, debido a la amplia difusión de las tecnologías de la información y las comunicaciones, el tratamiento de los datos personales se encuentra en una situación de tensión. Esta deriva del valor asociado a las bases de datos personales y el derecho de las personas titulares de los datos a conocer el tratamiento al que están siendo sometidos sus datos personales y preservar su privacidad.

2. Ley Nº 18.331 de Protección de Datos Personales y Habeas Data

La doctrina ha elaborado una serie de principios para regular este nuevo derecho que se han ido consagrando en los diferentes textos positivos en los diferentes países.

En nuestro país, la Agencia para el desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) impulsó el anteproyecto de ley de protección de datos personales, con el objetivo de establecer un marco jurídico claro y necesario para garantizar y hacer efectivo uno de los derechos fundamentales del ser humano, como es el derecho a la protección de los datos de carácter personal y por tanto de la intimidad de las personas, lo que culminó con la aprobación de la Ley Nº 18.331 de 11 de agosto de 2008.

El fundamento del mismo está dado por el artículo 72 de la Constitución de la República que establece: "*La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno*".

Como característica fundamental del proyecto debemos señalar que el mismo incluye a todos los datos personales, ya que hasta ahora los mismos eran protegidos en base al tríptico jusnaturalista recogido en los artículos 7, 72 y 332 de la Constitución. Uruguay contaba con protección específica únicamente para los datos destinados a brindar informes comerciales, regulados por la ley Nº 17.838 del 24 de setiembre de 2004, la cual quedó derogada por la ley Nº 18.331, aunque mantiene el mismo régimen para esta clase de datos.

Por otra parte, se consagra la Acción de Habeas Data, como instrumento y garantía procesal de defensa de los derechos a la libertad informática. El procedimiento propuesto incorpora modificaciones al régimen que establecía la ley Nº 17.838.

Otro aspecto relevante que aborda el proyecto es la vinculación con terceros países, procurando cumplir con los requisitos establecidos por la Unión Europea a los efectos de obtener la Declaración de Adecuación a la Directiva Nº 95/46/CE, trámite que se inició a fines del 2008 ante la Comisión Europea, estando en este momento esperando el informe que realizará la Universidad de Namur sobre nuestra normativa.

En este punto, se han tenido presente los elementos de cumplimiento necesarios a ese fin, que son: asegurar un nivel satisfactorio de cumplimiento de las normas, la posibilidad de ofrecer apoyo y asistencia a los interesados en el ejercicio de sus

[5] ORWN George. 1984. Ediciones Destino. Barcelona. Séptima edición, junio 1984.

derechos, ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas, tanto en vía administrativa (ante el organismo de control) como en vía jurisdiccional (acción de habeas data).

El aspecto anterior tiene consecuencias económicas importantes, basado en que la adecuación a las políticas de intercambio de datos con la Unión Europea permitiría la captación de inversiones en el sector tecnológico y de servicios, de hecho así lo han manifestado diferentes actores privados que apoyaron la iniciativa del Poder Ejecutivo.

La ley creó como órgano de control la Unidad Reguladora y de Control de Datos Personales (URCDP) como organismo desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión electrónica y de la Sociedad de la Información y del Conocimiento (AGESIC).

La URCDP está dirigida por un Consejo Ejecutivo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

Este Consejo asegura la independencia técnica en la materia, teniendo como función principal la toma de decisiones en todo lo concerniente a la protección de datos personales. En la última Ley de Rendición de Cuentas se aprobó la estructura básica la Unidad la cual ha comenzado a operar, recibiendo consultas de ciudadanos y responsables de las bases de datos, trabajando en la elaboración de un sitio web y en el sistema informático que permita la preinscripción on line.

El Consejo Ejecutivo de la URCDP funcionará asistido por un Consejo Consultivo, que estará integrado por 5 integrantes: una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser un legislador en actividad; un representante del Poder Judicial; un representante del Ministerio Público; un representante del área académica; y un representante del sector privado, que se elegirá en la forma establecida reglamentariamente.

3. Decreto Nº 664/008 de 22 de diciembre de 2008

Por Decreto Nº 664/008 de 22 de diciembre de 2008 se creó el Registro de Bases de Datos Personales a cargo de la URCDP.

En el artículo 2º dispuso el traslado del Registro de Bases de Datos Personales, creado por Decreto Nº 399/2006 de 30 de octubre de 2006, que funcionaba en el ámbito del Ministerio de Economía y Finanzas al nuevo Registro creado en la URCDP.

El Decreto establece las condiciones de inscripción, la información y documentación que deberán presentar los responsables de las bases de datos comerciales y el procedimiento para realizar la misma. A tales efectos, se puede solicitar el formulario que se está utilizando en forma provisoria – estando en etapa de implementación el sistema informático-, personalmente o por correo electrónico.

4. Conclusiones

La aprobación de la Ley Nº 18.331 tiene importantes repercusiones, entre las que destacamos:

a) la existencia de un marco regulatorio general en materia de protección de datos personales;

b) la creación de la URCDP como organismo que viabilice y otorgue garantías en cuanto a la efectiva aplicación de la norma;

c) la existencia de un proceso de Habeas Data sumarísimo con alcance general; y

d) la posibilidad de obtener la declaración de adecuación a la normativa de la Unión Europea, fundamental para el intercambio internacional de datos personales.

Por último, quiero destacar que la URCDP se encuentra funcionando provisoriamente en la calle Andes 1365 piso 7. Los ciudadanos y responsables de las bases de datos pueden realizar consultas personalmente, en forma telefónica al 901 2929 interno 1352 en el horario de 10 a 18 y en breve a través del sitio web www.protecciondedatos.gub.uy.

Montevideo, marzo de 2009