34° Conferencia Internacional de Autoridades de PROTECCIÓN DE DATOS Y PRIVACIDAD

Privacidad y tecnología en equilibrio

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

PRÓLOGO

Cuando –en oportunidad de la 33° Conferencia realizada en la ciudad de México– Uruguay fue designado como Sede de la 34° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad a efectuarse en el año 2012, surgió de manera inmediata la necesidad de constituir un Comité Académico a los efectos de preparar el programa de la Sesión Abierta de la Conferencia.

Esta responsabilidad fue asignada a la Gerencia de Derechos Ciudadanos de la Agencia para el Desarrollo de Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC), la que cumplió la tarea directamente con el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP).

En este marco, con una fuerte formación en derecho informático y con la impronta y experiencia de la AGESIC, la URCDP decidió que el eje temático fuera "Privacidad y tecnología en equilibrio".

El Comité realizó investigaciones temáticas, exposiciones y mesas de trabajo sobre los distintos temas que, finalmente, conformaron el programa de la Conferencia.

A un año del evento, queremos hacerles llegar el trabajo realizado, el cual –enriquecido con los videos y relatorías publicados en el sitio web de la 34° Conferencia – esperamos constituyan una herramienta enriquecedora en el quehacer diario de todos los actores de la protección de datos personales.

Prof. Dra. Esc. María José Viega
Gerente Derechos Ciudadanos
AGESIC

Prof. Dr. Felipe Rotondo Tornaría
Presidente del Consejo Ejecutivo
URCDP

PRIVACIDAD Y TECNOLOGÍA EN EQUILIBRIO
ÍNDICE

PRÓLOGO

CAPÍTULO I. DERECHOS FUNDAMENTALES. Dr. Marcelo Bauzá

1. Introducción
- 1.1. Caracterización de los Derechos Fundamentales
- 1.2. La "estimativa jusnaturalista" en la Constitución uruguaya
- 1.3. La Sociedad de la Información y los DD.HH.

2. Protección de datos personales y DD.HH.
- 2.1. Un movimiento constante y sin retroceso
- 2.2. Algunos rasgos típicos de este derecho
- 2.3. Situación de Uruguay hasta el año 2004
- 2.4. La Ley Nº 18.331 y su enfoque jus-humanista
- 2.5. Coexistencia entre Derechos Fundamentales

3. La aprobación del Convenio Nº 108
- 3.1. Un hito en la materia
- 3.2. Aspectos esenciales de este Tratado

4. Conclusiones

CAPÍTULO II. SOCIEDAD DE LA INFORMACIÓN. Dr. Ramiro Prieto

1. Consideraciones preliminares sobre Sociedad de la información
- 1. a. Introducción
- 1. b. Conceptualización, origen y evolución del Fenómeno
- 1. c. Importancia
- 2. Desarrollo del fenómeno Sociedad de la Información en Latinoamérica y Europa

2. Sociedad de la Información en Europa
- 2.1. a. Desarrollo de la Sociedad de la Información en Europa y el surgimiento de la Agenda Digital Europea
- 2.1. b. El plan avanza en España: Un modelo exitoso de política de Sociedad de la Información
- 2.2. Sociedad de la Información en Latinoamérica
- 2.2. a. Aspectos más relevantes de la evolución de la Sociedad de la Información en Chile y en Colombia
- 2.2. b. El caso de Uruguay: Agenda Digital 2011-2015

3. Sociedad de la Información en la actualidad y su vínculo con la protección de Datos Personales
- 3.1. Marco Normativo en Europa y Latinoamérica
- 3.2. Nuevos Desafíos de Protección de Datos Personales de ante los avances en las TIC. Casos de BigData

4. Conclusiones

CAPÍTULO III. GOBIERNO ELECTRÓNICO. Dr. Federico Abbadie

1. **Introducción**
2. **Gobierno Electrónico y Protección de Datos Personales en Uruguay**
3. **Nociones y alcance del e-gov, sus rasgos esenciales y la relación directa con la Administración Electrónica, las TIC y el Big Data**
4. **Desafíos de las Administraciones Publicas en las políticas del Gobierno Electrónico**
5. **Necesariedad de una interconexión en los sistemas de información y su relacionamiento directo con la protección de datos personales como la preservación de un derecho fundamental**
6. **Maximización en la eficacia de los cometidos estatales y el rol del Servidor Público en el Gobierno Electrónico, dentro un contexto de democratización e integración electrónica**
7. **Proyecciones y expectativas del e-gov en las regiones con potencial crecimiento socio - económico y el especial desafío de la satisfacción y protección de sus habitantes**
8. **Reflexiones finales**

CAPÍTULO IV. CONSENTIMIENTO INFORMADO: ¿REGLA O EXCEPCIÓN?. Dr. Felipe Rotondo

1. **Introducción**
2. **Sistemas en la materia: opt out y opt in**
3. **Caracterización del consentimiento**
   - 3.1. Libre
   - 3.2. Previo al tratamiento de datos
   - 3.3. Debidamente informado
   - 3.4. Inequívoco
4. **Continuación: otros aspectos relativos al consentimiento**
   - 4.1. Medios
   - 4.2. Procedencia
   - 4.3. Responsabilidad de su requerimiento
   - 4.4. Prueba
   - 4.5. Revocabilidad
   - 4.6. Validez por tiempo determinado
   - 4.7. Tratamiento sin consentimiento
5. **Exenciones del consentimiento**
6. **Cuestiones específicas**
   - 6.1. Datos sensibles
   - 6.2. Datos de incapaces
   - 6.3. Geolocalización en dispositivos móviles inteligentes
   - 6.4. Publicidad comportamental
7. **Normativa y dictámenes de la Unión Europea: mención**

CAPÍTULO V. GOBIERNO ABIERTO. Dra. Laura Nahabetián Brunet

1. **Introducción**
2. **Un paso previo ...**
3. **Conceptualizando realidades**
4. **De la participación de la sociedad civil**
5. **Del gobierno electrónico al gobierno abierto**
6. **Gobierno abierto**
   - 6.1. Un poco de historia
   - 6.2. Hacia la construcción del gobierno abierto
   - 6.3. Principales beneficios
   - 6.4. Características fundamentales
7. **Datos abiertos**
8. **Otro elemento a no perder de vista**
   - 8.1. Open Source Governance y Wiki Government
   - 8.2. Open Politics
9. **¿Apertura del gobierno o apertura de mentes?**

CAPÍTULO VI. SMART DATA. Dra. Silvana Casciotti

1. **Introducción**
2. **Concepto**
   - 2.1. Smart Metering o Medidor Inteligente
3. **Problemas que presenta para la privacidad**
4. **Smart metering y Privacy by Design**
5. **Proyecto de George Tomko**
6. **Conclusiones**

CAPÍTULO VII. BIOMETRIA. Dr. Marcelo Bauzá

1. **Conceptos técnicos preliminares**
   - 1.1. Definición y consecuencia jurídica
   - 1.2. Clases y especies de datos biométricos
   - 1.3. Propiedades de los datos tratados biométricamente
   - 1.4. Fases de un procedimiento biométrico y resultados posibles
2. **Los principios jurídicos aplicables**
   - 2.1. La aplicación del régimen general
   - 2.2. El principio de licitud
   - 2.3. El principio de necesidad
   - 2.4. El principio de dignidad
   - 2.5. El principio de proporcionalidad
   - 2.6. El principio de finalidad
   - 2.7. El principio de seguridad
3. **Experiencias traídas a comentario durante la 34ª Conferencia**
   - 3.1. Cuestiones tratadas
   - 3.2. El reconocimiento facial en redes sociales

3.3. La inversión en este campo y sus beneficiarios
3.4. Experiencia de México
3.5. Experiencia de Uruguay
3.6. Intervenciones a pedido del público

CAPÍTULO VIII. E – SALUD. Dra. Flavia Baladán

1. **Introducción**
   1.1. Introducción a la E-Salud
   1.2. Salud 2.0
   1.3. Salud 3.0
   1.4. Salud en dispositivos móviles
   1.5. Sistemas de tarjeta sanitaria electrónica
   1.6. Historia clínica electrónica
2. **La seguridad en la E – Salud**
3. **El ejercicio de los derechos**
4. **La E – Salud en los casos de emergencia**
5. **La E – Salud y las transferencias internacionales**
6. **E – Salud y Gobierno Electrónico**
7. **Conclusiones**

CAPÍTULO IX. HERRAMIENTAS FORENSES. Dra. Rosario Ierardo

1. **Introducción**
2. **Definición de e- Discovery**
3. **Leading case Da Silva Moore vs Publicis Groupe**
   3.1. Funcionamiento de la Predicción por Codificación (predective coding) y el Reconocimiento óptico de Caracteres (OCR)
4. **Proceso del e- Discovery**
   4.1. Orden modelo en los casos de patentes
   4.2. Protocolo para los documentos almacenados electrónicamente "ESI Protocol"
5. **Conclusiones**

CAPÍTULO X. GEOLOCALIZACIÓN PÚBLICA Y PRIVADA. Dra. Beatriz Rodríguez

1. **Introducción**
2. **Concepto**
3. **Clasificación**
4. **Consecuencias de la geolocalización**
   4.1. Marketing de proximidad
   4.2. Realidad aumentada
   4.3 Geolocalización social
5. **Privacidad**
6. **Casos prácticos**
7. **Conclusiones**

CAPÍTULO XI. MARKETING COMPORTAMENTAL EN LÍNEA. Dra. María José Viega

1. **Introducción**
2. **Modalidades de publicidad comportamental**
   - 2.1. Las cookies
   - 2.2. Control del contenido de los usuarios
   - 2.3. Localización física
   - 2.4. Redes sociales
3. **Aspectos normativos de la Unión Europea**
   - 3.1. Directiva 2009/136/CE de 25 de noviembre de 2009
   - 3.2. Dictamen 2/2010 del Grupo de Trabajo del Artículo 29 de 22 de junio de 2010 sobre Publicidad Comportamental
   - 3.3. Dictamen 4/2012 del Grupo de Trabajo del Artículo 29 de 7 de junio de 2012 sobre la exención del requisito de consentimiento en la cookies
4. **Estados Unidos**
5. **Conclusiones**

CAPÍTULO XII. PIRATERÍA Y PRIVACIDAD. Dra. Jimena Hernández

1. **Introducción**
2. **Derechos de autor y piratería**
   - 2.1. Introducción a los Derechos de autor
   - 2.2. Infracciones al Derecho de autor
   - 2.3. Regulación nacional
3. **Piratería en Internet**
   - 3.1. Problemática que plantea
   - 3.2. Iniciativas mundiales para combatir la piratería en Internet
   - 3.3. Normativa en los países europeos
4. **Ley SOPA**
   - 4.1. Conceptualización
   - 4.2. Principales problemas que plantea
5. **Repercusiones de las leyes planteadas para el derecho a la protección de datos personales**
6. **Conclusiones finales**

CAPÍTULO XIII. COOPERACIÓN INTERNACIONAL. Esc. Cecilia Montaña

1. **Introducción**
2. **Implicancias de la Cooperación internacional en el ámbito de las autoridades de Protección de Datos**
3. **Funcionamiento de la Cooperación Internacional**
4. **Sistemas de Cooperación Internacional**
   - 4.1. Asia Pacífico
   - 4.2. Asistencia de CNIL a otras autoridades
   - 4.3. Sistema de información europea, (Cooperación Schengen)
   - 4.4. El Grupo de trabajo del artículo 29, (Article 29 Working Party)
   - 4.5. Red Iberoamericana de Protección de Datos, (RIPD)

5. **Buenas prácticas**
6. **Conclusiones**

CAPÍTULO XIV. HERRAMIENTAS DE CONCIENTIZACIÓN Y DIFUSIÓN: ¿PREPARADO PARA UNA VIDA 3.Ø?. Dra. Bárbara Muracciole

1. **Introducción**
2. **¿Evolución o Revolución?**
   - 2.1. Web 1.0
   - 2.2. Web 2.0
   - 2.3. Web 3.0
   - 2.3.1. Web semántica
   - 2.3.1.1.¿Qué es la Web Semantica?
   - 2.3.1.2.¿Para qué sirve?
   - 2.3.1.3.¿Cómo funciona?
   - 2.3.2. Web 3D
   - 2.3.3. Web geoespacial
   - 2.3.4. Web de las cosas
3. **Privacidad y protección de datos**
4. **Propuestas**
5. **Conclusiones**

CAPÍTULO XV. LA NUEVA NORMATIVA EUROPEA. Dra. Graciela Romero

1. **Introducción**
2. **Ámbito de aplicación de la nueva normativa**
   - 2.1. Alcance
   - 2.2. Objetivos
   - 2.3. Impacto
3. **La protección de datos en un mundo globalizado**
   - 3.1. Definiciones
   - 3.2. Consentimiento: modificaciones y alcance
   - 3.3. Tratamiento de datos especiales
4. **Reconocimiento de nuevos derechos**
   - 4.1. Derecho al Olvido
   - 4.2. Derecho a la Portabilidad de los Datos
   - 4.3. Derecho a reclamar ante las autoridades de control
5. **Obligaciones atrubuidas**
   - 5.1. A los responsables
   - 5.2. A los encargados del tratamiento
6. **Funcionamiento y control en el nuevo sistema**
   - 6.1. Las Autoridades Nacionales de Protección de Datos
   - 6.2. Mecanismo de coherencia para la actuación conjunta
   - 6.3. Consejo Europeo de Protección de Datos
7. **A modo de conclusión**

CAPÍTULO XVI. PROTECCIÓN DE DATOS EN AMÉRICA LATINA. AMPLIANDO HORIZONTES. Dra. Esc. María José Viega. Dra. Flavia Baladán

1. Introducción
2. Argentina
3. Bolivia
4. Brasil
5. Chile
6. Colombia
7. Costa Rica
8. Ecuador
9. El Salvador
10. Guatemala
11. Honduras
12. México
13. Nicaragua
14. Paraguay
15. Perú
16. República Dominicana
17. Uruguay
18. Venezuela
19. Conclusiones

CAPITULO I
DERECHOS FUNDAMENTALES

Dr. Marcelo Bauzá

DERECHOS FUNDAMENTALES

Dr. Marcelo Bauzá

1. Introducción

1.1. Caracterización de los Derechos Fundamentales

En la Memoria de Unidad Reguladora de Protección de Datos Personales[1] correspondiente al año 2011 se hacía la siguiente reflexión: "¿Por qué hablar de `derechos fundamentales´? La respuesta adecuada a esta interrogante supone conocer, en principio, qué es un derecho fundamental, para luego explicar de qué manera se aplica esta categoría de análisis a las bases de datos personales, e incluso a los datos personales aislados, siempre que exista algún tratamiento externo que afecte en cierta medida a sus titulares".[2]

Los Derechos Fundamentales (también llamados Derechos Humanos o simplemente DD.HH.) son aquellos derechos subjetivos esenciales o básicos, inherentes a los seres humanos por su sola calidad de tales, sin distinción ni discriminación alguna en función de factores tales como la nacionalidad, el sexo, origen nacional o étnico, credo o religión.

El derecho a la vida e, inmediatamente consustanciado con éste, el derecho a gozar de una vida digna, pueden resumir el catálogo de estos derechos subjetivos calificados como esenciales, que incluyen entre otros el honor, la libertad, la seguridad, el trabajo, la propiedad, la atención educativa y sanitaria.

Se trata de una categoría o institución cuyas especies y particularidades admiten cierta flexibilidad en función de la evolución histórica de la sociedad, respondiendo a las exigencias morales más acuciantes de cada época.

Como todo clase de derechos subjetivos, en especial la clase en examen, conllevan la facultad de ejercer una cierta acción reivindicativa o de defensa, en pos de obtener el correspondiente amparo a la hora de su goce efectivo.

Otros aspectos a destacar son la supremacía y la universalidad de estos derechos. La caracterización de los mismos no estaría completa si se omitiera considerar, además, que frecuentemente estos derechos operan en escenarios muy cercanos, cuando no haciendo parte crucial, a la vida política de los Estados y naciones, imponiendo límites o gravámenes a las actuaciones por momentos avasallante de los órganos públicos.

Como bien lo ha señalado prestigiosa doctrina "no puede dejarse a un ser humano sin derechos aunque sea posible limitar, restringir y hasta excluir, en determinados supuestos, su ejercicio y goce, de acuerdo con las pautas constitucionales. Estos límites y armonizaciones de los derechos fundamentales entre sí, vienen enmarcados por la ley (principio de legalidad) y las exigencias de

1 Se trata de la Autoridad garante de la protección de datos personales de Uruguay, creada en la misma ley que reconoce y regula la protección de datos personales como derecho fundamental, la Ley Nº 18.331 de 11-08-2008. Del punto de vista orgánico, es una entidad gubernamental desconcentrada de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información", esta última creada por el art. 72 de la Ley Nº 17.930 de 19-12-2005, cuyo texto original ha sido sometido a sucesivos cambios (redacción actual dada por el art. 80 de la Ley Nº 18.834 de 04-11-2011).

2 Memoria 2011 de la URCDP, pág. 6. www.agesic.gub.uy/innovaportal/file/2228/1/memoriaurcdp2011.pdf (Página visitada el 3 de setiembre de 2013).

razonabilidad, proporcionalidad y ajuste al fin debido.[3]

Por su alto valor ético, todos estos derechos están reconocidos y protegidos por los Tratados Internacionales y las Cartas Constitucionales de los Estados democráticos, destacando no solo la formulación de los mismos sino, además, las garantías y fórmulas apropiadas para hacer valer su respeto y vigencia.

1.2. La "estimativa jusnaturalista" en la Constitución uruguaya

Si hablamos de Derechos Fundamentales no podemos obviar que la Constitución Uruguaya contiene un par de artículos muy preclaros y hasta originales, que permiten una generosa receptividad del llamado jus naturalismo personalista.[4]

Se trata de dos normas nacidas en la segunda Carta Magna que se diera el país (la de 1918 que siguiera a la inaugural como estado independiente de 1830), textos que también figuran en las sucesivas de 1934, 1942 y 1952, hasta llegar a la actual de 1966 con los siguientes números:

Art. 72: La enumeración de derechos, deberes y garantías hechas por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.

Art. 332: Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de la leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.

¿Qué podemos inferir de la lectura de estas normas? ¿Qué es lo que merece ser agregado a modo de interpretación vinculada al tema central en examen de los alcances de la protección de datos personales como derecho fundamental?

Lo que hay que significar es que el sistema constitucional uruguayo dispone desde muy temprano, de una de las mejores herramientas jus-filosóficas, convirtiendo en derecho positivo del más alto nivel en la pirámide normativa lo que en otras latitudes requirió ser derivado con mayores esfuerzos y discusiones a partir de fuentes jurídicas diferentes, más precarias o susceptibles de mudanza.

Para Uruguay nunca existieron problemas de lagunas jurídicas en materia de DD.HH. Con el contralor jurisdiccional de constitucionalidad irrestricto de las leyes (arts. 256 a 261 de la Constitución uruguaya), el cuadro de garantías resulta completo, en un doble sentido: tanto sea para declarar fuera del orden jurídico un precepto legal que violente un derecho, o deber, o garantía, atinente a los derechos de la personalidad o a la forma republicana de gobierno, como para considerar vigente y eficaz cualquiera de estos tópicos jurídicos aun cuando no tuvieran previsión y reglamentación expresas (pero se ubiquen en la zona de mayor exigencia proteccionista como son los "derechos de la personalidad" o la "forma republicana de gobierno". Todo esto es posible y sucede gracias a la receptividad de la "estimativa jusnaturalista".

La peculiar fórmula confiere saludable dinamismo a un sistema jurídico particular, como el sistema de los DD.HH., que requiere necesariamente de sucesivas adaptaciones al compás de los cambios sociales.

3 Durán Martínez, Augusto. "¿Se puede limitar derechos humanos por actos administrativos dictados por órganos reguladores de la actividad privada? Especial referencia a las unidades de regulación creadas en Uruguay", http://www.direitodoestado.com/revista/REDE-2-ABRIL-2005-DURAN%20MARTINEZ.pdf (Página visitada el 2 de setiembre de 2013).

4 Bauzá, Marcelo. "La protección jurídica de los datos personales en Uruguay" http://www.bioeticachile.cl/felaibe/documentos/uruguay/LA%20PROTECCI_N%20JUR-DICA%20DE%20LOS%20DATOS%20PERSONALES%20EN%20URUGUAY.pdf (Página visitada el 2 de setiembre de 2013).

1.3. La Sociedad de la Información y los DD.HH.

La experta norteamericana Deborah Hurley ha definido apropiadamente la inserción de los Derechos Fundamentales en la sociedad de la información.[5]

En afinada síntesis y clara advertencia, nos señala que "los derechos humanos son la piedra angular de la civilización. Si este elemento central se derrumba a causa de nuestra negligencia o es despedazado por la fuerza, la sociedad y sus preciosos componentes como las artes, el comercio y la cultura, perderían un soporte y una protección esencial, se marchitarían y tambalearían." [6]

Aludiendo al "ubicuo entorno informativo" que caracteriza la actual sociedad, expresa que este rasgo esencial de la sociedad actual "plantea retos y oportunidades específicas en lo que se refiere a los derechos a la privacidad, seguridad, libertad de expresión, movimiento y asociación, así como también al acceso a la tecnología e información, los derechos de propiedad intelectual y el derecho a la educación."[7]

Los Derechos Fundamentales existen y operan en los múltiples planos del complejo entramado social contemporáneo. Al respecto nos dice la autora: "Si la sociedad de la información existe en realidad para servir a la humanidad y para contribuir a nuestra meta común de lograr que los derechos se cumplan para todos, entonces las discusiones internacionales sobre las nuevas tecnologías deberán apoyarse firmemente en los principios de derechos humanos previamente definidos y aceptados por la gran mayoría de los Estados del mundo."[8]

2. Protección de datos personales y DD.HH.

2.1. Un movimiento constante y sin retroceso

Dentro del marco que se acaba de exponer, y como uno de los Derechos Fundamentales que reciben acogimiento normativo relativamente reciente, aparece el "derecho a la protección de datos personales", integrado al llamado "bloque constitucional de derechos".[9]

Escribíamos unos años atrás: "Desde la década del 70´ del siglo pasado en adelante, se fue superando progresivamente el concepto restringido e individualista del `derecho de intimidad´ aplicado a la sociedad de la información, en beneficio de un concepto dinámico y socializante que recibe los nombre de `libertad informática´ o `autodeterminación informática (o informativa)´. Existen piezas de jurisprudencia extranjera destacables al respecto, como la Sentencia del Tribunal Constitucional Federal Alemán del 15 de diciembre de 1983, y la sentencia 292/2000 del 30 de noviembre de 2000 del Tribunal Constitucional Español, que anuncian la emergencia de un `derecho fundamental a la protección de datos de carácter personal´ independiente del derecho de intimidad, al que abraza

5 Hurley, Deborah. "La estrella polar: los derechos humanos en la sociedad de la información", en http://www.corteidh.or.cr/tablas/23206.pdf (Página visitada el 3 de setiembre de 2013).

6 Hurley, Deborah. Ob. Cit. pág. 7.

7 Hurley, Deborah. Ob. Cit. pág. 7.

8 Hurley, Deborah. Ob. Cit. pág. 8.

9 A modo de entender con precisión y síntesis este importante concepto del constitucionalismo moderno: "... la doctrina y la jurisprudencia constitucional han llegado también a aceptar la integración de todos los principios y normas sobre derechos humanos, cualquiera sea su fuente, en un bloque de la más alta jerarquía y fuerza normativa, tanto en el ordenamiento interno, como en el internacional. Tal bloque de constitucionalidad de los derechos humanos , representa la superación de la antigua y negativa disputa entre monismo y dualismo y ha abierto el camino hacia el reconocimiento de un derecho de los derechos humanos, supralegal y supraconstitucional, que, según se ha señalado, no es ya meramente derecho interno o internacional, sino universal". Tomado de BARBAGELATA, Héctor Hugo – "El bloque de constitucionalidad de los derechos humanos laborales", en http://www.fder.edu.uy/contenido/rrll/contenido/curricular/sector-publico/el-bloque-de-constitucionalidad.doc (Página visitada el 3 de setiembre de 2013).

pero al que también supera en varias facetas".[10]
Ni que hablar que en el tiempo transcurrido, las normas de este campo se han multiplicado en todo el planeta, no siendo ajeno a este incremento los países de nuestra región.[11]

Ha pasado el tiempo y hoy día existe consenso en que la protección de los datos personales debe ser entendida, profesada se podría decir sin ambages, como un "derecho fundamental autónomo". Un derecho que ha pasado a ser, de esta forma, un pilar indiscutido en toda sociedad justa y democrática, al mismo tiempo que se observa el esfuerzo por trazar puentes de adaptación entre las TI y este derecho, y entre el mismo y otros derechos igualmente trascendentes, demostrando con ello que su efectiva y justa vigencia pasa por esfuerzos aplicativos e interpretativos.

2.2. Algunos rasgos típicos de este derecho

Su reconocimiento así como su desarrollo y evolución, lo muestran como un derecho estrechamente asociado, y hasta causado, por algunos de los rasgos básicos de la sociedad contemporánea globalizada, donde la amplia disponibilidad de medios tecnológicos permite acopiar y someter a tratamientos de la más diversa índole y propósitos, grandes masas de datos identificatorios y caracterizantes de las personas. Ello puede ocurrir, y ocurre, aún sin el consentimiento de los titulares de los datos, lo que en épocas pretéritas resultaba prácticamente intrascendente, pero que hoy día -merced a la tecnología- conduce a situaciones que requieren intervención regulatoria, fundamentalmente por el riesgo y eventual perjuicio a los titulares de los datos que pueden causarse con tales actividades.

En pocos años, este nuevo derecho se ha ido destacando progresivamente de modo diferenciado respecto de otros derechos fundamentales afines con los cuales se lo asociara durante su periplo evolutivo (derecho de intimidad, derecho de privacidad), con los que generalmente, pero no en todos los casos, entra en vinculación y servicio.

Detenerse en la reflexión sobre la importancia de la protección de datos como derecho fundamental, en última instancia significa poner el foco en el principio y fin de todo el ropaje regulatorio. Nos permite conocer mejor, por sus raíces, la totalidad del sistema normativo que se ha ido construyendo en derredor de aquella protección. También nos enfrenta con algunas consecuencias irreductibles que no cabe perder de vista a pesar del embate de otros intereses: el carácter moral o ético de todo el sistema, su acendrada apoyatura en principios jurídicos de alcance universal, su porfía y eventual ponderación o proporcionalidad a resolver en los casos concretos donde entran en juego otros derechos y valores de alto rango.

Hay preguntas que por su sola formulación hablan de la trascendencia del tema: ¿Porqué considerar la protección de datos personales como un derecho fundamental? ¿Cómo influye el continuo avance de las TI en la vigencia de este derecho? ¿Cómo se armoniza su real efectividad en los casos donde comparece junto a otros derechos y valores de rango similar?

La magnitud del tema asoma también en frases como ésta: "Un orden social y un orden jurídico como su base, donde los ciudadanos ya no pueden saber quién sabe qué, cuándo y en qué situación, respecto a su propia persona, no sería compatible".[12]

10 Bauzá, Marcelo. La protección jurídica de los datos personales en Uruguay a través de la Ley Nº 17.838, en "El Derecho en Red. Estudios en Homenaje al profesor Mario Losano". Obra Colectiva del Instituto de Derechos Humanos "Bartolomé de las Casas" de la Universidad Carlos III de Madrid. Madrid, 2006.

11 El mapa de Iberoamérica muestra realidades diferentes, pero en mayoría con normativa proteccionista (constitucional, legal), ya sea a través del reconocimiento de la acción de habeas data, del derecho de intimidad o –los más avanzados- mediante leyes orgánicas de protección de datos personales. El estado de situación puede consultarse en la página web de la Red Iberoamericana de Protección de Datos Personales (RIPD), www.redipd.org/

12 Podlech, Adalbert. "Das Recht auf Privatheit", 1979. Citado por Aristeo García González en "La Protección de Datos Personales, Derecho Fundamental del Siglo XXI. Un Estudio Comparado" http://www.egov.ufsc.br/portal/sites/default/files/la_proteccion_de_datos_personales_derecho_fundamental_del_siglo_xxi._un_estudio_comparado.pdf (Página visitada el 3 de setiembre de 2013).

2.3. Situación de Uruguay hasta el año 2004

En Uruguay no existió sino hasta el año 2004[13], una ley de protección de datos personales, y la misma resultó acotada a los datos de origen o aplicación comercial.

En modo muy sintético puede decirse que antes del dictado de esta primera ley específica sobre el tema, el marco normativo uruguayo aplicable a la problemática general en juego se encuadraba en las siguientes normas: arts. 7º, 10, 28, 72 y 332 de la Constitución de la República; arts. 12 y 19 de la Declaración Universal de DDHH, art. 17 del Pacto Internacional de Derechos Civiles y Políticos, art. 5º de la Declaración de Bogotá de 1948, arts. 11, 14 y 25 de la Convención Interamericana de DD.HH; ley 16.011 (proceso de amparo); ley 16.616 (Sistema Estadístico Nacional); art. 694 de la ley 16.736; art. 218 de la Ley 17.283; numerosas normas legales relativas a diversas situaciones donde se consagra la obligación de guardar secreto o confidencialidad (registro de estado civil, tributario, bancario, etc.); decretos 258/992 y 396/003 relativos a datos médicos e historias clínicas electrónicas.

A cambio de la anotada carencia en cuanto a la existencia de una ley especial, lo que sí había desde tempranas épocas en el país era un excelente punto de partida en el plano constitucional, como quedara expuesto líneas arriba.

En suma, en el derecho uruguayo, aun careciendo hasta ese momento de un régimen legal particularizado para la protección de datos personales, en la medida que la temática en juego hace parte ineludible de los derechos inherentes a la personalidad humana bien puede afirmarse que ya se contaba con un régimen tuitivo. Régimen, claro está, de rango generalista y más bien principiológico. En nuestro concepto, de muy buena factura, no obstante lo cual revelado como insuficiente a la luz de las complejidades y especificidades regulatorias que demanda la problemática social que está detrás de la norma, como es la del conflicto entre la privacidad y el uso incentivado de las tecnologías de información y comunicación en la sociedad contemporánea.

Quiere decir que el "derecho a la intimidad" (y más avanzado aún -como sabemos- el llamado "derecho a la autodeterminación informativa" de cuyo reconocimiento y desarrollo hacen gala los ordenamientos modélicos en la materia), pudo en todo momento considerarse encartado dentro del sistema protector constitucional básico. En el caso que nos interesa relevar, esto aplicaba a posibles afectaciones de la intimidad y privacidad, merced al uso incontrolado de los bancos de datos. Sin embargo, es forzoso también reconocerlo a la luz de los antecedentes jurisprudenciales y doctrinarios que existían a aquella fecha, la verdadera aplicación de este derecho no sucedió sino a partir de que sobrevinieron las leyes específicas en la materia.

2.4. La Ley Nº 18.331 y su enfoque jus-humanista

Cabría manifestar que la ley anterior configuró un ensayo acotado de lo que vendría luego, desde el momento que si bien incluía la acción de habeas data (mecanismo garante del derecho fundamental en plano adjetivo), de todos modos no se pronunciaba acerca del plano sustantivo de este derecho, y en todo caso restringía el alcance del régimen a los datos comerciales.

La Ley Nº 18.331, en cambio, delinea un régimen mucho más acabado que el anterior, desde el momento que se extiende en tres planos jurídicos: el derecho sustantivo en juego, su anclaje orgánico institucional de regulación y control, su defensa en juicio.

El ámbito de protección ya no será el circunscrito a los datos comerciales como en la anterior ley, sino a todo tipo de datos personales. La nueva ley adopta el modelo europeo estatuyendo un conjunto

13 Ley Nº 17.838 de "protección de datos personales para ser utilizados en informes comerciales y acción de hábeas data", promulgada el 28-09-2004. Esta ley fue sustituida por la actualmente vigente Ley Nº 18.331 "protección de datos personales y acción de hábeas data" promulgada el 11-08-2008.

de principios tuitivos generales, una serie de derechos de los titulares de los datos, regímenes particulares para segmentos de datos calificados como especialmente protegidos, y un régimen de registro de bases de datos personales.

Se crea un órgano de regulación y control también diferente al que venía en la ley anterior, con autonomía técnica y competencias suficientes como para contribuir a la capilaridad e inserción efectivas del régimen en los diversos estratos de la sociedad (incluyendo potestades sancionatorias administrativas).

Se instaura, finalmente y con mayor precisión que el observable en la ley anterior, un régimen jurisdiccional de protección de este derecho, a través de la llamada "acción de protección de datos personales" o brevemente "habeas data".

Por su especial relevancia es del caso comentar que esta nueva ley comienza por una declaración vinculante, con lo cual despeja cualquier tipo de dudas acerca de la calificación y estatuto del derecho que simplemente reconoce la ley (no lo crea, de acuerdo con la doctrina jus naturalista):

"Artículo 1 – Derecho Humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República".

2.5. Coexistencia entre Derechos Fundamentales

En simultáneo con lo que se viene exponiendo, se observa la necesidad de armonizar el conjunto de derechos y libertades fundamentales que operan y se desenvuelven en el contexto de la Sociedad de Información. En un mundo donde el uso de la **network** se expande sin cesar, la transparencia de los asuntos públicos y la libertad de expresión también importan, y es por ello que es dable que aparezca otro escenario digno de atención. Un escenario enraizado en otro derecho de última generación, como es el derecho de acceso a la información, el que frecuentemente aparece conectado con cuestiones relativas a la privacidad y los datos personales.

De manera que el derecho de protección de datos personales, al igual que los restantes explícitos o implícitos derivados de nuestro texto constitucional, tampoco es de aplicación irrestricta, sino que resulta limitable en función de otras necesidades, debiendo serlo a través del dictado de una ley (material) de interés general (art. 7º de la Constitución).

Y es que la realidad a menudo muestra situaciones concretas de encuentro o confluencia entre este derecho y otros que se le enfrentan. Ha podido expresarse por lo mismo lo siguiente: "En la vida real con frecuencia entran en conflicto dos o más derechos fundamentales. Es el caso del `derecho de información´ y sus derivaciones asociadas a la libertad de pensamiento (expresión, comunicación, etc.), respecto del `derecho a la protección de los datos personales´".[14]

En algunos dictámenes e informes de la Unidad Reguladora y de Control de Datos Personales se hace caudal de la armonización requerida a la hora de aplicar el derecho en examen a casos concretos sometidos a la competencia de la Unidad:[15]

" II- Que ello no inhibe de advertir, como es de orden en el Estado de Derecho, que tales facultades se deben utilizar aplicando juicios de razonabilidad y ponderación, procurando compatibilizarlas lo más posible con la vigencia y efectividad de otros Derechos Fundamentales."[16]

"En la presente hipótesis estamos en presencia de dos derechos fundamentales. Por un lado el

14 Memoria 2011 de la URCDP, pág. 8. www.agesic.gub.uy/innovaportal/file/2228/1/memoriaurcdp2011.pdf (Página visitada el 3 de setiembre de 2013).

15 Consultables en www.agesic.gub.uy/innovaportal/file/2228/1/jurisprudencia.pdf (Página visitada el 3 de setiembre de 2013).

16 Dictamen N° 6 de 26 de mayo de 2011 sobre el procedimiento de inspección de las empresas amparadas por el secreto profesional.

derecho a la protección de los datos personales que consiste en el poder de disposición y de control sobre ellos, que se concreta en la facultad de consentir su recolección, la obtención y acceso, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular; y el derecho de acceso a la información pública que implica en puridad la facultad que ostenta cualquier ciudadano de acceder a toda la información que se halle en poder del Estado, en sentido amplio, para así ejercer un poder de controlar en el manejo de los recursos que en definitiva pertenecen a toda la sociedad.
En razón de ello corresponde realizar una ponderación de ambos derechos, atendiendo fundamentalmente al cumplimiento de la finalidad perseguida en el tratamiento de los datos de los becarios."[17]

"Agrega que `el tratamiento de los datos personales debe estar (...) sujeto a un principio de proporcionalidad, (...) datos personales adecuados, pertinentes, no excesivos y circunscritos a la finalidad que tiene el reportaje, que no es otra que ilustrar la información aportada (subrayado nuestro).
Por ende, los medios de comunicación deben valorar la necesidad de que su actuación se dirija a conciliar, en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales, ambos derechos fundamentales.[18]

3. La aprobación del Convenio Nº 108

3.1. Un hito en la materia

Por invitación del Consejo de Europa y atendiendo a un reconocimiento de los avances del país en el reconocimiento y defensa de la protección de datos personales, Uruguay se convirtió recientemente en el único país fuera de la región europea, que ha suscrito este tratado internacional, directamente enlazado a la temática que venimos analizando.
En efecto, a través de la Ley Nº 19.030 de 27-12-2012, el país aprueba este texto jurídico internacional denominado oficialmente "Convenio N°108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", y también el "Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos".
La finalidad del Tratado al que Uruguay adhiere, es garantizar, en el territorio de cada Parte, a toda persona física, el respeto de sus derechos y libertades fundamentales, independientemente de su nacionalidad o su residencia. Más concretamente, se alude al derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona, lo que el propio texto aprobado califica como «protección de datos».
El país completa de esta manera un círculo de perfección en torno al modelo asumido, ya que previamente había obtenido la aprobación de la Unión Europea como país adecuado para recibir por transferencia internacional los datos personales de los ciudadanos europeos.[19]

17 Informe N° 6.039 de 13 de junio de 2011, por consulta del Fondo de Solidaridad respecto si puede informar o no la identidad de los beneficiarios de las becas.

18 Informe N° 7.010 de 18 de noviembre de 2011 sobre consulta relativa al tratamiento de datos personales de imagen por parte de la prensa, y donde se invocan expresiones de la Agencia de Protección de Datos y el Tribunal Constitucional españoles.

19 Decisión de Ejecución de la Comisión Europea, de 21 de agosto de 2012, "de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32012D0484:ES:NOT (Página visitada el 3 de setiembre de 2013).

3.2. Aspectos esenciales de este Tratado

Coinciden con los previstos en la ley uruguaya, caso contrario no habría sido aceptada la adhesión.
Abarca los tratamientos automatizados y manuales, tanto del sector público como privado (arts. 3.1. y 3.2.c.).
Estatuye una serie de principios que califica como los "básicos para la protección de datos" (se trata de un convenio "de mínimos" como lo especifica el art. 11), abogando porque los adherentes tomen las medidas de derecho interno necesarias para hacerlos efectivos en sus respectivas jurisdicciones (art. 4º).
Estos principios son los relativos a la calidad de los datos (art. 5º), y que especifica en "obtención y tratamiento leales y legítimos", "finalidad determinada y legítima sumado a un utilización compatible con dicha finalidad", "adecuación-pertinencia-no excesividad", "exactitud y actualización", "conservación que permita identificar a la persona concernida durante tiempo acorde a la finalidad del registro".
Restringe el tratamiento de los datos raciales, etc. (datos sensibles) a la existencia de garantías apropiadas, al igual que los datos de condenas penales (art. 6º).
Impone el deber de tomar medidas de seguridad apropiadas para la protección de los datos contra destrucciones o pérdidas, así como accesos, modificaciones o difusiones, no autorizadas (art.7º).
El Convenio impone igualmente lo que llama "garantías complementarias para la persona concernida", consistentes en poder conocer la existencia de los archivos y datos conexos (finalidades, identidad y residencia del responsable); obtener información de sus contenidos en relación a la persona concernida y, llegado el caso, la rectificación o borrado de los datos cuando corresponda; disponer de un recurso para ejercitar cuando no es atendido el pedido por parte del responsable (art.8º).
Se prevé el compromiso de los Estados parte de establecer sanciones y recursos convenientes contra las infracciones a las normas de derecho interno que efectivicen estos principios básicos (art. 10).
Están regulados también los "flujos transfronterizos de datos" (capítulo III, arts. 12 a 17).
El Protocolo Adicional, por su parte, contiene entre sus cláusulas más importantes la relativa al deber de disponer de una o más autoridades responsables de garantizar el cumplimiento de las medidas previstas en el derecho interno para hacer efectivos los principios, "con total independencia" según reza el apartado 3 del art. 1º.

4. Conclusiones

La protección de datos personales ha tomado dimensión jurídica en los países occidentales, en un lapso que va desde las primeras normas anglo americanas y europeas de la pasada centuria (años 60 y 70 respectivamente), hasta los tiempos que corren, en términos generales recorriendo un periplo de cuarenta o cincuenta años.

Justo es advertir que la encarnadura progresiva de este derecho y su regulación, ha estado tempranamente identificada con el apreciado elenco de los Derechos Fundamentales, sin que baste su raigambre constitucional. Esta última puede verse como una condición necesaria pero no suficiente, desde el momento que el auténtico y eficaz régimen protector en esta materia, requiere de otros componentes: una ley articuladora con su reglamento, un conjunto de principios y derechos básicos aplicables a los distintos casos de asunción del ultra citado derecho en la vida real, un órgano de control para ocuparse de todo lo referente a la institucionalidad y organicidad del mismo derecho, un recurso jurisdiccional de reclamo para cuando el derecho es desatendido por quien debió atenderlo.

Todo esto es pasible de adecuado cumplimiento cuando se adopta la estrategia de edificar las políticas de aprovechamiento de las tecnologías informáticas y comunicacionales del Estado y la Sociedad, poniéndole palancas de impulso a los múltiples derechos de la ciudadanía.

La protección de datos personales es uno de estos derechos. Su realidad y eficacia en la comunidad siempre dependerán de dos factores por igual: la bondad de los textos normativos, y el **enforcement**[20] aplicados a una inteligente impregnación social y cumplimiento a cabalidad de la regla jurídica. De nada más y nada menos que estos factores, depende la suerte de este derecho fundamental bajo las circunstancias en las que le toque explayarse.

Bien decía la ex presidenta del Tribunal Constitucional Federal de Alemania dirigiéndose al público uruguayo en oportunidad de su visita al país algunos años atrás sin por ello perder vigencia: "Si nosotros queremos aprovechar las oportunidades que nos brindan la informática y comunicación modernas, debemos procurar una protección preventiva del derecho a la autodeterminación informativa, porque la protección de datos garantiza las libertades civiles, que a su vez son la savia vital de una sociedad democrática. Por lo tanto la institución del encargado de protección de datos es una de las garantías más importantes de una democracia viva."[21]

20 Entendiendo por tal, el activismo de las autoridades en todos los frentes necesarios para que una norma jurídica tenga acatamiento cabal entre los diferentes actores del sistema social al que va dirigida, comprendiendo los propios encargados de ejecutar o aplicar la norma.

21 Limbach, Jutta. "Veinticinco años de Ley Fundamental de Protección de Datos alemana" (11 de junio de 2002). Conferencia de Clausura brindada en la Suprema Corte de Justicia cerrando el Coloquio "La protección de datos personales" llevado a cabo en Montevideo del 14 al16 de mayo de 2003 bajo el esfuerzo conjunto de varias instituciones. Las Actas comprensivas de este coloquio, fueron publicadas bajo el título "¿Seguridad, privacidad, confidencialidad? El desafío de la protección de datos personales", Ediciones Trilce, Montevideo, 2004.

CAPITULO II

SOCIEDAD DE LA INFORMACIÓN

Dr. Ramiro Prieto

SOCIEDAD DE LA INFORMACIÓN

Dr. Ramiro Prieto

1. Consideraciones preliminares sobre Sociedad de la información

1.a. Introducción

Asistimos de un tiempo a esta parte a una nueva etapa en el desarrollo de la sociedad. La implementación de las tecnologías, así como su constante manipulación, han generado una avalancha de información la cual ha determinado la vida de los ciudadanos. Esta revolución tecnológica que envuelve cada vez más a la sociedad provoca la necesidad de resaltar y plantear la vigencia de sus pilares fundamentales.

Con motivo de este nuevo marco social y del virtuoso avance de las TIC, el acceso, tratamiento y transmisión de la información por parte de la sociedad no solamente se produce en grandes proporciones o cantidades, sino que su intensidad es cada vez más pronunciada, convirtiendo a ésta en el eje central de la vida de las personas.

Esta nueva concepción de sociedad no solamente se manifiesta desde el punto de vista tecnológico, económico, cultural y social, sino que implica también un gran desafío para el derecho, en especial para una de sus ramas como lo es la Protección de Datos Personales.

La Sociedad de la Información es el contexto dentro del cual se enmarca la Protección de Datos Personales. Esto nos obliga a determinar el alcance y las características de este nuevo fenómeno social para determinar así las consecuencias jurídicas en el ámbito de los datos personales, estableciendo los caracteres para su regulación y alcance, a los efectos de fortalecer su control protección y vigencia.

Los Datos Personales, y su protección pasan a tomar un rol protagónico frente al avance de las TIC. Este se manifiesta entre otras cosas por el surgimiento de grandes bases de datos que traen como consecuencia la aparición cada vez más frecuente de mecanismos de identificación o generación de perfiles de los individuos. Frente a estas situaciones la búsqueda del equilibrio entre los derechos de los ciudadanos, la protección y el control de éstos por parte de los organismos gubernamentales, y la dificultad de conciliar las normativas de protección de datos locales, con la regulación o estándares internacionales, aparecen como los principales escollos que en esta nueva etapa la sociedad debe resolver.

El derecho a la Protección de Datos Personales y su reconocimiento como derecho humano lo ponen como protagonista en este escenario de constante innovación, manipulación y desarrollo de las Tecnologías de la Información y Comunicación. El desafío de su protección en este nuevo marco social, surge como uno de los elementos centrales en esta temática.

1.b. Conceptualización, origen y evolución

Al día de hoy tanto a nivel académico, gubernamental como a nivel de la sociedad civil (instituciones, empresas) se reconoce de manera unánime la existencia del concepto de Sociedad de la Información. Dichos sectores no solamente confirman su existencia sino que han incorporado dicho concepto al

lenguaje común de todos los actores participantes del mundo de las Nuevas Tecnologías.
Dicha unanimidad no se ve tan marcada respecto de determinar la conceptualización, el origen y la trascendencia del fenómeno. En el primer caso porque las definiciones dadas, pecan en algunos casos de ser muy escuetas o muy amplias; en el segundo porque su inicio es de difícil determinación histórica y en el tercero por las diferentes visiones de cada autor que entienden al fenómeno desde un punto de vista tecnológico, ocupacional, cultural o económico.

La IBM Community Development Foundation definió en el año 1997 a la Sociedad de la Información como "una sociedad caracterizada por un alto nivel de intensidad de información en la vida cotidiana de la mayoría de los ciudadanos, organizaciones y sitios de trabajo, por el uso de tecnología común compatible para un amplio rango de actividades de negocio, educacionales, personales o sociales, y por la habilidad de transmitir recibir e intercambiar datos digitales rápidamente entre sitios indistintamente de la distancia"[1].

Por otro lado, el portal web de AGESIC señala que: "Sociedad de la Información y del Conocimiento" es el nombre que se le da a la sociedad actual, caracterizada por la importancia que, en términos económicos y sociales, tienen las actividades de creación, distribución y manipulación de la información y el conocimiento." [2]

Este último concepto, tal vez es el más difundido y extendido por parte de la doctrina la cual le añade también las consecuencias que produce desde el punto de vista social económico, político y cultural, en función de la perspectiva que cada uno tiene del fenómeno.

Señalábamos también que su punto de partida es de difícil precisión en virtud de que la mencionada amplitud del concepto y de las referencias que con el mismo se hace a situaciones en apariencia distintas pero todas ellas vinculadas e integrantes del mismo fenómeno genera la dificultad de su ubicación en un momento histórico preciso y determinado igualmente se entiende que su origen es anterior al auge de las Tecnologías de la Información y Comunicación.
Teniendo en cuenta esto, parte de la comunidad académica afirma que ya en el año 1914 al inicio de la primera guerra mundial con la referencia y la conceptualización que de la sociedad post-industrial hace Arthur J. Penty se sientan los cimientos del concepto que hoy conocemos como Sociedad de la Información.

Penty remontándose a esa época señalaba que el transcurso de una etapa a la otra en la evolución de la sociedad estaba marcado fuertemente por la comunicación y el intercambio de información entre personas.

Otros autores sitúan el puntapié inicial en el año 1973 y le atribuyen la nomenclatura al sociólogo estadounidense Daniel Bell quien continuando la línea propuesta por Penty introdujo el concepto de Sociedad de la Información al mundo occidental. Bell señalaba que "Una sociedad post-industrial es básicamente una sociedad de la Información. El intercambio de información en términos de varios tipos de procesamiento y almacenamiento de datos, investigación de mercado, etc...es la base de la mayoría de los cambios económicos"[3].

Respecto de esto algunos entienden que este último concepto está condicionado a la aparición del fenómeno y su determinación ya una década antes en Japón por Jiro Kamishima en enero de 1964.

Posteriormente ya a partir del año 1995 Frank Webster basándose en un estudio realizado por Fritz Machlup en 1962 referente la utilización de la información como materia prima por parte de la industria estadounidense, llega a la conclusión de que es extremadamente dificultoso tomar al fenómeno

1 Crespi Albert, Serrano, Antonio y Cañabate, Carmona. Análisis de la Evolución y Tendencias Futuras de la Sociedad de la Información. Publicada en Cátedra Telefónica –UPC. Barcelona. 2010. Pág. 7.

2 www.agesic.gub.uy. (Página visitada el 8 de marzo de 2013).

3 Albert Crespi Serrano, Antonio Cañabate Carmona. Ob. Cit. Pág. 7.

Sociedad de la Información como algo absoluto y uniforme, concibiendo al mismo como un fenómeno heterogéneo al igual que todos aquéllos que se producen en una sociedad lo que implica analizarlo desde diferentes enfoques aplicando un concepto distinto dependiendo del ámbito tecnológico, cultural, económico, ocupacional o espacial al que se refiera.

Como resulta de manifiesto no solo la conceptualización del fenómeno sino también su surgimiento no han generado unanimidad en la doctrina situación que refleja la complejidad del tema.

1.c. Importancia

Al igual que lo que sucede con el concepto y el surgimiento de lo que conocemos como Sociedad de la información, tampoco existe unanimidad en la comunidad académica respecto de la importancia de dicho fenómeno. Los mencionados contrapuntos devienen básicamente de la concepción que cada autor tiene del fenómeno, algunos hacen más énfasis en el plano social y otros hacen hincapié en el desarrollo de las Tecnologías de la Información y Comunicación.
Los autores que atribuyen la importancia al plano social, entienden que la sociedad esta transitando por una revolución social similar a la ocurrida en la Revolución Industrial, no obstante no dejan de reconocer la importancia de las nuevas tecnologías pero entienden que éste no es el elemento central a analizar y que se está frente a un verdadero fenómeno social. En cambio aquéllos que atribuyen la importancia del fenómeno al desarrollo tecnológico, entienden que estamos frente a una fase más del desarrollo humano en esta área, priorizando esto frente al análisis de los factores sociales.

Más allá de los distintos enfoques dados por la comunidad académica, la sociedad civil o los organismos gubernamentales que han generado una importante variedad de conceptos y denominaciones de la Sociedad de la Información no existen dudas que nos encontramos frente a un fenómeno nuevo y trascendente en la historia de la humanidad, cuyo alcance es de difícil delimitación dependiendo del enfoque y la órbita en que lo analicemos.

2. Desarrollo del fenómeno Sociedad de la Información en Latinoamérica y Europa.

2.1. Sociedad de la Información en Europa

2.1.a. Desarrollo de la Sociedad de la Información en Europa y el surgimiento de la Agenda Digital Europea.

La informatización de la información y el procesamiento de grandes volúmenes de datos han generado un impacto muy importante no solamente en la economía, con el surgimiento de nuevas industrias y la modificación de las ya existentes, sino también desde el punto de vista social con el surgimiento de innumerables oportunidades de empleo, desarrollo cultural de las sociedades y acortamiento de las distancias existentes entre los integrantes de las mismas.

Esto ha generado que se fomente en Europa el desarrollo de políticas que fomenten la utilización del fenómeno Sociedad de la Información a nivel comunitario y que los países integrantes de la Unión tiendan a la búsqueda de la explotación máxima de los beneficios que surgen de esta nueva era.

Uno de los pilares básicos de esta política Europea, tendió al desarrollo de la conectividad en toda Europa, a los efectos de que todos los países integrantes del bloque puedan explotar y desarrollar la era digital en todos sus aspectos, centrándose en el objetivo de lograr el acceso a Internet por parte de todos los ciudadanos, empresas y centros educativos además de ampliar su utilización a la

administración pública, situación que será piedra fundamental para el desarrollo de la Sociedad de la Información y sus beneficios.

El inicio de esta serie de políticas tendientes a fomentar la aplicación de la Sociedad de la Información en Europa, podemos determinarlo aproximadamente en el mes de diciembre de 1999, en donde es lanzada por parte de la Comisión Europea la iniciativa eEurope con el objetivo antes señalado de conectar en línea a toda Europa. Correlativamente en el mes de enero de 2000 la Comisión también se expide emitiendo un documento denominado "Estrategias para la creación de Empleo en la Sociedad de la Información" fundándose en el potencial de innovación y crecimiento económico que posee la Sociedad de la Información y su importancia cada vez más marcada en la política económica.

La iniciativa eEurope marcaba como objetivos principales, entre otros los siguientes: Fomentar el máximo acceso por parte de la juventud europea a la era digital, disminuir el costo del acceso a internet, ampliar el desarrollo del comercio electrónico, aumentar la velocidad de navegación para estudiantes e investigadores, desarrollo de tarjetas inteligentes para el acceso seguro a las aplicaciones electrónicas, participación de las personas con discapacidad en la cultura electrónica, desarrollo de la salud en línea, transporte inteligente y administración pública en línea.

Este primer proyecto denominado eEurope es ampliado tiempo después en marzo del año 2000 por el Consejo Ministerial Europeo creando las Estrategias de Lisboa conocidas también como Agenda de Lisboa, la cual tenía como objetivo principal potenciar al máximo la economía europea para convertirla en la más competitiva y dinámica del mundo antes del 2010, utilizando como herramienta para ello las nuevas oportunidades económicas que surgen a partir de Internet.

A partir de aquí los Jefes de Estado y de Gobierno de los países miembros se comprometen a redoblar esfuerzos e instaurar una serie de medidas para el cumplimiento del Plan eEurope, algunas de esas medidas constaban en: conectar y expandir la utilización de la red a todos los ciudadanos, centros educativos, empresas y administración pública de cada país; generar una cultura digital y fomentar los emprendimientos relacionados con ella; consolidar el proceso digital, generar confianza en el mismo y aumentar al máximo las posibilidades de integración social que el mismo brinda, etc.

A partir del modelo del proyecto eEurope del año 2000 y con motivo de las reacciones del Parlamento Europeo y los Estados Miembros, el Consejo Europeo de Lisboa entiende necesaria la realización de una serie de actualizaciones que vengan a afirmar algunos aspectos fundamentales de ese proyecto original, lo que va a generar e Plan eEurope 2002 con nuevas metas a cumplir para los años siguientes.

Esas nuevas metas se decide agruparlas en función de tres objetivos: Internet más rápida, barata y segura; mayor inversión en las personas y su formación; y la estimulación al máximo del uso de Internet.

Los objetivos fijados para el Plan eEurope 2002 se cumplieron de manera satisfactoria, lo que genero que el Consejo Europeo de Sevilla en el año 2002 impulse la segunda fase con el desarrollo del Plan eEurope 2005 con nuevos objetivos a cumplir en los años posteriores.

El Plan eEurope 2005, se ejercita a partir de medidas políticas que adapten y generen coherencia entre las legislaciones nacionales y europeas, fomentando el desarrollo de buenas prácticas, compartiendo datos comparativos de logros y objetivos alcanzados, que fomenten los mecanismos de coordinación de las políticas digitales y continuar así el desarrollo de la Sociedad de la Información en Europa. Para alcanzar esto el Plan parte de dos premisas fundamentales: la primera consta en fomentar los servicios, aplicaciones y contenido con especial énfasis y relevancia en los servicios públicos, y la segunda se basa en la ampliación de la infraestructura de banda ancha con especial relevancia en la seguridad de la transmisión de la información y las transacciones que en ella se producen

Con estos elementos para el año 2005 Europa se proponía tener: modernos servicios públicos en línea; una administración electrónica más eficaz; servicios electrónicos de educación y salud y un escenario confiable y que fomente las transacciones y negocios electrónicos.

Esta etapa del eEurope, sin dudas la más trascendente para el desarrollo digital de Europa continuó con nuevos objetivos planteados por la Comisión Europea tendientes a la búsqueda del desarrollo de una economía digital abierta, competitiva y con especial énfasis en las Tic como mecanismo para lograr mayor inclusión social y una sustancial mejora en la calidad de vida de los individuos. Este nuevo plan se denominó Iniciativa i2010. Dicha herramienta dio una sustancial importancia a las recomendaciones realizadas por los miembros y a todas las partes integrantes del fenómeno Sociedad de la Información teniendo en cuenta el análisis y los resultados y objetivos alcanzados por los planes anteriores.

A partir de allí esta iniciativa y con modificaciones a los marcos jurídicos y regulatorios y una mejora en la calidad de los servicios, Europa se pone como meta para el año 2010 poseer un espacio único de información con servicios de banda ancha que sean accesibles a la población, con garantías de seguridad necesarias y amplios contenidos y servicios digitales; también se propone fomentar la investigación, el desarrollo y la inversión en la órbita de las Tecnologías de la Información y la Comunicación para poner a Europa en los primeros lugares a nivel mundial y no perder distancia respecto de sus principales competidores tanto desde el punto de vista tecnológico, jurídico y organizativo; y por último, alcanzar una Sociedad de la Información con base en el individuo logrando una mayor inclusión social, un mejor nivel de vida y disminuyendo las desigualdades existentes, aprovechando las oportunidades que brinda este nuevo entorno como son: mayores posibilidades de educación y desarrollo cultural, mejora en los servicios públicos y un mayor alcance por parte de éstos, aumento de puestos de trabajo, mejora en los servicios de transporte, entre otros.

El advenimiento de la crisis económica en Europa a partir del año 2009 la cual estancó su crecimiento y golpeó de manera muy profunda no solo en el rubro económico sino también en el social, plantea la necesidad de replantearse determinadas cuestiones y objetivos que ya no se veían acompasadas a la Agenda de Lisboa, esto generó que la Unión Europea adopte un nuevo Plan en la búsqueda de mitigar en mayor medida los efectos negativos de la crisis y buscar una rápida salida a la misma. Así surge en marzo de 2010 lo que se denomino Estrategia Europa 2020, la cual tenía como prioridades en primer lugar la búsqueda de un crecimiento inteligente, esto se basaba en un desarrollo económico basado en el conocimiento y la innovación y la búsqueda de más facilidades de financiación a las iniciativas de esta índole; crecimiento sostenible con una utilización más eficaz de los recursos y con énfasis en la protección del medio ambiente y en la utilización de recursos renovables; y un crecimiento económico que no descuide la integración social busque la disminución al máximo de la pobreza y aumente los niveles de empleo y capacitación de los individuos, con gran énfasis en la educación de los más jóvenes; y por último la impulsión de la creación de una Agenda Digital Europea que genere en base a la utilización de Internet un mayor beneficio a las familias y empresas.

Con motivo de este último objetivo y a través de la Presidencia Española de la Unión Europea, en el año 2010 se elabora un proyecto que se denomina la Estrategia de Granada para la Agenda Digital Europea como plan a afrontar por la Unión Europea en materia de Sociedad de la Información para el periodo 2010-2015. Esta iniciativa española, pasa a convertirse en la Declaración de Granada para la Agenda Digital, en la que se fijan los ámbitos de actuación que debe seguir Europa para el período señalado, algunos de ellos son: fomento del uso avanzado de Internet, creación de marcos de protección de derechos de los usuarios, la creación de un "Mercado Único Digital", el avance y mejora de los servicios públicos digitales, la dimensión internacional de la Agenda Digital y la fijación de nuevos indicadores sobre Sociedad de la Información[4].
Posteriormente, como sucesor de la Iniciativa i2010 y confirmando lo anteriormente planificado en la Estrategia de Granada se aprueba la Agenda digital Europea el 19 de mayo de 2010, la cual plantea

4 CEDDET. Políticas Públicas para el impulso de la Sociedad de la Información. El proyecto Red.es, 3ª Edición. Modulo 1 (Parte I): el impulso de la Sociedad de la Información desde la administración pública, pág. 18.

líneas estratégicas que permiten la reactivación económica y social y delimitan los planes de acción en Europa para el año 2015 con referencia a la Sociedad de la Información.
Dichas líneas estratégicas se agrupan en siete objetivos primordiales como son:

En primer lugar, la creación de un mercado digital que fomente el intercambio y las transacciones transfronterizas, tratando de buscar mecanismos de solución a las posibles distancias que puedan existir respecto de la regulación interna de cada uno de los miembros de la comunidad, en función de esto se busca fomentar el acceso a contenidos legales, con mas autorizaciones referentes a derechos de autor, concesión de licencias, búsquedas de mayor facilidad en los pagos online, lineamientos comunes respecto a la facturación electrónica y la búsqueda de mecanismos más eficaces de solución de controversias que puedan provocarse con ocasión de la red.

En segundo lugar, se busca fomentar la interoperabilidad y el surgimiento de mas normas referentes a Tecnologías de la Información y Comunicación.
En tercer lugar se propone generar mayor confianza en el sistema y en la seguridad del mismo, con políticas de seguridad tendientes a evitar ciberataques y mal manejo de datos.
En cuarto lugar, la agenda tiende a la búsqueda del aumento potencial en el acceso por parte de los europeos a una Internet con velocidades superiores, como pilar de la creación de mayores servicios y acceso a contenidos por parte de los individuos.

En quinto lugar busca impulsar la investigación y la innovación en las Nuevas Tecnologías, potenciando inversiones privadas e implementando subsidios a las ideas productivas que puedan generarse.

El sexto objetivo tiene como premisa la implementación de herramientas digitales que aumenten las capacidades de los ciudadanos, disminuyan la brecha digital y permitan una mayor oferta de servicios públicos y un mejor aprovechamiento de los mismos.

Y como último objetivo la Agenda Digital Europea se propone explotar al máximo el potencial de servicio que permiten las nuevas tecnologías, brindando mayor importancia a la computación en la nube, con especial hincapié en el ahorro energético, la prestación de servicios de salud y la igualdad de oportunidades entre los ciudadanos.[5]

2.1.b. El plan avanza en España: Un modelo exitoso de política de Sociedad de la Información.

España ha sido uno de los países que más hincapié ha hecho en el desarrollo de políticas para implementar la Sociedad de la Información, no solamente a través del trabajo mancomunado con los demás integrantes de la Comunidad Europea, sino también con políticas internas que han tenido el objetivo de implementar dichas medidas.

El plan avanza, llevado adelante por España es visto como un modelo exitoso de política referente a la Sociedad de la Información y es analizado como caso de éxito o modelo a seguir para algunos países Latinoamericanos en el tema. Su implementación y los logros alcanzados respecto a cuestiones como: la difusión de TIC y sus consecuencias a nivel de la educación, salud, gestión del estado y coordinación público-privada son vistos como sus aspectos más relevantes.

El Plan avanza contó con varias fases, y en su inicio logró congeniar los esfuerzos de las comunidades autónomas, el gobierno español, y la comunidad Europea, a tal punto que la Comisión de Sociedad de la Información del Senado español aprobó el proyecto por unanimidad en octubre de 2004.

La primera de las fases tenía el objetivo de lograr la recuperación de España respecto a la difusión y aplicación de TIC y adaptar el proyecto español a la Estrategia de Lisboa, puesto que se entendió

5 CEDDET. Ob. Cit. Págs. 19 y 20.

necesario acortar las diferencias existentes al respecto, para con el resto de Europa. Esa primera etapa contó con 4 áreas de actuación: Ciudadanía Digital (con el objetivo de dotar a los hogares de TIC y hacerles comprender la importancia de su utilización); Economía Digital (tiene como objetivo incrementar la utilización de TIC en las PYMES); Servicios Públicos Digitales (con el objetivo de adoptar las TIC en la gestión del Estado y brindar mayores servicios públicos a través de su utilización por la sociedad con especial énfasis en los servicios educativos); Contexto Digital (tiene como objetivo el aumento de la infraestructura de banda ancha y servicios de telecomunicaciones, además de generar conciencia y capacitación en TIC), todos estos objetivos se complementan con reformas normativas que buscaban adaptar el sistema jurídico a la realidad actual.[6]

A partir de ese primer paso y cumplidos varios de sus objetivos en el 2009 se estructura la segunda etapa denominada Plan Avanza 2 para la cual se propuso para el periodo 2011-2015 utilizar esa base tecnológica generada para potenciar servicios y productos que lograran colocar a España a la vanguardia de utilización de TIC y lograr a través de ellas, superar la fuerte crisis financiera reinante. Así en 2012 se envía al Parlamento español la propuesta de la Agenda Digital española para el periodo 2013-2015 con dos objetivos primordiales: mayor cobertura, adopción y desarrollo de la banda ancha y el desarrollo de la Economía Digital con la meta de superar la mencionada crisis.

El Plan Avanza 2 se centro en fomentar las inversiones para la creación de productos de internet que versaran sobre servicios, contenidos, protección del medio ambiente y demás mejoras tecnológicas y organizativas. Además, buscó impulsar la incorporación de TIC en las PYMES, implementando subsidios, planes pilotos y demás cuestiones que demostraran los beneficios de la utilización de tecnología en la gestión de las empresas y sus productos, e incorporarlos a un contexto tecnológico muy beneficioso para su productividad.
La estrategia desarrollada por España se ha implementado con éxito y como se mencionó es vista como un ideal a seguir por parte de aquellos países que están en fase de implementación de políticas de TIC; algunos de sus logros son: el acuerdo alcanzado por todos los actores (Gobierno, Comunidades autónomas y Sociedad Civil) para implementar las medidas y lograr así los objetivos propuestos; ampliar la cobertura de banda ancha a un 99% de la población; completar exitosamente la transición a la televisión digital terrestre; la realización vía web de un 99 % de trámites ante el gobierno central; maximizar la utilización de TIC en PYMES, entre otras.[7]

2.2. Sociedad de la Información en Latinoamérica.

CEPAL, en su publicación Estrategias de TIC ante el desafío del cambio estructural en América Latina y el Caribe señala que: "...Las TIC como tecnologías de propósito general, pueden contribuir a modernizar y revitalizar las actividades productivas tradicionales de la región, así como a tornar más eficientes e inclusivos los servicios públicos. Las nuevas plataformas y redes de información están transformando radicalmente los sistemas de toma de decisiones y modelos operativos en industrias como la minería, la pesca, la agricultura, el transporte y el turismo, así como en muchos otros servicios. Los datos abiertos y el Big Data están llamados a revolucionar completamente la gestión de la información, seguridad y logística en las grandes ciudades (smart cities). Las pequeñas empresas pueden apoyarse en las TIC para dar saltos en la eficiencia de su gestión y en sistemas productivos y comerciales, así como para ingresar en mercados antes difíciles de alcanzar, como el de compras públicas y el internacional. El comercio electrónico abre nuevas oportunidades para las micro y pequeñas empresas que consigan participar de estas plataformas..." El fragmento transcripto, nos demuestra el impacto del fenómeno Sociedad de la Información en el mundo actual, por dichos motivos. Latinoamérica no se quedó tras Europa y salió en la búsqueda de implantar planes y proyectos a los efectos de aprovechar al máximo las ventajas de este nuevo fenómeno, ya sea desde el punto de vista económico (con la mejora en la gestión de las empresas), cultural (democratizando el acceso a diferentes contenidos culturales), social (disminuyendo las diferencias

6 CEDDET. Ob. Cit. Pág. 37.

7 CEPAL. Estrategias de TIC ante el desafío del cambio estructural en América Latina y el Caribe. Colección documentos de proyectos, pág. 41. Santiago de Chile, 2005.

de acceso a las TIC y generando un nuevo modelo de sociedad más inclusiva, y con el desafío aun pendiente de ir en busca de la disminución de la brecha digital), entre otros elementos.

El inicio de este tipo de políticas de implementación de TIC y desarrollo de la Sociedad de la Información en América Latina y El Caribe puede determinarse aproximadamente a finales de la década de los 90 con algunas estrategias importantes implementadas por Brasil, Chile y Colombia. Posteriormente estas políticas implementadas por estos países se vieron reforzadas en los años 2003 y 2005 por las Cumbres Mundiales de Sociedad de la Información, por una marcada decisión de Naciones Unidas de incluir este tipo de políticas como sus objetivos principales y posteriormente por la aparición del primer plan de acción regional sobre Sociedad de la Información para América Latina y El Caribe eLAC2007.

El plan de acción de la Conferencia Mundial de Sociedad de la Información reunió a 175 países bajo la premisa del cumplimiento de una serie de principios a los efectos de promover procesos destinados al desarrollo de la sociedad de la información para el año 2015.

Por otro lado, el eLAC 2007, fue la confirmación por los países de la región de comprometerse con los planes propuestos en la Cumbre Mundial de Sociedad de la Información y se configuró en una de las tres etapas del Plan de Acción de América Latina y el Caribe los restantes son eLAC2010 y eLAC2015.
El inicio del plan puede establecerse en el año 2005, donde se tomó conciencia y compromiso por parte de los Estados miembros de la región de fomentar y promover el desarrollo de la Sociedad de la Información en América Latina y el Caribe. La segunda etapa aparece ya en el año 2008 y tenía como objetivos primordiales, trabajar en las áreas de educación, infraestructura, salud, gestión pública, sector productivo y políticas y estrategias, también se tratan temas tales como entorno, acceso, entre otros.

Y finalmente el eLAC2015 destinado básicamente al fomento del aumento de cobertura de banda ancha.

La mayoría de las agendas digitales en Latinoamérica, se promueven a partir del año 2005 indudablemente influenciadas por la aplicación del proceso eLAC.
La primera agenda digital conocida en la región, o lo que se entendía por tal, se promovió en Brasil en el año 2001. Titulado Sociedad de la información en Brasil, y más comúnmente conocido como el Libro Verde, dicho material promovía la estrategia de Sociedad de la Información para ese país, y posteriormente se convirtió en el Plan Nacional de Banda Ancha.

Concomitantemente con Brasil, Argentina fue también uno de los principales propulsores de la Sociedad de la Información en Latinoamérica y el Caribe. Ya en el año 2000 se promulgó el programa de Sociedad de la Información. Posteriormente surge en el año 2009 la Agenda Digital Argentina con el objetivo de asentar el proceso en el país, proyecto que se modifica ampliando y marcando lineamientos más firmes en el año 2010, con el plan Argentina Conectada cuyo objetivo es ampliar la cobertura de Banda Ancha en el país argentino.

Este punto de partida, extendido por varios países de la región planteó la interrogante de la creación de órganos o instancias que proyecten, controlen y replanteen los objetivos fijados para el avance de los planes de Sociedad de la Información en sus respectivos países. Para el caso de Colombia se opto por un alto nivel de Jerarquía política lo que le permite ejercer en todos sus aspectos el rol de articulador estatal a los efectos del cumplimiento de los planes trazados, con la competencia asignada al Ministerio de Tecnologías de la Información y las Comunicaciones. En otros países han optado por dotar a dichas instancias de un segundo nivel de jerarquía como es el caso de una instancia viceministerial, o en su defecto un tercer nivel correspondiente a la creación de una oficina administrativa con competencias en el desarrollo, implementación y control de todo lo referente a la Sociedad de la Información y el cumplimiento de los objetivos propuestos en las respectivas Agendas Digitales.

Para el buen funcionamiento de las mencionadas instancias es necesaria la coordinación de diferentes factores, como: la creación de políticas y estrategias, adaptación de los marcos legales, coordinación de los sectores públicos y privados, financiamiento, cumplimiento de directivas planteadas por órganos de supervisión internacional, etc.

En función de la aplicación de los elementos antes mencionados, según la información publicada por CEPAL, la región se enfrenta a la situación de un grupo de países tales como: Argentina, Brasil, Chile, Colombia, México y Uruguay los cuales tienen agendas digitales que cumplen con los parámetros propuestos y pueden considerarse avanzadas, y el restante grupo de países, los cuales están en fase de implementación y en proceso de adaptación a los requerimientos propuestos.

2.2.a. Aspectos más relevantes de la evolución de la Sociedad de la Información en Chile y en Colombia.

La implementación de políticas de Sociedad de la Información en Latinoamérica, no pueden analizarse aisladamente del avance de las TIC y sus distintas fases de desarrollo.

Como consecuencia de esto, la primera etapa de implementación de este tipo de políticas refirió a la búsqueda de la disminución de la brecha digital, visto este fenómeno como aquella brecha que se genera entre personas que tenían acceso a dichas tecnologías y personas que no solamente no podían acceder a ellas por cuestiones socio-culturales. Esto genero que las políticas tuvieran como enfoque principal agotar los esfuerzos de los Estados a los efectos de combatir esas desigualdades.

En segunda instancia y ante el mayor desenvolvimiento de las redes de banda ancha y la mayor penetración en la sociedad de internet, esta herramienta se comienza a convertir en una plataforma útil a los efectos de la prestación de infinidad de servicios tanto públicos como privados, lo que generó que las políticas destinadas al desarrollo de la sociedad de la información no solamente tuvieran como objetivo el acceso a las tecnologías, sino también la modernización de la infraestructura, a los efectos de lograr la prestación de mayor cantidad de servicios y con mejor calidad para las personas.

Así ya a partir de 1990 se comenzaron a implementar políticas destinadas a aumentar la infraestructura tecnología y a financiar el acceso a las TIC, las mismas contaban con el desafío de superar las carencias sociales sufridas por muchos ciudadanos, así como las grandes extensiones de territorio.

Posteriormente, los Estados comenzaron a priorizar el acceso compartido o el acceso público, visto éste como la búsqueda de mayor acceso a las TIC por parte de los individuos, lo cual no solo buscaba el aumento de la población con manejo de tecnología (con lugares públicos que disponían de computadores o con subsidios económicos para facilitar la adquisición de los mismos) sino que tenía como objetivo también el despliegue de políticas educativas con la finalidad de instruir a la sociedad en el uso de estas herramientas. Algunos de dichos programas fueron: en Colombia COMPARTEL en 1998; en Chile en el 2000 el Programa Nacional de Infocentros Comunitarios; y en México en el año 2001 los Centros Comunitarios Digitales.

Este avance de la Sociedad de la Información en Latinoamérica, tenía naturalmente que ser acompañado por reformas legales que adaptaran el sistema normativo de cada uno de los países al contexto y realidad actual que se vivía. Así aparecieron en los distintos países normas que regularon: el documento y la firma electrónica (Colombia en 1999 y Chile en 2002), la factura electrónica (Chile 2004), los delitos informáticos (Chile 1993), etc.

El acceso a las TIC a nivel educativo siempre se constituyo en uno de los objetivos que acompañaron cada etapa de implementación de la Sociedad de la Información. Así se buscaba que en las escuelas, tanto los alumnos como los docentes tuvieran la posibilidad de acceder a internet, y de explotar

todo su potencial como herramienta educativa, por lo que con ese fin se implementaron planes nacionales como: La Red de Enlaces de Chile, en 1993, que posteriormente dio lugar a la creación del portal EducarChile en el año 2001, con la finalidad de dotar a los docentes de más herramientas para el desarrollo de la actividad pedagógica.

Otro de los objetivos que acompañó el fenómeno desde sus inicios fue el desarrollo del Gobierno Electrónico. Dicha actividad tenía como algunas de sus finalidades la implementación de tecnología en la labor diaria de los órganos del Estado, así como el aumento de la oferta de servicios prestados hacia la sociedad. En esa línea trabajó el gobierno chileno el cual en el año 2001 instaura el Instructivo Presidencial de Gobierno Electrónico como puntapié inicial, dando lugar posteriormente a: la aplicación de tecnología en la Administración Tributaria (Servicio de Impuestos Internos) con la implementación en 2003 de un sistema de declaración de impuestos a la renta; la realización de trámites online por parte de los individuos con el portal TramiteFacil; y a las Compras Estatales con el portal ChileCompra en el año 2003.

Ya avanzada la década del 2000, el avance del fenómeno y los resultados positivos que arrojó la utilización de las Tecnologías generaron políticas que buscaban la mayor profundización de algunos planes y objetivos trazados anteriormente ya sea en educación, gobierno electrónico y aumento de infraestructura tecnológica, y también generaron derivaciones en otras áreas aparentemente novedosas como eran la salud, el medio ambiente y la implementación de TIC en el sector productivo.

Con respecto a la infraestructura, las políticas no solamente buscaban la conectividad sino que avanzaban aun mas, con la búsqueda de aumentar el manejo diario de tecnología y la mayor oferta de aplicaciones para la sociedad.

Con este fin se crea en Colombia el plan ViveDigital, que comprendía la implementación de un proyecto federal de fibra óptica, y en Chile se crea el plan TodoChileComunicado el cual también tenía como objetivo el aumento de la cobertura de banda ancha.

El marco normativo siempre acompañó la evolución y se siguieron sancionando leyes que en esta instancia buscaban ya sea: reglamentar determinados sectores como las telecomunicaciones por ejemplo, así como la sanción de normas que promuevan el interés público. En esa línea se sanciona en el año 2009 en Colombia la Ley TIC, Ley N°1341 de 2009, la cual tenía como algunos de sus objetivos regulatorios: aumento de acceso y uso de TIC, promoción de la libre competencia, protección de derechos de los individuos, etc. También se sanciona en Chile la Ley N° 20.453 que determina la neutralidad de la Red.

Otro de los objetivos propuestos fue el incentivo a privados para mayor utilización de tecnologías en el sector productivo, en ese ámbito Colombia crea el programa MiPymeDigital, en búsqueda del desarrollo de las TIC con la unión de esfuerzos entre el sector público y el privado.

A nivel educativo se buscó intensificar el acceso a la tecnología, pero también se centraron los esfuerzos en el desarrollo de plataformas y aplicaciones de educación en línea. En este ámbito Colombia y Chile han trabajado profundamente logrando que varios millones de sus habitantes puedan acceder a capacitación online.

El gobierno electrónico siguió acompañando el desarrollo y siguieron surgiendo políticas que buscaban el aumento de la utilización de tecnología en la Gestión del Estado y una mayor oferta de servicios por parte del Estado a la sociedad. Colombia y Chile profundizaron sus medidas, logrando modernizar la gestión del Estado, lo que los fue colocando como pionero en los rankings mundiales de gobierno electrónico.

2.2.b. El caso de Uruguay: Agenda Digital 2011-2015

Con base en la Declaración de Principios de la Sociedad de la Información, Uruguay se plantea

a través de la sanción de su Agenda Digital para el periodo 2011-2015 la implementación de TIC como forma de afianzar su recuperación económica, aumentar su productividad, mejorar la gestión gubernamental, modernizar los servicios educativos, innovar, generar conocimiento y lograr mayores niveles de inclusión social, con el objetivo de obtener el mayor bienestar para todos sus habitantes.

Como primer objetivo en la agenda se encuentra lograr la conectividad a Internet para todos los habitantes de la República a través de la universalización de la banda ancha, con la finalidad de lograr mayor inclusión social.

El segundo objetivo propuesto consiste en la implementación de la Televisión Digital Interactiva, la cual proveerá al país de mejor infraestructura audiovisual y democratizará los contenidos en función del aumento en la cantidad de señales recepcionadas por la sociedad.

El tercer objetivo se centra en la implementación de TIC en la Educación, teniendo como piedra angular el Plan Ceibal (el cual permitió dotar a cada alumno de educación primaria de un computador personal) Uruguay busca profundizar la aplicación de tecnología en la educación, ya sea a través de la mejora de la infraestructura, fomentando la educación en línea, y el impulso de redes de investigación y redes académicas en línea.

El cuarto objetivo se centra en la Educación en TIC, con el objetivo de especializar y capacitar posibles recursos a los efectos de potenciar aun más la Industria de las TIC, lo que generará un aumento de puestos de trabajo y su consecuente repercusión en la economía del país.

Como quinto objetivo de la Agenda se busca el aumento de habilidades en TIC para los ciudadanos, fomentando la utilización de tecnología en la sociedad enfocada a la vida económica, social y cultural, lo que traerá como consecuencia la familiaridad con el sistema.

El sexto objetivo se centra en el aumento a través de la utilización de TIC de contenidos culturales a los efectos de dotar a la sociedad del acercamiento y conocimiento del Patrimonio Cultural Nacional.

El séptimo objetivo, busca la modernización de la gestión pública con base en la interoperabilidad de los productos y servicios gubernamentales y la simplificación de los trámites y servicios prestados.

El próximo objetivo fijado consiste en aumentar la interacción entre el ciudadano y el gobierno a través del desarrollo de la administración electrónica.
En la misma línea, Uruguay se plantea lograr un Estado integrado y que su actuación frente al ciudadano sea vista como una unidad. También se estipula como objetivo en la agenda la mayor utilización de TIC en la administración pública logrando un entorno confiable y eficiente que mejore la gestión del Estado.

El siguiente objetivo fijado por el Estado Uruguayo gira en la órbita de la Economía Digital con el fomento de iniciativas tendientes a desarrollar el comercio electrónico como forma de generar mayores ingresos y de diversificar mercados para las PYMES y así generar una mayor dinámica económica. En el mismo camino se apunta también a la promoción de la industria del software y contenidos digitales.

Los restantes objetivos, centran su preocupación en la implementación de TIC para la mejora de la gestión agropecuaria, el desarrollo de los servicios de salud a través de la implementación de la historia clínica electrónica y la creación de redes avanzadas de salud a nivel nacional, así como políticas destinadas al cuidado del medio ambiente y el uso responsable de TIC.

Estos objetivos forman parte de una política asumida por Uruguay a nivel país. La implementación gradual y el cumplimiento de varios de ellos en el periodo 2011-2015 han colocado a Uruguay en el lote de países Latinoamericanos que lideran los rankings de implementación de TIC en todos los niveles de la sociedad.

3. Sociedad de la Información en la actualidad y su vínculo con la protección de Datos Personales:

3.1. Marco Normativo en Europa y Latinoamérica.

El desarrollo de la sociedad de la información genera la necesidad de adaptar los distintos contextos normativos a la realidad actual. La modificación o adaptación de lo que se denomina como entorno habitador, da lugar a la aparición de nuevas normas que comienzan a regular la protección de ciertos derechos o aspectos que se generan como consecuencia de relaciones que comienzan a tejerse a través de las redes.

Tanto Europa en primera instancia como en Latinoamérica posteriormente se han sancionado normas tendientes a regular estas nuevas situaciones, normas que van desde la regulación de la factura electrónica, la protección de datos personales, delitos informáticos, gobernanza, entre otras.

Con respecto a la protección de datos personales, existió un fuerte compromiso y una política muy marcada a nivel europeo, con la sanción de la Directiva 95/46 del Parlamento Europeo, la cual reconoce al dato personal como un derecho propio de la persona e inherente a su personalidad y por tanto fija la necesidad de su regulación y la consagración de mecanismos tendientes a su protección por todos los Estados integrantes de la Comunidad Europea. Otra norma de especial relevancia que acompañó ese proceso de regulación y que fue sancionada con anterioridad por la comunidad europea es el Convenio N°108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos.[8]

Al día de hoy en Europa se continúa trabajando por parte del Parlamento Europeo con respecto a este tema y dicho marco normativo está siendo ajustado a los efectos de modernizar aún más todos los mecanismos de protección de datos personales.

Latinoamérica no se quedó atrás y con el influjo europeo comenzó la regulación de todos estos aspectos, lo que generó que varios países sancionen normas que refieran a la protección de datos personales, tales son los casos de Argentina, Chile, Colombia y Uruguay.

En el caso de Uruguay el tratamiento de datos personales se reguló a través de la Ley N° 18.331 sancionada en agosto de 2008 y su consiguiente Decreto Reglamentario N°414 del año 2009, siguiendo la línea ya marcada por la Directiva 95/46 del Consejo de Europa y consagrando la protección de datos personales como un derecho inherente a la personalidad humana. Uruguay ha logrado en agosto de 2012 la adecuación al sistema Europeo de Datos Personales lo que lo convierte en un país que reúne máximas garantías para el manejo y protección de datos de carácter personal, acarreando dicha adecuación consecuencias muy positivas no solo desde el punto de vista jurídico sino también desde la óptica económica y comercial.[9]

Posteriormente se ratifica por parte de Uruguay el Convenio N°108 del Consejo de Europa, lo que lo convierte en el primer país no integrante de la Comunidad Europea que ratifica dicho Convenio, marcando así una política y un compromiso muy firme en todo lo referente a Protección de Datos Personales.

8 http://www.datospersonales.gub.uy/inicio/noticias/de+avanzada+uruguay+se+adhirio+al+convenio+108 (Página visitada el 2 de mayo de 2013).

9 http://mjv.viegasociados.com/?p=232 (Página visitada el 2 de mayo de 2013).

3.2. Nuevos Desafíos de Protección de Datos Personale ante los avances en las TIC. Casos de BigData.

El avance del fenómeno Sociedad de la Información trae como consecuencia el aumento en las transferencias de datos y el manejo de grandes volúmenes de información, lo que genera la confección de grandes bases de datos y en función de las cuales se crean mecanismos tecnológicos que utilizan y relacionan dicha información generando así perfiles de los individuos utilizando los mismos con fines comerciales o de control, situación denominada comúnmente como BigData.

El manejo y procesamiento de dichos datos se ha convertido en una nueva oportunidad de negocio para empresas de gran porte así como para fabricantes y desarrolladores.

Una de las aristas más importantes del Big Data es determinar pautas de consumo de los individuos a los efectos de generar así mecanismos publicitarios con la intención de captar un mayor número de consumidores, con consecuencias muy importantes a nivel comercial y económico, pero con el riesgo de dañar la privacidad de los individuos. La información o rastros que los individuos van dejando a través de su camino por las redes y su posterior recolección ha pasado a convertirse en una riqueza invaluable para todos los operadores comerciales.

Tan importante es el procesamiento y manejo de estos datos que hasta se habla de un negocio de los datos, situación que ha pasado a convertirse en parte fundamental de la estructura empresarial de determinadas empresas a los efectos de obtener con ellos una ventaja competitiva que acarree un rédito más que importante desde el punto de vista económico.

Tales circunstancias han generado la preocupación por parte de las autoridades Europeas y de todo el mundo ya que ponen en riesgo la privacidad de los titulares de los datos y plantean el desafío de lograr un adecuado manejo y protección de los mismos a los efectos de no afectar los derechos de sus titulares.

La preocupación ha sido tal que en el mes de abril de 2013 la Agencia Española de Protección de Datos, ha generado una investigación a Google a los efectos de determinar si el gigante de Internet hace un correcto manejo de los datos de los ciudadanos españoles ya que existen a juicio de dicha autoridad determinados indicios de que dicha situación no ocurre. Esta se produce en función del cambio de políticas de privacidad implementado por Google en marzo de 2012. Dentro de los temas a investigar por parte de las autoridades se encuentra el manejo que Google hace de la información de los individuos, así como el periodo de conservación de la misma, la existencia de consentimiento de los titulares y garantías que los mismos tienen de oponerse a la entrega de su información y sus datos personales. [10]

La mencionada investigación cuenta con la colaboración de las Autoridades de Protección de Datos de Alemania, Francia, Holanda y Reino Unido lo que demuestra la preocupación de Europa sobre este tema y el desafío que se plantea respecto a la protección de la privacidad de los individuos.

10 http://www.eldiario.es/turing/BigData_0_120038458.html (Página visitada el 2 de mayo de 2013).

4. Conclusiones

A lo largo de este trabajo hemos intentado desentrañar y caracterizar al fenómeno Sociedad de la Información.

Como se ha podido apreciar es un fenómeno de difícil contextualización, análisis y conceptualización como lo son la mayoría de los fenómenos sociales que implican el cambio a una nueva era y los cuales repercuten en todos los aspectos de la Sociedad.

Hoy el mundo afronta la era de las Tecnologías de la Información y la Comunicación, su utilización ha cambiado la vida de los individuos y su mayor desenvolvimiento y expansión generará muchos beneficios para los países y sus habitantes.

Dichos cambios conllevan riesgos, y el mundo está trabajando a los efectos de minimizarlos y que ellos acompasen dicho avance, protegiendo los derechos de los individuos, promoviendo el mayor uso de la tecnología, y buscando generar mayor confianza en el sistema a través de políticas que logren que este fenómeno solo acarree consecuencias positivas para las personas.

El desarrollo de más tecnología y su utilización genera consecuencias a nivel social, cultural, educativo, de gestión pública, comerciales, económicas, entre otras, las cuales sin dudas pueden contribuir a la mejora en la calidad de vida de los individuos, la disminución de las desigualdades sociales y el respeto, garantía y ejercicio de sus derechos fundamentales.

CAPITULO III

GOBIERNO ELECTRÓNICO

Dr. Federico Abbadie

GOBIERNO ELECTRÓNICO

Dr. Federico Abbadie

1. Introducción

El tema de referencia nos presenta el desafío de relacionar dos temas de suma trascendencia y actualidad. Analizaremos el concepto y las características generales del gobierno electrónico, a la vez que reseñaremos las políticas de protección de datos, en tanto derecho fundamental tutelado a texto expreso, existentes en nuestro país, asumiendo el desafío de analizar el límite entre dichas políticas estatales las que en definitiva se presentan en pro de una mejora en las gestiones públicas.

En forma preliminar podemos afirmar que existe una directa conexión en lo que refiere a la protección de datos personales (en lo sucesivo "PDP") y la gestión de las políticas públicas a través de las Tecnologías de la Información y de la Comunicación (o indistintamente "TIC") las que son utilizadas fundamentalmente al servicio de los ciudadanos en un contexto de "Gobierno Electrónico"; lo antedicho lo es en virtud de una cotidiana aplicación y un frecuente manejo de tecnologías por parte del Estado que facilitan el acceso a la información y que en definitiva buscan optimizar la eficacia y la eficiencia en los servicios brindados a los ciudadanos, así como una mayor "democratización" de los sistemas públicos.

Estas TIC que venimos de señalar son utilizadas comúnmente tanto en el ámbito privado como en el público, operando como verdaderos canales de comunicación y consecuentemente de transmisión de datos. Esto provoca que naturalmente las administraciones estatales sean actualmente grandes recopiladores de datos personales, recogiéndolos y tratándolos al servicio de sus cometidos, con el desafío de preservar el derecho humano fundamental inherente a la persona humana[1].

El derecho de Acceso a la Información Pública (AIP), la Interoperabilidad de los organismos estatales, los datos abiertos, la transparencia del mercado financiero, las inspecciones realizadas por el fisco en uso de su potestad inspectiva, son algunos de los escenarios e instrumentos que plantean tensiones, abriendo interrogantes sobre cuándo y cómo legitimar una colecta inicial de datos personales por parte del Estado, pero también una cesión o comunicación posterior de datos en contextos de una administración electrónica.

La necesaria vinculación y el consecuente desafío que plantean a diario estos conceptos claramente lo vemos reflejado ya en las propias definiciones de Gobierno Electrónico y de Protección de Datos que existen en los diferentes niveles.

De esta forma podemos destacar que dentro de la Carta Iberoamericana de Gobierno Electrónico[2](en adelante indistintamente "Carta Iberoamericana de Gobierno Electrónico" o simplemente "la Carta") un concepto específico de Gobierno Electrónico que se proyecta especialmente hacia una preservación de la PDP, considerándola como un verdadero derecho a tutelar. En este sentido el art. 3° de la referenciada Carta lo define como: "(...) el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos (...)".

1 La Protección de Datos Personales es considerada un Derecho Humano inherente a la persona humana comprendido en el art. 72 de la Constitución de la República Oriental del Uruguay. Referencia expresa del art. 1° de La ley N° 18.331, Ley de PDP.

2 "Carta Iberoamericana de Gobierno Electrónico", aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado (Pucón Chile 31/05/2007 y 01/06/2007) - Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno (Santiago de Chile (10/11/2007) – Resol. N° 18 de la Declaración de Santiago.

En armonía con la definición que acabamos de exponer, y siguiendo con el texto reseñado encontramos en la misma Carta unos artículos más adelante (art. 18°) una protección a texto expreso de los Datos Personales. Al efecto esta norma especialmente detalla que: "Se reconoce el derecho de todo ciudadano de solicitar ante los organismos competentes la actualización, la rectificación o la destrucción de aquellos datos contenidos en registros electrónicos oficiales o privados, si fuesen erróneos o afectasen ilegítimamente sus derechos (...)".

Asimismo y en sintonía con las definiciones previstas en la Carta, se proyecta una garantía de protección atendiendo a que se detalla la obligación de asegurar a todo ciudadano el derecho de acceso a la información y a los datos que sobre sí mismo o sobre sus bienes consten en registros oficiales o privados, con las excepciones que justificadamente se establezcan, así como a facilitar el conocimiento del uso que se haga de dichos datos y naturalmente su finalidad.

Tanto las definiciones que venimos de exponer así como el planteo de la relación existente entre Gobierno Electrónico y PDP, dejan en evidencia la vigencia y el desafío actual de las autoridades estatales de encontrar las fórmulas racionales y legitimas en cada caso, a fin de evitar que un avance pujante y necesario del gobierno electrónico se deslice hacia un descuido o avasallamiento del resguardo o tutela jurídica construida alrededor de la protección de datos personales y su especial preservación como un derecho humano fundamental.

2. Gobierno Electrónico y Protección de Datos Personales en Uruguay

Preliminarmente al abordar el tema en análisis, definiremos el concepto de Gobierno Electrónico y de Protección de Datos Personales dentro de un marco jurídico nacional, para lo cual citaremos normas internas de nuestro Estado las que sin perjuicio de destacarse por su fuerza y valor en el ámbito nacional ingresan en un contexto internacional de políticas proteccionistas del derecho a la autodeterminación por un lado y de implantación de políticas públicas o estatales por el otro, lo cual desde ya adelantamos es de suma trascendencia dado que en el marco de una sociedad de la información las fronteras políticas no necesariamente coinciden con las tecnológicas y mucho menos con las regulatorias de cada país.

A efectos de definir el concepto de un Gobierno Electrónico nuestro derecho prevé el Decreto Nº 450/009[3], el cual expresamente se titula: "Gobierno Electrónico en Red. Se aprueba el documento Principios y Líneas Estratégicas", y en el que se define expresamente al Gobierno Electrónico en base a lo dispuesto en la Carta Iberoamericana de Gobierno Electrónico (Pucón – Chile 2007)[4] a la cual ya hemos hecho referencia, establece que: "Gobierno Electrónico es el uso de las tecnologías de la información y de la comunicación (TIC) en los órganos de la Administración Pública para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.

En lo que respecta a la protección de datos personales, Uruguay ha hecho una gran labor legislativa reconociendo expresamente en una norma de carácter general y abstracto a la protección de datos personales como un verdadero derecho fundamental inherente a la personalidad humana, ya reconocido genéricamente en el artículo 72 de la Constitución de la Republica. La protección de datos personales considerada como un derecho humano fundamental, es reconocida a texto expreso a través de la Ley N° 18.331, de 11 de agosto de 2008 y su Decreto reglamentario N° 414/009,

3 Véase el Decreto del Poder Ejecutivo N° 450/009, de 28 de setiembre de 2009.

4 Carta Iberoamericana de Gobierno Electrónico. Ob. Cit.

de 31 de agosto de 2009[5]. La regulación del derecho de protección a la intimidad inserto en una concepción proteccionista del derecho a la autodeterminación informativa del individuo, responde a los lineamientos regulatorios de origen europeo, los que han encuadrado de forma excepcional en nuestro ordenamiento jurídico por haber sido fuente de inspiración más remota de la construcción del derecho nacional y haber acompasado con políticas legislativas que acompañan los niveles internacionales de PDP.

Lo que viene de expresarse, cobra gran relevancia con la reciente aprobación de la Ley N° 19.030[6] de fecha 27 de diciembre de 2012 que posiciona a nuestro país como el primero que sin pertenecer a dicho continente ha sido invitado por el Consejo de Europa a suscribir un Convenio en mérito a sus avances en la defensa del derecho a la protección de datos personales. La referenciada ley aprueba el Convenio N° 108 del Consejo de Europa: "para la protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal de 28 de enero de 1981 adoptado en Estrasburgo y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001", posicionado a nuestro país a la par de los países europeos en la materia.

El desafío será plantear el tema a fin de interiorizar ambos conceptos y efectuar una reflexión que nos conduzca hacia la armonización de la implementación y próspero desarrollo de un gobierno electrónico, en una sociedad que a través de la informática ha podido almacenar, recoger y utilizar todo tipo de información haciendo cada vez más necesario un verdadero control en el derecho de la intimidad y especialmente en la protección de datos personales.

3. Nociones y alcance del gobierno electrónico, sus rasgos esenciales y la relación directa con la administración electrónica, las TIC y el Big Data.

El concepto de Gobierno Electrónico debe de ser precisado a efectos de dar un marco conceptual sobre el cual podremos reflexionar y especialmente sobre el cual podemos analizar el alcance e implicancias y especialmente en este desafiante análisis, la coexistencia con el derecho a la protección de datos personales. Es precisamente a estos efectos que nos remitimos a las definiciones previstas en la Carta Iberoamericana de Gobierno Electrónico, la que identifica y particularmente caracteriza un derecho al Gobierno Electrónico como un precepto fundamental y esencial, para los habitantes de los distintos Estados. En este sentido, la Carta detalla que la implantación y naturalmente la gestión del Gobierno Electrónico hace al reconocimiento por parte de los miembros participantes (Estados Iberoamericanos) al derecho de los ciudadanos a relacionarse electrónicamente con sus Gobiernos y Administraciones Públicas, reforzando los principios básicos de la democracia o a efectos de contextualizarnos dentro de la sociedad de la información, como ha sido caracterizada la sociedad actual, una verdadera "democracia electrónica" como la misma Carta nos ayuda a reflexionar.

Será de esta forma en que a través del uso e implementación de las Tecnologías de la información y Comunicación en búsqueda de producir una mejora en la prestación y en definitiva en la gestión de las políticas públicas que se habla de la administración electrónica como un sinónimo del gobierno electrónico.

Un claro ejemplo de la asimilación de ambos términos surge a texto expreso de la ya citada Carta

5 El Decreto del Poder Ejecutivo N° 414/009, de 31 de agosto de 2009, reglamentó la Ley N° 18.331 (LPDP).

6 Véase Ley Nº 19.030, de 12 de diciembre de 2012. Sitio web: www.parlamento.gub.uy

Iberoamericana, donde se manifiesta que : "A los efectos de la presente Carta Iberoamericana se entienden las expresiones de "Gobierno Electrónico" y de "Administración Electrónica" como sinónimas (...)" , asociando en forma inmediata el uso de las TIC en ambos conceptos, " (...) ambas consideradas como el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos. Todo ello, sin perjuicio de las denominaciones establecidas en las legislaciones nacionales."

Por tanto, hemos visto que es indistinta la forma en la que se haga referencia en lo que respecta al uso de las TIC en las Políticas de Estado, ya sea que hablemos de un gobierno electrónico, o de una administración electrónica, utilizando los preceptos técnico jurídicos del derecho público, mientras que se haga referencia a la interacción que se genera mediante el uso de las TIC entre el gobierno, los ciudadanos, las empresas y en general la sociedad toda. En el mismo sentido que venimos de exponer la interacción que se genera entre los distintos actores involucrados, corresponde citar al autor Ricardo Sebastián Piana, quien [7]expresaba que: "(...) En el ámbito estatal, la introducción de las TIC forma parte de la agenda de todo gobierno, pues son una herramienta fundamental y facilitadora de los cambios necesarios para la modernización del Estado.

A través de las TIC se crea una nueva interacción entre los gobiernos, en todos los niveles, y sus ciudadanos, organizaciones y empresas, generando el surgimiento de una nueva disciplina llamada Gobierno Electrónico (GE) o e-government. El GE se basa en un modelo organizacional de arquitectura más horizontal, empírico y endógeno, que vincula y permite el acceso y la interoperatividad sistémica de la información de las diferentes instituciones del gobierno.1 Esta nueva rama tiene como objeto optimizar, a partir del uso de las TIC, las interacciones entre gobiernos y entre gobierno y los diferentes actores de la sociedad civil (...)".

El uso de las TIC en las políticas de la administración pública hacen que el Estado al igual que los particulares, reconozcan el valor de la información que en la actualidad tiene en sí misma. Este cúmulo de información o de datos que los estados manejan respecto de sus ciudadanos, puede ser denominado como un verdadero "Big Data" o "grandes datos" expresión que ha sido adoptada del idioma Inglés y que básicamente refiere al cúmulo o almacenamiento de grandes conjuntos de datos. Es clave que cuando estos datos obran en manos de las administraciones públicas, necesariamente deben ser tutelados, esto por la esencia misma de un estado social que protege a sus ciudadanos, máxime cuando se trata de datos de corte personal, en donde entre otros principios rectores el previo consentimiento informado y la finalidad que se le dé a los mismos, deberán operar como verdaderos lineamientos a efectos de protegerlos como un derecho humano fundamental y evitar que sean utilizados por las redes comerciales que en torno a estas grandes bases de datos existen y precisamente el Estado es encargado de controlar .

4. Desafíos de las Administraciones Públicas en las políticas del Gobierno Electrónico.

Nuestro país conjuntamente con Chile y Colombia lideran actualmente en materia de Gobierno Electrónico en Latinoamérica. Uruguay ha efectuado en los últimos años un gran esfuerzo en lo que refiere a infraestructura, en pro del desarrollo e implementación de políticas públicas a través del uso de las TIC, para los servicios a prestar al ciudadano.

En nuestro país AGESIC es el organismo a cargo de llevar a cabo la implementación de estas políticas relacionadas con las TIC. El organismo fue creado en diciembre de 2005 con la denominación "Agencia

7 Piana, Ricardo. "Gobierno electrónico, organización en red y gobernabilidad democrática", Derecho Político – Facultad de Ciencias Jurídicas y Sociales Universidad Nacional de La Plata.

para el Desarrollo de Gobierno Electrónico" (Artículo N° 72 - Ley N° 17.930)[8] y su funcionamiento fue reglamentado en junio de 2006 (Decreto N° 205/006), normas que posteriormente han sido modificadas parcialmente. Tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las Tecnologías de la Información y la Comunicación[9].

Es menester el rol de las administraciones estatales en tanto por un lado deben asegurar a los ciudadanos una debida protección en sus derechos y libertades y por otro son a su vez grandes recopiladores de datos, a los cuales deben de proteger y dar la utilidad final para la cual en definitiva han sido recolectados. Esa desafiante armonía entre la utilización o manipulación de información personal por un lado y la gestión de servicios eficaces y eficientes para los habitantes del estado, necesariamente obliga a la utilización de sistemas de seguridad de información que resguarden estos derechos fundamentales mientras que a la vez apoyen un pujante manejo informatizado de servicios al ciudadano.

La armonización planteada que podemos traducir en una vinculación entre la protección de datos personales y el gobierno electrónico, se ve normativamente plasmada a texto expreso en la Carta Iberoamericana, reconociendo expresamente el derecho de todo ciudadano de solicitar la actualización, rectificación e incluso la destrucción, de datos existentes en registros electrónicos que ilegítimamente afectasen sus derechos. Esto asume una mayor relevancia en un contexto internacional, dado que el instrumento ha sido adoptado por diversos países de América Latina, y especialmente cobra relevancia en aquellos casos donde la normativa interna no prevé expresamente disposiciones al efecto. En el caso de nuestro país, las disposiciones de la Carta Iberoamericana se ven reforzadas jurídicamente con leyes y decretos que conforman nuestro derecho interno, que garantizan la protección de datos personales y fijan lineamientos de gestión del gobierno electrónico.

Naturalmente el hecho de que Uruguay haya adherido en forma activa a la carta, y adicionalmente haya dictado normativa específica a tales fines, sin perjuicio de los preceptos constitucionales ya existentes, implica que nuestro país ha enfocado sus políticas hacia una mejora participativa en el acceso a la información, valor de gran entidad en el contexto de una sociedad moderna. Lo que venimos de señalar, debe de ser analizado en un sentido amplio de acceso a la información comprendiéndolo en forma genérica como el "derecho a obtener datos", ya sea que se trate de información pública que obre en manos del Estado, o sea que se trate de datos personales que identifiquen a una persona directa o indirectamente o de cierta forma la hagan identificable[10] sea que éstos se encuentren en manos de particulares o del propio Estado.
En este sentido, nuestro país ha hecho un gran esfuerzo por incorporar disposiciones normativas tendientes a la optimización e incorporación de procesos que faciliten el acceso a la información pública, esto es en un sentido genérico, el acceso a la información que obra en manos del Estado. Estas políticas en pro de la transparencia y la información en sentido amplio[11], han de ser reflejadas en la especial tutela que existe de los datos personales, lo que como ha sido reseñado forman parte de una protección especial y son reconocidos en forma expresa como derecho humano fundamental, con una tutela administrativa a manos de la Unidad Reguladora y de Control de Datos Personales (creada por la Ley N° 18.331) y eventualmente por un proceso judicial sumarísimo a cargo de los órganos de justicia competentes.

Los datos públicos han pasado en la sociedad contemporánea a ser considerados como una entidad con verdadero valor en sí misma, a ser reutilizados por la ciudadanía y la sociedad civil en general. Pero estos datos no necesariamente deberían ser datos personales, sino que se trata de datos para

8 El parágrafo primero de la citada Ley Nº 17.930 establece respecto a AGESIC que: "(...) Su objetivo será procurar la mejora de los servicios del ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones. Los cometidos asignados por el Decreto Nº 225/000, de 8 de agosto de 2000, así como sus complementarios y modificativos, serán reasignados a esta Agencia (...)".

9 Véase la página web de AGESIC: www.agesic.gub.uy.

10 A estos efectos se debe tener presente el concepto de "dato personal" detallado en el artículo 4º literal D) de la Ley N° 18.331 "(..) Definiciones - A los efectos de la presente ley se entiende por: (...) literal D) Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables (...)".

11 Téngase presente el derecho de Habeas Data, ha sido clasificado doctrinariamente como propio e impropio, según se trate de información objetiva o subjetiva, para el caso de la ley 18.331 se hace referencia al Habeas Data propio.

el uso y su eventual reutilización en la comunidad a la que involucra. A tales efectos se puede hacer cita o remisión al sitio web uruguayo "datos.gub.uy"[12], creado con el fin de presentar un Catálogo Nacional de Datos Abiertos, el que en síntesis busca facilitar el acceso de los ciudadanos a los datos públicos, fomentando su reutilización y posterior desarrollo en nuevos servicios y productos, incentivando a los distintos organismos estatales a publicar sus datos en formatos abiertos y ofrecer espacios de coparticipación ciudadana, en definitiva nuevas instancias generadas a partir del pujante desarrollo del gobierno electrónico.

5. Necesariedad de una interconexión en los sistemas de información y su relacionamiento directo con la protección de datos personales como la preservación de un derecho fundamental.

Es claro que esta recolección de datos por parte del Estado y que encuadra dentro de los preceptos del Gobierno Electrónico, se encuentran en un punto de análisis complejo, encontrándose inserta bajo un manto del "ser" jurídico y por tanto necesariamente responderá, al menos a priori, a delimitaciones o porciones territoriales y aún a divisiones por determinados servicios. Lo expuesto es en especial atención a las disposiciones existentes en nuestra Constitución, norma de máxima jerarquía en nuestro sistema jurídico e inspiradora de un sinfín de disposiciones normativas que han sido dictadas siguiendo sus preceptos, tal como sucede en el caso de la Ley de Protección de Datos Personales. En lo que refiere a "descentralización", comprendiendo a este concepto como un "desplazamiento de competencias", la Constitución esboza básicamente dos tipos diferenciados, el primero relativo a una descentralización por servicios y el otro con un antecedente histórico más político, es el fraccionamiento territorial. En este sentido, veremos que un claro reflejo de la descentralización por servicios se proyecta en las disposiciones de los artículos 197 y 198 de la Constitución[13], donde los órganos dotados de determinada autonomía o independencia se ven sujetos a determinados "controles", aunque sin dependencia jerárquica del gobierno central. En el caso de la descentralización por territorios, actualmente regulada por la Ley N 18.567 (conocida comúnmente como ley de "Municipios o Alcaldías"), también existen en este ámbito determinados controles del gobierno central, (reiteramos, controles y no sometimiento de jerarquía orgánico administrativa) y un claro ejemplo de ello se refleja en las disposiciones del artículo 300 de nuestra Constitución[14].
Lo que venimos de exponer no es sino una breve referencia a la existencia de disposiciones normativas que muchas veces, y casi sin considerarlos alcanzan a la implementación de una verdadera gestión de Gobierno y naturalmente también a las de gobierno electrónico, y especialmente hacen a la interconexión entre las distintas reparticiones estatales, las cuales son muchas veces divisiones cuasi teóricas para los ciudadanos, lo que naturalmente dificulta el acercamiento y fundamentalmente la participación ciudadana. Esto cobra relevancia cuando pensamos que nuestros datos pueden ser tratados o utilizados por todo el conjunto de reparticiones estatales y aún nos indignamos cuando en una oficina del Estado nos piden datos que otra oficina del Estado nos dio o a la cual ya le han sido entregados. Muchas veces la realidad práctica inspirada en la descentralización normativa de origen constitucional y legal que hemos brevemente reseñado, hace que esto no funcione de esta forma, dificultando procesos de interconexión estatal y operando como un verdadero desafío en las políticas y gestión electrónica.

12 Véase página web: datos.gub.uy (Catálogo de datos abiertos).

13 Véase artículos 197 y 198 de la Constitución de la República Oriental del Uruguay.

14 Véase el ejemplo de contralor establecido en el artículo 300 de la Constitución de Republica Oriental de Uruguay : "(...) El Poder Ejecutivo podrá apelar ante la Cámara de Representantes dentro de los quince días de publicados en el "Diario Oficial", fundándose en razones de interés general, los decretos de los Gobiernos Departamentales que crean o modifican impuestos. Esta apelación tendrá efecto suspensivo (...)".

Claro es que la intención no es la de discutir preceptos constitucionales los cuales sin lugar a dudas, hacen a la esencia de un sistema republicano de gobierno, sino el de reflexionar sobre un punto de especial magnitud sobre el cual la colectividad civil deberá trabajar en conjunto para encontrar la mejor forma de llevar a cabo un desarrollo para el gobierno electrónico interconectado al servicio de la ciudadanía a través del uso de las tecnologías de la información y comunicación, cooperando en todos los ámbitos de descentralización existentes, en un único compromiso de gestión y protección de datos con carácter integral.

Más allá de la cuestión que venimos de señalar, es importante reflexionar sobre algo que ya hemos mencionado y se trata de la información que obra en manos o en poder del Estado, punto sumamente trascendente el cual en la actualidad es regulado normativamente por la Ley N° 18.381 de 17 de octubre de 2008 (Ley de Acceso a la Información Pública)[15], y necesariamente decantar en ese mismo razonamiento qué cantidad o porción de esta información refiere a datos relativos a sus habitantes a efectos de imaginar la cantidad de datos personales que maneja este gran aparato de gestión. Desde el momento en el que comenzamos a vivir somos registrados con una identificación, detallando dónde y cómo nacemos; se confecciona un acta de nacimiento determinando la fecha, la hora, el sexo y lugar donde la persona ha nacido. Posteriormente y durante el transcurso de toda la vida seguimos realizando exámenes, chequeos, inscripciones y aún adoptando determinadas conductas de consumo o desarrollo que son gestionadas o tramitadas en algún punto por o ante el Estado.

Es evidente por tanto que la administración del Estado, necesariamente va a gestionar o manejar datos de sus ciudadanos, básicos éstos en principio para poder convivir sanamente en un Estado Social de Derecho, interrelacionándonos con otras personas. Es importante también recordar en este contexto la cantidad de datos que entregamos al aparato administrativo del Estado y que muchas veces refieren a datos considerados como "sensibles"[16] como lo serán los de salud o sexualidad y que por tanto se espera sean tratados con la confidencialidad y finalidad para la cual han sido entregados. Estos también formarán parte de los datos personales que maneja la administración y a los cuales será trascendental dar una finalidad ajustada, dotada de una serie de medidas de seguridad acordes al caso, que compatibilicen armónicamente con la protección de datos que el propio Estado debe garantizar a sus ciudadanos.

Todo este cúmulo de información a la cual hemos simplemente hecho una breve referencia se encuentra parcialmente almacenada actualmente en documentos con soporte papel, lo que no quita y por el contrario hace a la esencia del Gobierno Electrónico al cual hemos estado haciendo referencia, al hecho de que existan respaldos de dicha información en soportes o formatos digitales e incluso que únicamente existan en un mundo electrónico, con un soporte o respaldo ofimático, en sentido amplio. Esta multiplicidad de formas y soportes en que se almacenan los datos, la forma en que los ciudadanos pueden acceder a ellos y los mecanismos y procedimientos para lograrlo, son tarea de una gama de ciencias a la cual el derecho naturalmente no es ajeno, sino por el contrario debe de estar actuando permanentemente en resguardo de los derechos fundamentales del ser humano. Es por tanto un desafío interdisciplinario el de lograr esta armonización a la cual hemos hecho referencia entre el derecho fundamental a proteger los datos personales y la de lograr una implementación compartida entre el Estado y el ciudadano para la gestión, funcionamiento y desarrollo de un buen gobierno electrónico.

Está vigente aún dentro de los desafíos a resolver en nuestro colectivo social, el hecho de pensar

15 Por más referencias véase la Ley Nº 18.381 publicada en el Diario Oficial el día 07 de noviembre de 2008 sitio web: www.parlamento.gub.uy la que en su artículo primero establece como objeto de la ley que: " (Objeto de la ley).- La presente ley tiene por objeto promover la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública (...)".

16 De conformidad con lo dispuesto en el art. 18 de la LPDP se entiende que datos sensibles son : "(...) Artículo 18 - Datos sensibles.- Ninguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. (...) Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual (...)".

e incluso sostener y adaptarse en los hechos a que la información personal que obra en manos de la administración electrónica sea gestionada y tratada en formatos digitales, adaptándonos a utilizar estos soportes de forma tal que haga innecesario reincidir en problemas prácticos que muchas veces acarrea el soporte papel. Para ello el desafío como viene de expresarse será un desafío colectivo, por un lado la administración o gestión del gobierno electrónico, para la cual y dentro de la cual el ciudadano deberá contar con un rol activo participando en su construcción y naturalmente el gobierno abriendo los canales necesarios a tal finalidad. Pero a la vez el conjunto gobierno-ciudadano deberá actuar colaborando con la tarea de acortar la "brecha digital" existente dentro de la sociedad de la información, capacitándose, preparándose, dando a conocer cuáles y qué derechos existen y dónde éstos puedan ser ejercidos y en su caso bajo qué condiciones, fomentando en definitiva la participación activa en pro de un desarrollo favorable e igualitario para todos los habitantes.

Tanto el concepto de gobierno electrónico, como el de protección de datos personales se encuentran arraigados en nuestro marco jurídico. Claro ejemplo de ello son las disposiciones normativas existentes a nivel nacional, tanto sea por la existencia de decretos, leyes y aún de disposiciones constitucionales[17]. Es menester sin embargo cuestionarse si estas diversas disposiciones normativas se encuentran arraigadas en nuestra cultura ciudadana o si forman parte activa en el colectivo social dentro del cual vivimos. Por su parte es también trascendente analizar el marco en el cual estos conceptos encuentran un punto en común, produciendo determinadas consecuencias o efectos que repercuten en la vida cotidiana y adquiere por tanto un tenor jurídico de tipo activo que traspasa las disposiciones meramente declarativas, a fin de evitar incurrir en normas meramente enunciativas que inevitablemente no produzcan efecto alguno.

6. Maximización en la eficacia de los cometidos estatales y el rol del Servidor Público en el Gobierno Electrónico, dentro de un contexto de democratización e integración electrónica

El concepto de gobierno, puro y simple puede parecer a priori un concepto laudado a nivel jurídico-doctrinario, y aún puede ser un concepto ampliamente admitido a nivel social. Sin embargo el hecho de pensar en un concepto actualmente, agiornado a la vida diaria de todos los habitantes, inserto dentro del nuevo paradigma colectivo de una verdadera sociedad de la información, donde el uso de las tecnologías ya se trate de telefonía móvil, computadores o cualquier otro dispositivo tecnológico, utilizado en forma directa o indirecta, nos enfrenta necesariamente con una nueva modalidad de gestión de políticas de Estado, una nueva forma de pensar en el concepto de gobierno y encausarnos directamente en la noción de tecnologías aplicadas a la gestión y desarrollo de la administración del Estado, esto es pensar en un Gobierno electrónico integral, donde no solo se garantice la tutela de los derechos fundamentales, sino que activamente se cumpla de forma ejemplar con la protección de los mismos.

Esto es claro en tanto es el Estado quien lleva adelante determinadas actividades para dar cumplimiento a fines que lo caractericen como un verdadero estado social y de derecho a través de sus componentes orgánicos tales como lo son los tres poderes (Poder Ejecutivo, Judicial y Legislativo), los organismos descentralizados (por servicios o territorio) según hemos señalado oportunamente, entre otros. Dentro de estos cometidos a los que el Profesor Sayagués Laso ha clasificado en cuatro grandes grupos podemos encontrar los "servicios esenciales" o necesariamente estatales, a los

17 Véase citas a la LPDP, al Decreto Nº 414/009 y disposiciones Constitucionales citadas ut supra.

que al decir del profesor Jose Korzeniak[18] : (...) No concebimos el Estado sin que realice por si estas tareas y no las imaginamos cumplidas por particulares (...)": los "servicios públicos" los que si bien pueden llegar a ser desempeñados por particulares, a través del proceso de "concesión pública", se trata en principio de una actividad que corresponde al Estado y se identifican dado que se trata de necesidades colectivas básicas para la población. Asimismo dentro de esta clasificación encontramos a los "servicios sociales", los que si bien asumen un gran rol para la población el Estado los realiza en concurrencia con particulares (claro ejemplo de lo que sucede en nuestro país con la educación) y finalmente encontramos a los "servicios comerciales e industriales" los que Sayagués Laso[19] referenciaba como "(...) actividades privadas a cargo de la administración (del Estado) (...)", algunas en forma de monopolios y otras no.

Estas clasificaciones de los diferentes cometidos estatales hacen directamente una referencia a la participación de los particulares en las actividades del Estado así como a la realización de tareas que necesariamente (y exclusivamente) serán ejercidas por el Estado. Esos cruzamientos de información que necesariamente deben existir a efectos de llevar adelante cualquier gestión pública deben ser cautos en tanto no se debe incurrir en un traspaso excesivo de información que vulnere los derechos de los titulares a la vez que obstruya el normal desarrollo de los cometidos estatales a través de una gestión del gobierno electrónico.

El uso de las tecnologías de la información y comunicación en la gestión de los distintos cometidos y aún servicios prestados por parte del Estado, necesariamente nos lleva a reflexionar sobre la tutela o protección de determinada información de carácter personal en pro de garantizar el derecho a la autodeterminación informativa.

El encuentro entre la protección de datos personales y el gobierno electrónico, no es algo ajeno a la realidad actual en la que vivimos. Los estados modernos manejan mucha información automatizada, lo que implica la existencia de un valor muy importante en manos del aparato estatal y naturalmente un delgado margen en el que aparecen e interactúan activamente los datos personales. Esta información pudo haber sido obtenida en forma directa por el propio titular de los datos o por el cruzamiento de datos o "profiling" que aún de forma inconsciente el Estado puede llegar a realizar cruzando datos recabados en distintas instancias o esferas de interacción con sus ciudadanos, respetando siempre el principio de finalidad, consagrado en nuestro país a texto expreso en el artículo N° 8 de la Ley N° 18.331.

La expresión teórica de que nuestros datos se encuentran en grandes bancos donde se almacenan datos (Big Data), parece ajena a lo que sucede a diario y casi que sin imaginarlo, cuando efectuamos una búsqueda en algún servidor de la web, cuando utilizamos teléfonos móviles, intercambiamos correos electrónicos, usamos una tarjeta de crédito, activamos un GPS, o aún actualizamos fotos de perfiles en redes sociales, estaremos entregando parte de nosotros, un verdadero cúmulo de datos, huellas digitales y registros que ofrecen una información muy valiosa y cuya captación es la ambición de muchas corporaciones con fines de lucro. La enorme cantidad de datos que generan empresas y usuarios, ha experimentado un crecimiento voluminoso que requiere su análisis para obtener ventajas competitivas, pero también un marco regulatorio que acompañe estos procesos. El Big Data que puede estar en manos de un particular, también puede estarlo en manos del Estado, solo que con una finalidad ya no comercial, sino de gestión de políticas públicas, para lo cual como hemos dicho deberá actuarse como la mayor de las cautelas en lo que hace a la finalidad de los datos y especialmente al previo consentimiento informado del titular y las medidas de seguridad que al efecto deberán ser tomadas.

Estas grandes bases de datos en manos de las administraciones públicas a las que podemos identificar como Big Data, comprometen de forma activa a un buen manejo de los mismos y consecuentemente deben ser tratados con el mayor y mejor control en lo que hace al tratamiento de estos datos, ya sea

18 Korzeniak José. "Primer Curso de Derecho Público – Derecho Constitucional". Segunda Edición FCU, año 2002, págs. 291 y 292.

19 Véase página web: datos.gub.uy (Catálogo de datos abiertos).

frente a otros particulares o aún frente a otros estados, especialmente en lo que hace a la protección del derecho a la autodeterminación informativa.

7. Proyecciones del gobierno electrónico y la protección de datos personales y el especial desafío de la satisfacción y protección de sus habitantes.

Esta relación entre el gobierno electrónico y la protección de datos personales, puede llegar a ser paragonada en cierta medida con lo que sucede entre el comercio electrónico y la protección de estos derechos fundamentales, lo antedicho lo es en función al uso legitimo de dicha información, el tratamiento adecuado y especialmente a la finalidad para la cual estos datos fueron aportados. Obviamente que en lo que hace al uso por parte de los particulares de bases de datos personales, necesariamente debe de ser controlado y regulado por el Estado, esto en atención a los propios cometidos que hemos reseñado y aún los fines del Estado como una organización democrática, casi comparable con lo que sucede en materia penal, donde es el Estado el que tiene potestades punitivas o sancionatorias (Jus Puniendi). Esta potestad regulatoria por parte del Estado y esencialmente proteccionista de todos sus habitantes, hace aún más compleja la relación entre el Gobierno Electrónico y los derechos fundamentales de intimidad y privacidad, dado que el compromiso de buen uso y manejo de esta información se ve redoblado cuando es el propio Estado quien está manejando este tipo de información.

Esta relación entre el comercio electrónico y la protección de datos que venimos de señalar no debe ser confundida con el tratamiento de datos en manos del Estado y mucho menos del tratamiento de datos en la implantación o desarrollo de políticas en el marco de un gobierno electrónico. Esto parece muy claro cuando hablamos de particulares como personas físicas que manejan bases de datos personales, pero no debemos olvidar que la complejidad práctica surge de la propia realidad, donde muchas veces son verdaderas corporaciones transnacionales las que manejan estos datos impulsadas con un fin de lucro, donde la persona o individuo dotado de una serie de derechos especialmente protegidos no necesariamente se consideran una premisa en el negocio para el cual manejan estos datos.

El Estado, especialmente en la implementación de políticas de Gobierno Electrónico las cuales por excelencia serán a favor de los individuos, debe principalmente tutelar los derechos de autodeterminación y hacer un fuerte hincapié en el buen uso, finalidad y tratamiento de estos datos que necesariamente debe de manejar. Este equilibrio, bastante complejo de alcanzar en la práctica, deberá necesariamente estar abocado hacia la conciliación de derechos básicos para la implementación y desarrollo de una excelente gestión electrónica dirigida únicamente al ciudadano dándole la garantía de que sus datos serán preservados, actualizados y eventualmente eliminados en la forma previamente pactada, dando información necesaria y completa que facilite éste no tan nuevo relacionamiento; conceptos todos éstos que refuerzan la moderna noción de democracia participativa y hacen incrementar sustancialmente mejorando la confianza y relación entre el gobierno y la ciudadanía.

No debemos olvidar que todos formamos parte del Estado, claramente no en un sentido meramente orgánico, pero si en una acepción político jurídica del término. Es por esto fundamental que la protección de datos personales deberá ser uno de los pilares en la implementación de cualquier gestión de Gobierno Electrónico, reforzando los servicios brindados con una verdadera tutela de estos derechos fundamentales.

8. Reflexiones finales

Actualmente a unos años de sancionada la Ley N° 18.331 con sus modificativas y Decreto Reglamentario, la protección de datos personales como un derecho humano fundamental sigue siendo en nuestro país una norma innovadora, que aporta a los habitantes una garantía práctica para frenar el uso indiscriminado de la información personal, la que hoy en día posee un altísimo valor en sí misma.

Será un imperativo de cada uno de nosotros conocer, difundir e involucrarnos en la protección de este derecho, especialmente en una sociedad de la información tendiente a la gestión de políticas tanto comerciales como de gobierno a través de las tecnologías de la información y del conocimiento a fin de evitar un mal manejo de nuestros datos y evitar así efectos negativos o indeseados ya sea en la gestión de Políticas del Estado o sea en el relacionamiento con otros particulares.

Es un gran desafío que la administración pública ha estado desarrollando el preservar la garantía de protección de este derecho, sin perder el foco en una necesaria implementación de tecnología en el manejo de un aparato estatal. Este quiebre de paradigma presupone la cooperación entre los diversos sujetos que en él participan y es y será responsabilidad de todos los actores el adaptarnos a vivir en una nueva sociedad, una sociedad construida en base a un gobierno electrónico necesariamente enfocado hacia un ciudadano tutelado en sus esferas más intimas, especialmente en el goce y protección de sus datos personales.

CAPITULO IV

CONSENTIMIENTO INFORMADO ¿REGLA O EXCEPCIÓN?

Dr. Felipe Rotondo

CONSENTIMIENTO INFORMADO ¿REGLA O EXCEPCIÓN?

Dr. Felipe Rotondo

1. Introducción

"El consentimiento del titular es un tema clave en el sistema jurídico aplicado a la protección de datos personales. ¿Qué requisitos deben cumplirse para que sea lícito? ¿En qué situaciones no es necesario recabarlo?

Éstos y otros aspectos han dado lugar a diferentes enfoques y opiniones. La transparencia es una condición para la disposición de las facultades de control y legitimidad de un auténtico consentimiento. Por ende, el deber de información es un corolario ineludible. No obstante, surge como tema de discusión si será este un requisito que deba cumplirse en todos los casos.

Las leyes de protección de datos y el reciente dictamen sobre la definición del consentimiento adoptado por el Grupo de Protección de Datos del artículo 29 darán paso a la reflexión y brindarán oportunidad de compartir lecciones aprendidas"[1].

2. Sistemas en la materia: opt out y opt in

En contextos en línea como fuera de línea, puede hacerse referencia, de modo esquemático, a dos sistemas: de Opt out y Opt in, denominaciones que se utilizan en especial en el sector de comunicaciones comerciales.

El primero de ellos se fundamenta en la libertad de comunicación, que engloba la de información, así como también en la libertad de empresa.

Tiene en cuenta, por otra parte, la proliferación de dispositivos y aplicaciones que llevan a que no sea posible identificar al titular de datos y, entonces, el consentimiento no sea practicable.

Establece un régimen de listas de (auto) exclusión voluntaria por parte del titular de los datos personales, las que deben ser consultadas por parte de quien realiza el tratamiento de esos datos de manera de no efectuarlo si existe inclusión en la respectiva lista.

En lugar del consentimiento, lo decisivo es el derecho de oposición.

Las listas en materia comercial pueden ser nacionales o internacionales; también públicas o privadas en este caso por la naturaleza de la o las instituciones que las llevan: en el primer caso, corresponde la consulta periódica por el anunciante antes de enviar la comunicación comercial no solicitada; en el segundo caso, la lleva cada empresario, el cual no remitirá la comunicación a quien se opone a ello.

Específicamente en materia de publicidad existen los ficheros Robinson, que permiten inscribirse con el fin de no recibir más publicidad.

1 Términos que figuran en el Programa de la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Panel "J".

El sistema Opt in, en cambio, se fundamenta en una clara afirmación del derecho a la privacidad y su desarrollo específico, que es el derecho a la protección de los datos personales, por lo cual exige el previo consentimiento del titular.

Dicho consentimiento –en tanto no se trate de una mera rutina formularia – implica una mayor seguridad y control para ese titular, y, por otro lado, contribuye a una mejor imagen empresarial de quien trate los datos.

"Por tratarse de un acto positivo, la importancia del consentimiento excluye de facto cualquier sistema por el que el interesado solo tendría derecho a oponerse a la transferencia después de haberse producido"[2].

En materia de publicidad, da lugar al "marketing de permiso"; las listas de quienes dan el consentimiento, son llamadas "blancas".

On line este sistema puede encontrar problemas de opacidad de las políticas de confidencialidad, que comprenden, por ejemplo, opciones por defecto, las que –precisamente – se discuten como consentimiento válido; más adelante se considera este punto.

3. Caracterización del consentimiento

La exposición que se realiza al respecto tiene en cuenta el Dictamen Nº 15/011 adoptado con fecha 13 de julio de 2011 por el "Grupo de Protección de Datos del artículo 29" (GT) órgano consultivo creado por la Directiva europea 95/46/CE, en el cual se "analiza exhaustivamente el concepto de consentimiento en la Directiva de protección de datos y en la Directiva sobre privacidad".

El consentimiento como manifestación o expresión de la voluntad "de la persona cuyos datos sean objeto de un tratamiento"[3], tiene requisitos que la hacen válida.

En ese sentido, tiene que ser:

3.1 Libre

Por lo mismo, no debe tener vicios que afecten la voluntad por error, dolo, violencia o presiones de cualquier índole, como pueden ser consecuencias negativas significativas en caso de que no se consienta.

De esa manera procede atender posibles situaciones de dependencia de diversa índole (laboral, financiera, etc.): así, en el caso del uso de escáner respecto de las personas en los aeropuertos, en rigor no es el consentimiento el que habilita el tratamiento de quien –si no lo admite – no ingresa a la sala de embarque, es la normativa correspondiente, fundada en la seguridad pública, la que se aplica; otro caso de interés que anota el Dictamen aludido, es el de la colocación de fotos de empleados de una empresa en su Intranet, en que juega el consentimiento (válido) si aquellos remiten la foto o admiten la incorporación de la foto digital que ya posee la empresa, pulsando un botón, sin que la negativa a hacerlo tenga consecuencia alguna; también el acceso a redes sociales sujeto a la aceptación de recibir marketing, en el cual el consentimiento no será válido si no existe otra opción.

2 Documento de trabajo 114 del Grupo de Trabajo del art. 29 de la Directiva Europea 95/46/CE; citado en su Dictamen N° 15/011, página 11.

3 Términos del art. 4º "L" de la ley uruguaya Nº 18.331 de 11-VIII-2008. A su vez el apartado "M" de esa disposición define el "tratamiento": "operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias". Queda incluida la recolección de datos y su tenencia.

3.2 Previo al tratamiento de datos

El Dictamen 2/012 GT sobre reconocimiento facial en servicios en línea y móviles, en su apartado 4.5 dice: "Debido a los riesgos particulares asociados a los datos biométricos, antes de comenzar el tratamiento de las imágenes digitales a fines del reconocimiento facial se requerirá el consentimiento informado de la persona. No obstante, en algunos casos es posible que el responsable del tratamiento de los datos necesite llevar a cabo algunas etapas del proceso de reconocimiento facial con el objetivo, precisamente, de comprobar si el usuario ha dado o no su consentimiento, que es la base legal del tratamiento. En tal caso el tratamiento inicial (es decir, la obtención de la imagen, la detección de la cara, la comparación, etc.) puede tener una base distinta, especialmente el interés legítimo del responsable del tratamiento de los datos en cumplir las normas sobre protección de datos (...)".

3.3 Debidamente informado

Su otorgamiento debe efectuarse en base a información completa, concreta, comprensible o asequible, en la que se indique el tratamiento a realizar y su finalidad específica, el motivo y tipo, el destinatario, así como la identidad y dirección del responsable[4].

Por tanto, puede decirse que se desarrolla una especie de proceso, el cual es decisivamente necesario si refiere a la participación en ensayos clínicos ya que se exige tiempo para reflexionar, la confección de formularios específicos, los cuales en general se aplican en el ámbito de la salud[5]/[6], etc.

3.4 Inequívoco

Este aspecto se relaciona con los métodos para efectuar el consentimiento y, en consecuencia, se proyecta en la prueba de su existencia.

En tanto el consentimiento es una manifestación de voluntad, surge su carácter expreso o explícito, derivado de acciones o conductas positivas del titular de los datos[7].

En relación a la Directiva europea 95/46/CE, se ha planteado la duda de la admisibilidad de un consentimiento implícito derivado de la omisión del titular, circunstancia en la que, por cierto, se dificulta la prueba[8].

En el Dictamen Nº 15/011 se incluyen diversos casos que ejemplifican sobre el tema; así el de envío de carta o mensaje con propuesta de cesión de datos, al cual no se responda en un plazo de dos semanas; el no pulsar un botón para permitir que se vean los datos en red social; el consultar un motor de búsqueda, etc.

Dicho Dictamen se pronuncia claramente al respecto: "(...) el hecho de que la persona no realice

4 En términos del art. 4º "K" de la ley uruguaya antes citada: "Persona física o jurídica, pública o privada, propietaria de la base de datos o que decida su finalidad, contenido y uso del tratamiento".

5 La Administración para los Alimentos y Medicamentos (FDA) de EEUU estableció en 1977 normas de buena práctica clínica para asegurar la calidad y la protección de los derechos de los pacientes en la investigación clínica.

6 La especificidad de la información debe referirse a una situación bien definida y concreta en que esté previsto el tratamiento de datos médicos, documento WP 131 del GT del art. 29.

7 La ley uruguaya 18.331, art. 9º, bajo la denominación de "Principio del previo consentimiento informado", exige que sea expreso y que se documente; agrega que "El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido, de la información descrita en el artículo 13", o sea finalidad, quiénes pueden ser destinatarios o su clase; existencia de base de datos, electrónica o de cualquier tipo, identidad y domicilio del responsable; carácter obligatorio o facultativo de las respuestas; consecuencias de proporcionar los datos, de negarse a hacerlo o de la inexactitud de aquellos; posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

8 La propuesta de la Comisión fue la de requerir un consentimiento expreso y, en el caso de los datos sensibles, escrito; en la Directiva 95/46/CE se adoptó respectivamente los términos "inequívoco" y "explícito".

una acción positiva no permite concluir que ha dado su consentimiento. Por tanto, no cumple el requisito de consentimiento inequívoco". "El Grupo de Trabajo ha declarado la inadecuación del consentimiento basado en el silencio de la persona en el contexto del envío directo de publicidad por mensajes electrónicos (...)"[9]/[10].

4. Continuación: otros aspectos relativos al consentimiento

4.1 Medios

A los efectos indicados en el precedente apartado III.4 , el medio de formulación del consentimiento puede ser convencional o electrónico: firma manuscrita o electrónica; correo de esta naturaleza; pulsación de icono o tecla o selección de casilla en sitio web[11]; expresión oral (ejemplo, brindar de ese modo, dirección postal o electrónica para que se envíe información promocional de hotel) o mediante una acción positiva (ejemplo, participar en sesión de fotos como cliente de hotel, mediante concurrencia a sala prefijada al efecto).

No existe esa (clara) expresión de voluntad a través de casilleros ya marcados[12].

4.2 Procedencia

La correspondiente información debe darse directamente al titular de los datos y el consentimiento debe provenir de este, por lo cual – afirma el multicitado Dictamen Nº 15/011– "no basta que la información esté 'disponible' en algún lugar", por el ejemplo en algún punto del sitio web que el usuario visita.

4.3 Responsabilidad de su requerimiento

El requerimiento, a su vez, proviene del responsable del tratamiento, sobre el cual recaen las consecuencias si el consentimiento no existe o, si no puede ser acreditado; a él corresponde informar previamente al interesado.

Debe precisarse que "(...) la obtención del consentimiento no anula las obligaciones del responsable del tratamiento (...) en lo que respecta a la imparcialidad, necesidad y proporcionalidad, así como a la calidad de los datos. Por ejemplo, incluso un tratamiento de datos personales basado en el consentimiento del usuario no legitimaría la recopilación excesiva de datos para un fin particular"[13].

9 Pág. 27.

10 Págs. 13-14: tiene en cuenta que la Directiva citada alude a "Toda manifestación de voluntad libre (...) mediante la que el interesado consienta el tratamiento de datos personales que le conciernan" y afirma: "La expresión mínima de manifestación podría ser cualquier tipo de señal, suficientemente clara para poder indicar la voluntad del interesado y comprensible por el responsable del tratamiento de datos. Los términos 'manifestación' y 'mediante la que' apuntan a una acción realmente necesaria frente a una situación en la que el consentimiento podría deducirse de la falta de acción". También que "el requisito de que el interesado debe manifestar su consentimiento parece indicar que la simple inacción es insuficiente y se requiere algún tipo de acción para crear el consentimiento, aunque sean posibles diferentes tipos de acciones que se evaluarán 'según el contexto".

11 La admite la Directiva 2002/58/CE. El Dictamen Nº 15/011 ejemplifica con la selección hecha para programa de fidelidad respecto a hotel, en formulario en línea por medio del cual se efectúa una reserva de alojamiento.

12 El Decreto Nº 414/009 de 31-VIII-2009, reglamentario de la ley uruguaya Nº 18.331, art.6 inciso 2º, admite la validez de "la elección entre dos opciones claramente identificadas, que no se encuentren premarcadas a favor o en contra".

13 Dictamen N° 15/011 citado, pág. 8.

4.4 Prueba

Como ya se dijo, procede asegurar o crear lo necesario para (poder) probar la existencia del consentimiento, incluso en cuanto a la antes referida procedencia.

4.5 Revocabilidad

El (libre) consentimiento puede, libremente, revocarse en cualquier momento, de modo sencillo y sin precisarse justificación o motivación. Por otra parte, sin consecuencias negativas para el interesado ya que, de otro modo, desaparecería la libertad[14].

Si medió una cesión de datos a terceros, procede comunicarse la revocación a estos.

En cuanto a eficacia en el tiempo, la revocación no es retroactiva.

4.6 Validez por tiempo determinado

En algunos casos, por ejemplo respecto a servicios de localización, criterios de buena práctica aconsejan un consentimiento acotado en el tiempo y que se prevean mecanismos de aviso al titular, para que admita la prosecución de su consentimiento.

4.7 Tratamiento sin consentimiento

El recabar los datos sin consentimiento, en los casos que él corresponde, constituye una infracción grave al régimen de protección de datos; lo es especialmente, si se lo hace en forma engañosa o fraudulenta, si se agrega cualquier otro tratamiento o si la recolección refiere a datos sensibles[15].

5. Exenciones del consentimiento

En un sistema que lo tiene como eje, el consentimiento no se requiere en las siguientes situaciones:

5.1 En virtud de disposición legal que habilita el tratamiento, por razones de interés general[16].

"La naturaleza del responsable del tratamiento también puede ser decisiva a la hora de determinar el fundamento jurídico del tratamiento de datos personales.

Es el caso de los responsables del tratamiento del sector público, donde el tratamiento de datos suele estar vinculado al cumplimiento de una obligación jurídica (...) o al cumplimiento de una misión de interés público (...) Esto es especialmente evidente en el tratamiento de datos personales por parte de autoridades públicas con poderes coercitivos tales como los servicios de seguridad, que actúan en el ámbito de su competencia al realizar actividades policiales y judiciales (...)"[17].

5.2 Si se trata de datos provenientes de "fuentes públicas de información, tales como registros o

14 Lo dicho debe matizarse en caso de que exista una relación contractual, laboral, administrativa o fiscal, en que la revocación tendrá que tener un fundamento razonable.

15 En esa línea, Resolución Nº 320 dictada por el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales el 17-III-2011.

16 La ley uruguaya 18.331, art. 9 inciso 3º "B" alude a datos que "Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

17 Dictamen N° 15/011 GT art. 29, pág. 17-18. Agrega que "con frecuencia, en el tratamiento de datos personales en el sector público se mezclan regímenes diversos, lo que puede generar incertidumbre y abusos si no está debidamente justificado por el consentimiento".

publicaciones en medios masivos de comunicación"[18].
En tal hipótesis, el responsable tiene que poseer "un interés legítimo para su tratamiento" y no vulnerarse "los derechos y libertades fundamentales del interesado"[19].

5.3 En el caso de datos que "deriven de una relación contractual, científica o profesional del titular" y "sean necesarios para su desarrollo o cumplimiento"[20]
En materia de publicidad, ello es aplicable en tanto y en cuanto se relacione con productos o servicios similares a los que refiere la contratación, situación en la que corresponde el uso del opt out, como lo marca la Directiva europea 2002/58/CE.

El Dictamen N° 15/011 del GT del art. 29 expresa que "El consentimiento no es el único fundamento de legalidad", si bien es "claramente" presentado como tal en la Directiva europea. Hay casos en que no es "el fundamento más adecuado para legitimar el tratamiento de datos personales", si bien se requiere, entonces, una 'prueba de necesidad'.

6. Cuestiones específicas

6.1 Datos sensibles

En relación a estos datos[21] y por su propia esencia, el consentimiento aparece como especialmente exigente y así la normativa lo requiere expreso (cuando se admite el implícito) o escrito (cuando solo se alude al explícito o expreso).

En esta última línea, la ley uruguaya Nº 18.331 de 11-VIII-2008 los incluye como "datos especialmente protegidos" y su art. 18 dispone, en su primer inciso, que "Ninguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular".

6.2 Datos de incapaces

El consentimiento proviene de un titular de datos, con capacidad.

En relación a los incapaces se plantea la cuestión de la procedencia del consentimiento: provendrá de sus representantes (padres, tutor, curador), pero no puede dejarse de considerar, especialmente la situación de los menores de edad, según su concreto grado de madurez y, también, si ellos están habilitados a contratar, a contraer matrimonio, a emplearse, etc.[22].
En las circunstancias antedichas, es del caso considerar su personal voluntad.
Por su parte, si el consentimiento provino del representante de un menor, corresponderá la ratificación al alcanzarse la mayoría de edad[23].

18 Texto del art. 9 inciso 3º "A" de la ley uruguaya citada.

19 Conf. Curso sobre El Derecho a la Protección de Datos Personales, 1ª edición, Módulo 2- Fundación CEDDET-Agencia Española de Protección de Datos, pág. 32.

20 Art. 9 inciso 3° "D" de la ley uruguaya citada.

21 El art. 4º "E" de la Ley uruguaya Nº 18.331 define "dato sensible": "datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual".

22 El Real Decreto español 1720/007, art. 13 exige el consentimiento de padres o tutores si se trata de personas de menos de catorce años; si son mayores de esa edad, puede procederse al tratamiento de datos con su propio consentimiento, salvo en los casos en que la ley exija para su prestación la asistencia de los representantes.

23 En informe del 18-I-2008, el GT del art. 29 expresó que "por ejemplo, si un representante ha dado su consentimiento explícito a la inclusión del niño (el interesado) en un ensayo clínico, al alcanzar la mayoría de edad, el responsable del tratamiento debe asegurarse de que sigue siendo una base válida para el tratamiento de los datos personales del interesado. En concreto, deberá considerar la obtención del consentimiento explícito del propio interesado para que continúe el ensayo, ya que están implicados datos sensibles".

6.3 Geolocalización en dispositivos móviles inteligentes

El Grupo de Trabajo del art. 29 se ha pronunciado sobre el tema en el Dictamen 13/011.

Entiende que de forma predeterminada los servicios de localización deben estar apagados y que se exige el consentimiento para la activación de tales dispositivos, a los diversos fines para que los datos sean captados o almacenados. Además que ellos deben tener un icono de advertencia continua sobre la activación de la función de geolocalización; recomienda, además, limitar el alcance temporal del consentimiento y recordarlo a los usuarios la menos una vez por año.

En caso de utilizarse en ámbito laboral, en primer lugar interesa la legitimidad de la finalidad del tratamiento; en segundo lugar, procede buscar los medios menos intrusivos e informarse sobre la manera de desactivación fuera del horario de trabajo.

Para el caso de control infantil, apreciarse la justificación de tales aplicaciones, en circunstancias específicas; informarse a los hijos y, tan pronto como sea posible, permitírseles participar en la decisión de esa utilización[24].

6.4 Publicidad comportamental[25]

En este rubro, existen varios aspectos de interés, que se tratan en Dictámenes Nº 2/010-16/011-4/012 del GT del art.29.

En cuanto a los responsables lo son los proveedores de redes de publicidad.

Los editores, lo serán respecto al deber de información, si configuran los sitios de manera de redireccionar automáticamente a los buscadores de los usuarios a la página del proveedor. Por su parte, el anunciante lo será si capta información de rastreo.
En la información sobre la instalación de las cookies[26] debe informarse el plazo de duración de estas.

Admite la exención del previo consentimiento informado para las cookies que se utilicen "al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas" así como "en la medida de lo estrictamente necesario a fin de que un proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o usuario"[27].

Se admite que no es necesaria la reiteración de consentimiento para cookies con la misma finalidad y proveniente del mismo proveedor, si se opta por ventanas desplegables.

En cuanto a la configuración del navegador que acepta por defecto la orientación de los usuarios, no reviste el carácter de consentimiento válido de conformidad con el Dictamen Nº 16/011 GT del art. 29.

24 En todos los casos las políticas de conservación de datos deben garantizar que los datos de geolocalización como los perfiles que en con su base se efectúen, se eliminen en plazo razonable.

25 Sobre el tema, véase el e-book "Marketing comportamental en línea. El desafío de las cookies" de la Dra. María José Viega Rodríguez, julio 2012.

26 Fichas de información sistematizada que se envían desde un servidor web al ordenador del usuario y que constituyen técnicas de rastreo; la finalidad es identificar las visitas al mismo sitio.

27 Art. 5.3. revisado, de la Directiva europea sobre la privacidad y las comunicaciones electrónicas.

7. Normativa y dictámenes de la Unión Europea: mención

*Directiva 95/46/CE, en especial arts. 2 "h", 7, 8, 26 y "Considerandos" 30 y 45, aplicable a tratamientos automatizados y manuales de datos.
*Directivas sobre privacidad y comunicaciones electrónicas: la 2000/31/CE adoptó el sistema opt out; la 2002/58/CE, modificada por la Nº 2009/136/CE, establece el sistema opt in como regla general, "para el almacenamiento o la obtención de acceso a información ya almacenada, en equipo terminal de un abonado o usuario, sólo está permitido a condición de que el suscriptor o usuario haya dado su consentimiento (...)", con la excepción que se señaló en

7.1

*Dictámenes 2/010-16/011-4/012: sobre marketing comportamental
*Dictamen 12/01 GT sobre: smart meters y smart gris.
*Dictamen 13/011 GT sobre servicios de geolocalización
*Dictamen 15/011 GT sobre definición del consentimiento y su análisis, que ha sido especialmente tenido en cuenta en lo aquí expuesto.
*Dictamen 2/012 GT sobre reconocimiento facial en servicios en línea y móviles.

CAPITULO V

GOBIERNO ABIERTO

Dra. Laura Nahabetián Brunet

GOBIERNO ABIERTO

Dra. Laura Nahabetián Brunet

1. Introducción

La aparición de las tecnologías de la información y la comunicación ha generado una revolución innovadora determinante de modificaciones impensables y de retos, desafíos, expectativas y riesgos inimaginables.

Internet ha venido a constituirse en el sustento material y tecnológico de la sociedad en red, dado su carácter esencial de infraestructura tecnológica, por tanto ha favorecido el desarrollo de toda una serie de cambios de índole histórico, cultural y económico que si bien no tienen su origen propiamente tal en la red, sin ella nunca habrían sucedido. Así es que nuevas formas de interacción social, empresarial, gubernamental, individual y política están conformando la realidad de hoy.

Los desafíos a los que la sociedad se enfrenta están directamente vinculados con la asunción de este nuevo paradigma socio técnico que tiene como sustento la web y que sin lugar a dudas, constituye y cada día más constituirá el elemento clave de las nuevas formas de vinculación, trabajo y comunicación.

La web entonces se erige como un espacio de redes que habilita nuevos procedimientos para el acceso a la información por los ciudadanos, facilitando su interacción en tiempo real, pudiendo ser decisores, en caso de proponérselo.

De esta forma los ciudadanos esperan acción de parte de los gobiernos; la inactividad e incomprensión por parte de los ejercientes de los poderes políticos determinan riesgos para la institucionalidad y facilitan el descreimiento y la intrascendencia de que cada vez más son objeto.

La participación frente a la apatía generalizada es mucho más que la posibilidad – tantas veces impuesta – del ejercicio del voto cada determinado tiempo.

Con mayor frecuencia se verifican movimientos ciudadanos que convocados por intereses comunes que les son particulares se manifiestan y exigen participación; sólo tres ejemplos: los paradigmáticos estudiantes venezolanos, las revueltas musulmanas en África o los jóvenes en España.

Ahora bien, esta auto convocatoria por métodos y mecanismos tradicionales puede verse potenciada mediante la utilización de tecnologías de la información y la comunicación.

Los ciudadanos empiezan a exigir ser parte de la toma de decisiones y están aburridos de ser consumidores digitales de propaganda electoral, pretenden ser partícipes de acción en la gestión de las agendas y los asuntos públicos.

La era digital tiene el enorme potencial de facilitar una relación directa entre los ciudadanos y los actores políticos. La decisión como nunca antes tal vez es de éstos últimos, quienes deberán asumir el desafío de un accionar más efectivo, más transparente y más sincero.

"A diferencia de quienes ven en la sociedad civil el verdugo de los partidos y del Estado, los nuevos protagonistas de la vida en comunidad lo que han hecho es abrirle una oportunidad a los partidos y al Estado para trabajar conjuntamente en la búsqueda del interés público. Una mayor participación implica un mejor diálogo político y debe traducirse en mayor y mejor representación. Es una oportunidad para abrir las vías de acceso de los partidos a la sociedad civil; un acto de audacia pero

más de supervivencia para que los partidos puedan imaginarse cómo van a articular la sociedad civil al sistema político."[1]

2. Un paso previo ...

Es muy importante tomar cabal conciencia que gobernanza es ciertamente un compromiso profundo de incentivo del relacionamiento ciudadanos – gobierno.

La gobernanza electrónica implica un proceso a través del cual se pretende guiar a la sociedad para la obtención del mejor logro de sus objetivos, sus metas, sus intereses.

El gobierno electrónico será una de las múltiples formas de colaboración en términos instrumentales para la concreción de la gobernanza, ya no sólo electrónica sino en términos generales.

La pretensión, en definitiva, es la obtención de lo que ha dado en llamarse "buen gobierno". Es en él y a través de él, donde se asienta la viabilidad de un proyecto país de la envergadura que se considera debe llevarse adelante, en el sentido que no sólo se trata de una "situación" tecnológica, sino de un cambio en las estructuras funcionales ejecutadas desde siempre. No sólo se trata de un análisis y modificaciones desde una perspectiva tecnológica, sino también de ejecutar aquéllas que por imprescindibles repercuten directamente en los planos organizacional y legislativo.

Además este Buen Gobierno deberá constituirse en el corazón de los cambios a desarrollar en el futuro. Ésta es al menos la estrategia seguida por los países que muestran un mayor avance en el tema.

Se trata en definitiva de ejecutar acciones que favorezcan la gestión interna del gobierno, buscando instalar en el aparato público nuevos procesos internos y formas que habiliten la integración de los sistemas de los diferentes servicios, compartiendo recursos y ampliando, mejorando y otorgando calidad real a la gestión interna de los mismos.

3. Conceptualizando realidades

Existen diversas concepciones respecto de lo que debe entenderse por gobernanza electrónica en función de los diferentes énfasis que se hacen por parte de las diversas organizaciones que tienen interés en el progreso de la misma.

De esta manera, el Banco Mundial establece un importante subrayado en los aportes que la gobernanza efectúa al desarrollo económico y social a través de la generalización de las libertades de índole institucional y económica. De esta forma, la gobernanza electrónica "implica el uso de los canales de TIC para cambiar la forma en que los ciudadanos y las empresas interactúan con el gobierno para posibilitar la participación de los ciudadanos en la toma de decisiones, un mayor acceso a la información, más transparencia y el fortalecimiento de la sociedad civil."[2]

Existen vínculos importantes entre desarrollo humano sostenible y gobernanza. En efecto, ésta es la postura asumida por el Programa de las Naciones Unidas para el Desarrollo. La gobernanza electrónica tendrá su sentido de existencia en la medida que sirva para dar amplitud a las administraciones públicas facilitando el incremento de la calidad de vida de los ciudadanos, lo que será obtenible si facilita "equipar a las personas para una participación genuina en un proceso

1 Carrillo Flórez, Fernando.- "El déficit de democratización en América Latina", en Democracia en déficit: Gobernabilidad y Desarrollo en América Latina. BID. Washington, 2001.

2 Deane, Arsala. Increasing Voice and Transparency Using ICT Tools: E-Government, E-Governance. World Bank E-Government Websites, 2003.

político inclusivo que puede producir un consentimiento público bien informado, base cada vez más prevaleciente para la legitimidad de los gobiernos."[3]

De esta forma consideran que la gobernanza electrónica "es un proceso de creación de valor público con el empleo de las modernas TIC. El valor público está definido como una noción arraigada en las preferencias de las personas."[4]

Así, la afirmación que "el desafío primario del gobierno electrónico para el desarrollo es cómo lograrlo" habla de la convicción del carácter instrumental del mismo a la hora de la concreción de los mecanismos facilitadores y constructores de la gobernanza electrónica.[5]

Por su parte el Grupo de Administración Pública de la Organización para la Cooperación y el Desarrollo Económico[6] establece como base y fundamento de la gobernanza electrónica, los siguientes tres elementos:

- información;
- participación activa;
- consulta.

Además, la gobernanza debe contener como calificativos sustanciales las características de en línea y participativa.

En definitiva, la gobernanza electrónica implicará la materialización de procesos a través de los cuales sea posible usufructuar positivamente y aprehender las múltiples potencialidades que proporcionan las tecnologías de la información y la comunicación, sea en los diferentes estadios del gobierno y en su vínculo con la sociedad civil, de forma tal de facilitar los procesos de gobernanza considerada en sentido amplio de forma de contribuir al desarrollo de la buena gobernanza.

Ciertamente y a pesar de la existencia de multiplicidad de definiciones y de connotaciones particulares dependiendo de los énfasis que se otorguen en los diferentes casos, lo importante viene dado por el hecho de que la gobernanza genera la posibilidad de que los ciudadanos transformen su status de ciudadano pasivo, limitado a consumir servicios de diversa índole, para facilitar el desempeño de una actividad proactiva en la toma de decisiones en relación con las opciones de servicios que necesitan y en la decisión de qué tipo de opciones pueden asumirse para el mejoramiento de los mismos.

De esta forma, la gobernanza electrónica facilitará la creación de ciudadanías activas con mayor compromiso, habilitando a quienes estén dispuestos a ser parte del desafío de construir buen gobierno, una participación de relevancia. Por tanto el desafío es en una doble dirección. Por un lado los ciudadanos son llamados a ser parte, a participar en la construcción de las decisiones importantes de gobierno y por otro, las autoridades de gobierno deberán ser capaces de transformar los tradicionales estilos de liderazgo político para evitar rezagos, inacción y por tanto deslegitimación.

Seguramente éstos deberán asumir liderazgos por demás comprometidos en esa dirección, de forma de facilitar la construcción e implementación de políticas públicas que aborden modificaciones sustanciales en el desenvolvimiento de los procesos y procedimientos de tipo administrativo, las formas de gestión, el otorgamiento de recursos económicos y humanos. La contracara que seguramente también existe será la falta de compromiso político, en el entendido de que la gobernanza no está ya al servicio de intereses particulares de tipo jerárquico sino que colabora con ordenaciones de tipo horizontal.

3 Naciones Unidas. Informe Mundial del Sector Público (WPSR). 2003.

4 Naciones Unidas. Ob. Cit.

5 Naciones Unidas. Ob. Cit.

6 Riley, Cathia.- The Changing Role of the Citizen in the E-governance and E-democracy Equation. Commonwealth Centre for Electronic Governance. Ottawa, 2003.

"La gobernanza electrónica puede ser poco útil, si sugiere, erróneamente, que la aplicación de las TIC es un fin en sí misma. Puede ser que resulte más apropiado hablar de gobernanza integrada o, quizás, de gobernanza inteligente que prioriza los objetivos de la gobernanza y considera las TIC como una parte de los medios para lograr esos objetivos conjuntamente con las personas, los procesos y la información."[7]

En definitiva entonces, el objetivo de la gobernanza electrónica implicará determinar acercamientos no generados hasta estas fechas entre las diversas estructuras gubernamentales de distinto orden para con los ciudadanos, generalizando una oferta de servicios eficientes que finalicen en el incentivo y concreción de la participación ciudadana en los diversos ángulos del quehacer gubernamental.

Por tanto, las implicancias de esta afirmación determinan que el gobierno brinde más y mejores servicios a sus ciudadanos sin por ese motivo restar importancia a la forma en que éstos participan y efectivizan sus decisiones en el marco del funcionamiento del sistema democrático.

La gobernanza electrónica implicará mayor interacción bidireccional pero las preguntas vienen relacionadas con la instrumentación de los mecanismos que la faciliten.

Esta gobernanza tiene además connotaciones de diversa índole tanto en términos sociales, cuanto económicos, políticos y fundamentalmente económico - políticos.

En este sentido, organismos como el Banco Mundial han impulsado a los distintos gobiernos a formalizar "un marco legal e institucional para la transparencia, la previsibilidad y la competencia, así como la gestión del desarrollo económico."[8] Esto sucede en la medida que son los gobiernos los que tienen en sus manos la posibilidad de la generación de las condiciones básicas de facilitación de acceso igualitario a los mercados. Éstos pueden liberalizar o no los marcos económicos e institucionales. A través de la incorporación de las políticas públicas adecuadas podrán generar no sólo crecimiento sino distribución equitativa de posibilidades de acceso a la educación, a los sistemas sanitarios, entre otros aspectos.

Finalmente, en este sentido es dable establecer, que la tendencia debe ser a la concreción de desarrollo humano sostenible y éste no debe ser de manera alguna una cuestión anexa a los logros económicos o un derivado de éstos, sino que es de esencia de la gobernanza electrónica en tanto tributaria de la gobernanza en su consideración más amplia.

Compartido es el criterio de que "la governance incluye al Estado, pero lo trasciende al incorporar al sector privado y la sociedad civil. El Estado crea un ambiente político y legal favorable. El sector privado genera trabajo e ingresos. La sociedad civil facilita la interacción política y social, movilizando los grupos para que participen en las actividades económicas, sociales y políticas."[9]

La finalidad de tipo estratégico que cumple la gobernanza electrónica considerada desde una óptica de tipo político es servir de apoyo y facilitar simplificando la buena gobernanza entre todos los actores estratégicos involucrados, entre los que son de sustancia el Estado y la sociedad civil siendo el elemento diferenciador del proceso la incorporación de las tecnologías de la información y la comunicación.

7 Heeks, Richard. "Building e-Governance for Development: A Framework for National and Donor Action". E-Government Working Paper Series. Institute for Development Policy and Management, University of Manchester. Inglaterra, 2001.

8 Banco Mundial. "Managing Development. The Governance Dimension". Washington, 2004.

9 Naciones Unidas. "Interfase Pública - Privada en la Gestión Ambiental Urbana." Foro online. PNUD, 2002.

Según Richard Heeks[10] se verificarán tres modificaciones básicas a partir de la incorporación de las tecnologías de la información y la comunicación en la teoría y práctica de la gobernanza, a saber:

- La automatización, lo que remplazará los circuitos de ejecución que hoy día son cumplimentados por ciudadanos en sus diferentes facetas.
- La informatización, lo que colaborará desde el punto de vista de la información con los procesos ejecutados por ciudadanos en los diferentes ámbitos.
- La transformación, lo que implicará la creación de nuevos circuitos de acceso y generación de información a través de la utilización de las tecnologías de la información y la comunicación.

La gobernanza en red y la gobernanza electrónica aparecen en este marco, como una idea emergente con un fuerte componente de rechazo a la gobernanza burocrática de que hablaba Weber.[11]
Su modelo está determinado por dos facetas:

- Faceta estructural relacionada con todo lo que hace al ordenamiento de tipo jerárquico de las diversas situaciones, vinculadas a la base legal racional de la autoridad y a los sistemas de compensación.
- Faceta conductual relacionada a la posición meritocrática de los funcionarios poniendo un acento en las enseñanzas aprehendidas.

Ahora bien, los tradicionales principios weberianos de la gobernanza de tipo burocrático pretenden ser reemplazados y de hecho lo están siendo por las actuales opciones de gobernanza horizontal que implican mayor sencillez y dinamismo, a lo que se adiciona su componente electrónico a través de la posibilidad de hacerlo en red.

Las reformas de tipo administrativo que se sucedieron en América Latina desde los años noventa, incentivadas por el Consenso de Washington derivaron – en muchos casos – en reingenierías de procesos y en definitiva en la reinvención del gobierno.

La gobernanza se dirige a tratar de generar los mecanismos de ajuste entre la administración y el flujo cada vez más importante de la información de manera tal de acelerar los procesos decisorios optimizando los recursos a través de su autorregulación.

De esta manera entonces, sería importante incentivar la gobernanza en red en la medida que ésta implica un funcionamiento que determina el carácter instrumental de la red para con la política, facilitando la ejecución de consultas, la interacción entre las diferentes organizaciones que son activas en la toma e implementación de decisiones y los ciudadanos.

La gobernanza en red aparece como un instrumento más amplio que la gobernanza electrónica pero ambas se determinan y alimentan permanentemente.

En efecto, la gobernanza en red pone su énfasis en "la soberanía de las unidades (el Estado) cuyas interacciones facilitan o inhiben el funcionamiento de todo el sistema."[12]

La gobernanza electrónica, sin desconocer esa soberanía pone su énfasis en la "creación de valor público por medio de las tecnologías de la información y la comunicación."[13]

"La tecnología de la información por su propia dinámica genera una nueva institucionalidad. Las organizaciones públicas tanto como las privadas pueden asumir nuevas expresiones organizacionales, más desconcentradas, más descentralizadas, más participativas, más horizontales y con esquemas

10 Heeks, Richard. Ob. Cit.

11 Weber, Max. "Economía y sociedad". University of California. California,1921.

12 Sarker, Partha. "Gobierno en red y Governance electrónica", en Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información. París, 2005.

13 Naciones Unidas. Ob. Cit.

institucionales más flexibles que antes. Se abren nuevos espacios de interacción entre gobernantes y ciudadanos que dan paso al gobierno virtual, con expresiones que implican una relación distinta de las autoridades públicas con la ciudadanía en campos como la presentación de los servicios públicos domiciliarios por la vía electrónica."[14]

La gobernanza en red pretenderá poner en contacto pero fundamentalmente en interacción a los ciudadanos de forma tal que asuman el compromiso del aprendizaje, el debate y el riesgo positivo de la participación en lo que implica la elaboración de políticas públicas.

Su finalidad será encontrar en la diversidad los puntos de consenso.

"El intento de desarrollar el "conocimiento consensuado" puede favorecer al mínimo denominador común, como resultado eventual de la política. Además las redes no sólo adicionan recursos, sino también están estructuradas para beneficiarse del hecho de que cada sector participante aporte diferentes recursos al debate. Sin embargo, también es cierto que lograr el consenso puede ser un proceso lento y costoso, particularmente en un entorno conflictivo."[15]

Por su parte, la gobernanza electrónica facilita que las instituciones sean las que se ocupan de la constitución de los consensos, sin embargo, se verifica también importante el objetivo de ésta en la construcción de ciudadanías activas y más comprometidas e interactivas.

"El objetivo concreto de la gobernanza electrónica es apoyar y simplificar la gobernanza para todas las partes – gobierno, ciudadanos y empresas –. En otras palabras, la gobernanza electrónica emplea los medios electrónicos para apoyar y estimular la buena gobernanza."[16]

Ahora bien, no se puede desconocer que para que esto funcione se necesita también una actitud proactiva y positiva de parte de las propias instituciones y los actores políticos, los que generalmente son reacios al cambio.

Otro elemento importante viene dado por el hecho de que el Estado no es más que una organización más – tal vez en América Latina la más importante - de las existentes en la sociedad y en general las diferentes organizaciones son perfectamente hábiles para manejarse en forma independiente.

De esta manera, el Estado encontrará su tradicional papel paternalista, absolutamente disminuido, debiendo limitarse al ejercicio de la facilitación de la interacción.

4. De la participación de la sociedad civil

"En la década del 80 se verifican las primeras manifestaciones de utilización de las redes, antes del boom de Internet, para vincular activistas de derechos humanos, medio ambiente y paz usando los medios electrónicos. Algunos ejemplos son:

- Peacenet.
- Econet.
- Institute for Global Communications.
- Greennet.
- Association for Progressive Communication."[17]

"Durante la década de los 90, primero lentamente y luego con un crecimiento exponencial un "tercer

14 Carrillo Flórez, Fernando. Ob. Cit.

15 Sarker, Partha. Ob. Cit.

16 Backus, Michael. "E-Governance and Developing Countries: Introduction and Examples". Research Report. IICD, 2001.

17 Nahabetián Brunet, Laura. "Protagonistas del cambio: Derechos ciudadanos y nuevas tecnologías", en Libro de Ponencias del XII Congreso Iberoamericano de Derecho e Informática. Santiago de Chile, 2004

sector" comienza a cobrar forma haciéndose cargo de los temas sociales abandonados por el Estado y nunca contemplados por el mercado. La urgencia que impone el tipo de problemas que quedan desatendidos, además de la magnitud que alcanzan, empuja a la sociedad a actuar. La distancia que separa a los dirigentes de las necesidades de la gente y el descreimiento y la desconfianza de la sociedad respecto a sus representantes, instan a buscar nuevas formas de incidencia.

La escena pública se puebla así de nuevos actores, expresión de la diversidad y complejidad de problemáticas que enfrentan hombres y mujeres en los albores del nuevo milenio. Durante los segundos 90, las TIC, la Internet y una lógica de organización en red facilitan el tejido de lazos sociales que van enredando individuos y organizaciones. Los nuevos movimientos sociales aunque limitados por sus recursos y posibilidades de acceso, comienzan a apropiarse de la potencialidad de las TIC y de la Internet como medio de comunicación interactivo y democratizador tanto del acceso como de la producción de información."[18]

De esta forma, las diferentes organizaciones que iniciaron su accionar en forma solitaria van sumando cada vez más valor y reconocimiento, muchas de ellas ampliando su núcleo de accionamiento a diversas temáticas asociadas a la original, lo que permitió generar canales de interacción entre éstas y dar mayor visibilidad e impacto en las políticas públicas.

Así "estas instancias de participación democrática donde confluyen actores heterogéneos se constituyen en espacios sociales y políticos donde se democratiza información y se genera conocimiento social al pensar soluciones concretas a los problemas reales que enfrenta la sociedad."[19]

De esta forma, las redes electrónicas se caracterizan por la ausencia de una pertenencia a límites o fronteras de tipo geográficos, y por tanto pueden ser consideradas como un "lugar" de privilegio en lo que implica búsqueda de cooperación, interrelacionamiento y de regulación de la globalización. La utilización y apropiación de las tecnologías de la información y la comunicación por parte de los diversos actores sociales en este contexto se transforma en algo absolutamente trascendental.

Las redes electrónicas son un tipo de experiencia cada vez más utilizado por las Organizaciones de la Sociedad Civil. Se trata en definitiva de un bien con valor estratégico, un nuevo actor político por su carácter movilizador. Constituyen un punto innovador y de importante difusión tecnológica, política, cultural y fundamentalmente de participación de la sociedad civil."[20]

Estas redes coadyuvan con esa "necesidad de fortalecer la gobernanza y gobernabilidad democráticas habilitadoras de desarrollo humano, como requisito para revertir el subdesarrollo social, político, económico y humano de la región, imponen subordinar las políticas de e-gobierno y e-democracia a las necesidades impuestas por el gobierno y la democracia reales, integrando las decisiones de políticas TIC para un uso estratégico enrolado en el logro de los objetivos de un fortalecimiento democrático que habilite el desarrollo humano.

Una e-democracia al servicio del desarrollo humano debe favorecer la ampliación de actores autónomos informados y preparados para la participación en la elaboración de propuestas y en la toma de decisiones de políticas públicas que afectan en forma directa su vida."[21]

18 Goldstein, Roxana. "Sociedad de la Información, Democracia y Desarrollo: Las TIC como herramientas para los procesos participativos en la gestión local". Buenos Aires, 2004.

19 Goldstein, Roxana. "Democracia electrónica. Participación ciudadana y desarrollo. El rol de las tic en la construcción de capital social a través del fortalecimiento democrático", en Revista de Derecho Informático Nº 29. Perú, 2000.

20 Nahabetián Brunet, Laura. Ob. Cit.

21 Carrillo Flórez, Fernando. Ob. Cit.

"El desarrollo depende del empoderamiento de las personas y comunidades para tomar el control de sus vidas; el acceso a la información se convierte en un componente esencial para el progreso."[22]

Así es que los ciudadanos digitales – quienes conocen las tecnologías de la información y la comunicación e interactúan con éstas – se dividen en dos grupos prácticamente opuestos: los apáticos y desinteresados y los exigentes y cada vez más comprometidos con los problemas de la vida pública cotidiana.

Éstos forman parte de la generación internet que entiende y aprehendió a las tecnologías de la información y la comunicación como un elemento cotidiano.

La apuesta desde la gobernanza electrónica es doble, por un lado el rescate de los apáticos y por otro la ampliación y crecimiento de la incorporación de las tecnologías de la información y la comunicación.

Aparecen cada vez más, nuevas expectativas de participación en la medida que los consumidores digitales verifican las enormes potencialidades y logros obtenibles a través de internet. Esto obedece también al hecho que las tecnologías de la información y la comunicación tienen por fundamento de base la cooperación, la participación y la accesibilidad, todo lo cual no siempre y necesariamente está presente en la elaboración y aplicación de las políticas de gestión pública.

Sin dudas, las Tic ofrecen la oportunidad de dar nueva vitalidad a los gobiernos, empoderando a los ciudadanos, transformándolos no sólo en clientes digitales, sino en ciudadanos política, económica y socialmente digitales, con la vida facilitada por su intermedio y con ahorros en los gastos públicos y aumento de eficiencia y transparencia. Sin dudas, la asunción por los gobiernos de la necesidad de una redefinición de su funcionamiento, modernizándose, poniendo los énfasis correctos y facilitando la interacción de y entre los actores privados, la sociedad civil y éstos con el Estado, redundará en la obtención de un mejor gobierno.

5. Del gobierno electrónico al gobierno abierto

El gobierno electrónico es lo que facilita la redefinición del concepto de ciudadano facilitando su participación directa en el accionar público, otorgando posibilidades de denuncia, queja, contratación de éstos con el gobierno, entre otra multiplicidad de interacciones posibles.

Ahora bien, esta compenetración entre gobierno y ciudadanos parte de la necesidad de la existencia de los siguientes requisitos:

- Sociológicos: "Pensar en grande, partir pequeño y escalar rápido" dice el refrán de la industria. Esto tiene mucha validez para el mundo del e-gov. Se requiere un plan con una visión ambiciosa y soñadora de manera que capture la imaginación de la gente. Sin embargo, si dicha visión y plan no van acompañados de metas de corto plazo y alto impacto, no se podrá construir una coalición pro cambio y las posibilidades de éxito del mismo caerán."[23] Asimismo, la educación de los usuarios y los recursos humanos debe ser realizada por la administración en conjunto con el sector privado como forma de optimizar tiempos y recursos siempre escasos.
- Tecnológicos: el gobierno electrónico implica la existencia no sólo de las tecnologías de la información y la comunicación sino que éstas estén disponibles para los usuarios ya que si bien las infraestructuras son cada vez más importantes su incorporación social es muy lenta.
- Jurídicos: será imprescindible comenzar por determinaciones normativas que faciliten

22 Vizcarra, Mayte. "La nueva crónica y el buen gobierno en la economía digital", en Revista Electrónica de Derecho Informático N° 29. Perú, 2000.

23 Orrego Larraín, Claudio. "Los Caminos hacia el E-Government", en América Latina Puntogob: Casos y tendencias en Gobierno Electrónico. FLACSO – AICD/OEA. Santiago de Chile, 2004.

y agilicen su incorporación a la vida cotidiana de los ciudadanos. Para esto se deben incluir textos normativos que habiliten la protección de los datos personales, el acceso a la información pública, la interoperabilidad entre las diferentes entidades del Estado, la protección de la seguridad de los ciudadanos.

Los diferentes proyectos de gobierno electrónico deben analizarse y ejecutarse partiendo de la consideración del contexto social, económico, político y educativo de donde se pretenden aplicar.

No es posible no tener en cuenta la enormidad de situaciones problemáticas y la interrelación existente entre éstas y las diferentes organizaciones tanto públicas como privadas.

Por esto, los diferentes actores estratégicos no pueden basar su actuación y la decisión de las políticas a aplicar en relaciones de tipo jerárquico y de autoridad/sanción sino que se torna imprescindible generar consensos y cooperación. De este presupuesto es que parte la gobernanza electrónica para la consideración del gobierno electrónico.

"Con la incorporación del enfoque de la Gobernanza Pública, se enriquece el paradigma de la nueva gestión pública gracias a la incorporación de lógicas para la acción destinadas a desarrollar la capacidad de cooperación e interacción de los actores públicos con otros agentes público-privados. Al gestor público se le atribuyen responsabilidades relevantes al menos en tres niveles: a) el normativo, en el que es necesario abrir un amplio debate sobre los valores de la intervención pública, funciones del gobierno y configuración del proceso decisorio para la colectividad, en las que se entrecruzan el gobierno mismo y los diversos agentes sociales; b) el de formulación de las políticas públicas, donde el gestor deberá preocuparse de tener presentes los diferentes intereses implicados, incluidos aquéllos con una débil representación social; y c) en la ejecución de las políticas públicas, donde son competencias del gestor la innovación y experimentación mediante la introducción de instrumentos cooperativos y formas de asociación público-privadas."[24]

De esta forma la gobernanza se independiza del hecho del gobierno y se vincula más directamente con la coordinación con los gobernados.

Por tanto el gobierno electrónico desde la gobernanza electrónica implicará apoyo, simplificación y garantías para todos los actores estratégicos vinculados, esto es, Estado, ciudadanos y empresas.

"Las TIC son herramientas que permiten, técnicamente, ampliar las posibilidades de un modelo relacional e interactivo de gobernación, que siempre que exista voluntad política, permitirá obtener mejores resultados para el conjunto de la sociedad que los obtenidos por políticas sectoriales y territorializadas.
En esta línea, las iniciativas de e-Gobernanza se plantean como oportunidad para el desarrollo de nuevas dinámicas de relación con los distintos agentes sociales, favoreciendo un diálogo más fluido y una implicación más efectiva. De forma que en la medida en que se incorpore a los ciudadanos a la gobernanza de sus propias comunidades habrá una enorme posibilidad de ganar capital social y contar con mayores posibilidades para resolver de manera efectiva los problemas sociales cada vez más complejos y multidimensionales.
La capacidad del sector privado de incidir en la agenda pública, en materia de incorporación de Internet a las políticas públicas, resulta decisiva. Los actores privados disponen de las tecnologías, el conocimiento y la información necesaria para desarrollar proyectos e iniciativas innovadoras que garanticen la conectividad de los ciudadanos."[25]

Es importante que se consideren también la unicidad y coincidencia en muchos aspectos de los

24 Meneguzzo, Marco. "De la New Public Management a la Public Governance: el péndulo de la investigación acerca de la Administración Pública". Gestión y Análisis de Políticas Públicas (GAPP) Nº 10. Madrid, 1997.

25 Criado Grande, Ignacio y Ramilo Araujo, Carmen. "Hacia una visión integrada del gobierno electrónico", en Revista Vasca de Economía, Ekonomiaz Nº 54, 3er. Cuatrimestre. Vitoria-Gasteiz, 2003.

diferentes objetivos de la gobernanza electrónica y el gobierno electrónico. En efecto, éstos son:

Mayor eficiencia: se trata de un asunto trascendente y de base del gobierno electrónico, de hecho lograrla está en su esencia. La utilización de las tecnologías de la información y la comunicación, reduce las distancias, generando ahorros, disminuyendo costos gubernamentales, incrementando la transparencia, generando mayor accesibilidad a los servicios públicos sustituyendo y complementando los canales tradicionales de comunicación.
De la misma forma y visto este elemento desde la óptica de la gobernanza electrónica sin dudas que éste debe ser un logro de ésta.

En efecto los ciudadanos, en general, desconocedores de las dificultades que implica la articulación para el desarrollo de las políticas públicas, pueden tener a través de las tecnologías de la información y la comunicación un canal impensado hasta hace escasos años, en los que la cooperación transversal para la construcción de éstas sea cotidiano.

Cada vez más es real el hecho de que las políticas públicas necesariamente implican un apoyo activo de la sociedad civil y el sector empresarial.

El liderazgo corresponderá al gobierno. El compromiso sin dudas es compartido.

Mayor responsabilidad: las implicancias que para el gobierno electrónico y la gobernanza electrónica tiene este aspecto está en la base de la construcción de ambas.

Como nunca tal vez, los ciudadanos pretenden estar involucrados y ser parte de la resolución de las cuestiones públicas que les atañen y les determinan sus vidas. Quieren y necesitan involucrarse en los procesos políticos, quizás no en los partidarios y eso explica la apatía partidista frente a la participación puntual en causas comprometidas o en la búsqueda y exigencia de soluciones a conflictos, situaciones o expectativas de acción determinadas.

Esto sin duda genera un doble núcleo de responsabilidades. Por un lado, los ciudadanos que han optado por el compromiso, lo ejercen exigentemente. Por otro lado, se ha vuelto imprescindible el desarrollo de mecanismos de coordinación interinstitucionales, lo que viene determinando una nueva forma de ejercer la política. Quienes lo entiendan, seguirán teniendo la chance de la continuidad política, quienes no lo hagan, serán talvez una anécdota a contarse dentro de la historia de los países.

Gobierno responsable parece ser el centro de la dialéctica política como forma de generar nuevamente confianza de los ciudadanos en sus gobiernos.

Los ciudadanos están reclamando cada vez más dejar de ser consumidores de políticas públicas para ser creadores de tales.

"Ciudadanía activa es una relación basada en la asociación con el gobierno, en la que los ciudadanos activamente se involucran en definir los procesos y el contenido de la política."[26]

De esta forma la realidad indica la existencia de una necesidad de dar respuesta hacia y desde el sistema político y la sociedad civil, de forma de actuar transversal e integradamente como forma de sustentar la coexistencia, la estructura, los componentes y fundamentalmente la gobernabilidad del sistema.

26 Government Online International Network. "Online Consultation in GOL Countries". OCDE. Santiago de Chile, 2001.

Transformación y modernización reales: se verifica aquí la imprescindible acción gubernativa y de las administraciones públicas para construir y luego ejecutar activa y firmemente visiones estratégicas, las que ejercitando un accionar proactivo y dinamizante, actúe y lidere la temática económica y social que afecta a la totalidad de la sociedad.

"Sin duda, el esfuerzo realizado de diseminación de la información a través de Internet incrementa la presión sobre el gobierno para ser más transparente. Sin embargo, es responsabilidad de los gobiernos, decidir, en diálogo con los ciudadanos, empresas y sociedad civil, cómo cuidar el interés público de la mejor manera, conciliando la búsqueda por mejorar la administración del conocimiento con la demanda por la privacidad de la información, y respondiendo a presiones de mayor transparencia y acceso a un costo razonable.

La condición de inmaterial de las agencias virtuales en línea dificulta al ciudadano saber qué agencia gubernamental está realmente proveyendo el servicio o manejando las solicitudes, lo cual erosiona el proceso de rendición de cuentas. Adicionalmente, existe el peligro de que sean los mismos ciudadanos los que se vuelvan más transparentes mientras que las agencias intercambian sus registros personales detallados.

El e-gobierno tiene el potencial de permitir la adopción de prácticas de buen gobierno. Esto significa ser consciente del poder de creación de redes y de la construcción de capacidades de las TIC entre la constelación de los entes interesados, como las administraciones públicas, los ciudadanos, las empresas, las organizaciones de la sociedad civil, los parlamentos y las organizaciones observadoras. También significa tomar decisiones cuidadosas sobre el acceso, la seguridad y la protección de la privacidad de sus relaciones con estos grupos."[27]

De esta forma es posible proponer una visión integradora que abarque a la administración electrónica, en tanto prestación de servicios, a la democracia electrónica, en tanto participación en procesos democráticos, a la gobernanza electrónica en tanto participación horizontal en la elaboración de políticas públicas. Con el foco en la persona y sus derechos, será posible hablar entonces de gobierno abierto.

Finalmente conviene no olvidarse que "la e – governance es considerada una herramienta con un doble efecto sobre las libertades políticas. Si bien convierte a los gobiernos en más transparentes, más eficientes, menos corruptos, impulsa la participación ciudadana y la rendición de cuentas hay que tener en cuenta que también crea mayores oportunidades para la expresión de diferencias políticas en regímenes cerrados que, desde otro lado, se ven contrarrestadas con un mayor control integrado de las actividades de los ciudadanos."[28]

27 Lau, Edwin. "Construyendo una nueva gobernanza a través del e-Gobierno: una visión de la OCDE", en Revista del CLAD Reforma y Democracia N° 31. Caracas, 2005.

28 Rose, Richard. "Global Diffusion Model of e-Governance", en Journal of Public Policy. Cambridge University Press Vol. 25. Cambridge, 2005.

6. Gobierno abierto

"Un Gobierno Abierto es aquél que entabla una constante conversación con los ciudadanos con el fin de oír lo que ellos dicen y solicitan, que toma decisiones basadas en sus necesidades y preferencias, que facilita la colaboración de los ciudadanos y funcionarios en el desarrollo de los servicios que presta y que comunica todo lo que decide y hace de forma abierta y transparente"[29].

"Un gobierno abierto o transparente es esencial para la democracia porque ni los funcionarios públicos pueden ser tenidos por responsables, ni los electorales pueden tomar una decisión electoral fundamentada si no se dispone de una información exacta sobre la actividad del gobierno y las consecuencias de sus políticas. El acceso a dicha información debe considerarse un derecho de los ciudadanos – y de los medios de comunicación en su nombre – y no un favor de los gobiernos, ya que el electorado es el que paga por el funcionamiento del gobierno; es justo, por consiguiente que sepa qué está obteniendo a cambio de su dinero y qué se está haciendo en nombre suyo. Aunque se critica a menudo el hecho mismo de permitir tal acceso porque constituye una sangría en los recursos públicos, es muy útil para mejorar la eficacia del gobierno pues contribuye a denunciar el despilfarro, a inhibir la corrupción y a poner de manifiesto errores de política antes de que se vuelvan crónicos. El hecho de que los individuos tengan acceso a los expedientes personales que el gobierno y sus administraciones llevan sobre ellos es también un factor importante de protección de las libertades civiles.

Un gobierno abierto tiene cuatro características principales. La primera es la comunicación por el propio gobierno de información objetivo sobre sus políticas: en qué hechos se basan, sus consecuencias en la práctica, su costo, las reglas que rigen su aplicación, etc. La segunda es el acceso de los ciudadanos y de la prensa a los documentos gubernamentales, tanto directa como indirectamente a través del parlamento; esto incluye la posibilidad de acceso de los individuos a expedientes personales que les conciernen. La tercera es la apertura de las reuniones al público y la prensa; se puede tratar de las reuniones del parlamento y sus comités, o de las actas de organismos públicos y las reuniones de las autoridades locales. La cuarta es la consulta sistemática por el gobierno a los principales interesados en la formulación y la ejecución de determinada decisión política y la publicación de las informaciones y opiniones recogidas al respecto."[30]

La opacidad, el secretismo y una fuerte cultura del ocultamiento es parte de la realidad cotidiana de las sociedades que están tratando de abrir un camino de transparencia, el que de la mano del acceso a la información pública, es posible sea encontrado.

Se trata de una forma de relacionamiento entre las entidades públicas y las personas que tiene su característica más sobresaliente en la determinación de canales de comunicación y contacto directo entre ellos. Se verifica el desenvolvimiento de una constante conversación con la finalidad de escuchar qué se dice y qué se solicita, a los efectos de fortalecer la toma de decisiones que se hará teniendo en cuenta necesidades y preferencias, facilitando la colaboración de los funcionarios de las entidades públicas y las personas en el desenvolvimiento de los diferentes servicios que presenta y comunicando a su vez lo que decide y ejecuta en forma transparente y abierta.

El gobierno abierto brota en definitiva, desde la convicción de la necesidad de repensar la administración pública, transformar la sociedad y contribuir al desarrollo de democracias saneadas, pasando a las redes y avanzando en el abandono de las jerarquías, asumiendo compromisos de tipo transversal y generar de esta forma valor público. "Se trata de una nueva cultura de la comunicación, un nuevo modelo organizativo y la liberación del talento creativo dentro y fuera de los perímetros de la función pública. No hablamos solo de tecnología, sino de una tecnología social y relacional

29 Calderón, César y Lorenzo, Sebastián Coordinadores. "OpenGovernment: Gobierno Abierto". Madrid, 2010.

30 Beetham, David y Boyle, Kevin. "Cuestiones sobre la democracia: Conceptos, elementos y principios básicos". UNESCO. París, 1996.

que impulsa y estimula una cultura de cambio en la concepción, gestión y prestación del servicio público".[31]

6.1. Un poco de historia

Gobierno abierto no es un tema nuevo. Hacia finales de los años setenta surge por primera vez en forma oficial en el espacio político británico.

Originalmente refiere a diferentes temas relacionados con el secretismo del gobierno así como iniciativas vinculadas con la apertura del sector público de cara a la ciudadanía a los efectos de la obtención de una reducción de la opacidad tradicional.

Con el pasar de los años esta noción fue vinculándose y concretándose hacia una definición de las capacidades de los ciudadanos en una democracia a los efectos de la sostenibilidad de un gobierno que sea responsable por las acciones que ejecuta y evalúe la validez de las medidas que se adopten.

Asimismo refiere a los derechos de las personas frente a la información que se dispone de ellos por parte de las organizaciones públicas con el correspondiente adecuado manejo; motivo por el cual hablar de gobierno abierto tradicionalmente ha implicado un debate vinculado con la libertad de información, la protección de datos, los secretos oficiales y la necesidad de obtención de información vinculada con las acciones del gobierno y su disponibilidad para la opinión pública y las personas en general.

Con la asunción del Presidente Barack Obama como primer mandatario, se inició un camino de concreción hacia lo que ha dado en llamarse "open government". Esto no es otra cosa que una forma abierta de relacionarse gobiernos y ciudadanos.

El presidente norteamericano durante su campaña electoral, utilizó toda una serie de valores y herramientas que implican amplia interacción y apertura concreta para con la información que maneja el gobierno y que debe estar en manos de la ciudadanía. Esto implica tanto como una ampliación del dominio público imprescindible en una democracia transparente y conectada.

Este open goverment es aquel gobierno que entabla una constante conversación con los ciudadanos con el fin de oír lo que ellos dicen y solicitan, que toma decisiones basadas en sus necesidades y preferencias, que facilita la colaboración de los ciudadanos y funcionarios en el desarrollo de los servicios que presta y que comunica todo lo que decide y hace de forma abierta y transparente.

Según los expertos y particularmente de acuerdo con el Memorandum sobre Transparencia y Gobierno Abierto de enero de 2009 de los Estados Unidos de Norteamérica es posible indicar que los principios del gobierno abierto implican:

- Transparencia (saber) en la acción de gobierno, tanto en la forma en la que los ciudadanos conocen cómo se gastan sus impuestos como con la apertura de datos producidos por las Administraciones Públicas. Se trata de proporcionar información sobre lo que se está haciendo, sobre la planificación de actividades, en relación con las fuentes de datos y en vínculo con todo lo que es posible que sea considerado responsabilidad frente a la sociedad. En efecto, esto fomenta y promueve la rendición de cuentas de las administraciones para ante la ciudadanía y por tanto genera un permanente contralor social.
- Participación (ser parte de) aprovechando la inteligencia colectiva de los ciudadanos y apertura de su agenda a la ciudadanía. Todas las leyes, decretos, medidas o decisiones de otro tipo que toman los Gobiernos pueden ser debatidas, valoradas, criticadas y completadas (incluso antes de su elaboración) con las opiniones de los ciudadanos. Se trata de promover el derecho de las personas de participar en forma activa en la formulación de las diferentes

31 Diario Cinco Días. "Open Government y crisis económica". Columna de opinión del día 5 de enero de 2011. Madrid, 2011.

políticas públicas facilitando el camino para que las administraciones públicas obtengan beneficios del conocimiento, ideas y experiencias de las mismas. Verifica la promoción de nuevos espacios de vinculación favoreciendo el protagonismo y la implicación de todas las personas en los asuntos de todos.

- Colaboración (contribuir) entendiendo el gobierno como plataforma tecnológica de servicio que construye aplicaciones que pueden ser reutilizadas por otras administraciones, colaborando las distintas instancias de la administración entre sí, así como con la empresa privada y los ciudadanos. Se trata de implicar a las personas en el esfuerzo del trabajo conjunto transversal y entre las organización de todo el aparato público con el privado.

"El presidente Obama prometió en su campaña: democracia conectada y transparente, acceso online a los datos de la Administración y a los contratos públicos, fomento de la participación ciudadana a través de consultas y comentarios sobre los proyectos, herramientas sociales para una ciudadanía 3.0 y dar a la sociedad lo que es suyo, excluyendo restricciones a la propiedad y acceso de los datos y documentos públicos."[32]

6.2. Hacia la construcción del gobierno abierto

Tal como ha establecido Villoria[33], es indudable que una democracia de calidad exige un Gobierno abierto y transparente, que rinda cuentas y exija, además, una sociedad estructuralmente democrática, esto es, una sociedad donde las organizaciones de la sociedad civil sean democráticas y la propia administración abra vías de participación y deliberación a los afectados por sus decisiones.

Establece asimismo, una determinación sintética de las justificaciones que permiten hablar perfectamente de la vigencia y necesidad de la promoción de políticas vinculadas con la concepción actual de gobierno abierto:

- "Un Gobierno opaco no aporta información suficiente para configurar adecuadamente el voto, abusa de las asimetrías de información y reduce la calidad del voto.
- Un Gobierno opaco se apodera de lo público y lo gubernamentaliza en el mejor de los casos o lo patrimonializa en el peor.
- Un Gobierno opaco impide comprobar la imparcialidad de sus decisiones.
- Un Gobierno opaco que no rinde cuentas no se somete realmente al derecho.
- Un Gobierno que no rinde cuentas no aporta información para definir el voto con independencia. Un Gobierno que no rinde cuentas traiciona la soberanía popular y la igualdad política."[34]

En definitiva lo que existe es un compromiso de garantizar que todos los aspectos de forma tal que el Gobierno y los servicios públicos sean administrados y operados, estén abiertos al eficaz escrutinio público y a la supervisión de la sociedad. Esto debe acompañarse de la progresiva expansión de espacios de diálogo, participación y deliberación en conjunto con todas las personas, y de la imprescindible apertura hacia la colaboración para la obtención de las imprescindibles soluciones a problemas públicos cada vez más complejos, mediante el aprovechamiento del potencial y las energías disponibles en los diferentes sectores de la sociedad.

Por otra parte, se ha demostrado que cuanta mayor apertura, mayor ampliación de los índices de felicidad en los ciudadanos y éstos se implican de forma más concreta en las distintas tareas de Gobierno, de manera tal que surge un círculo virtuoso en una sucesión que comprueba que cuanto más abierto es un Gobierno, se genera mayor participación y por tanto se exige más transparencia, lo que en definitiva, promueve esfuerzos por desarrollar mejores prácticas que, dado el ciclo, nacen con

32 Obama, Barack. "Vote for change". Washington, 2008.

33 Villoria, Manuel. "La democratización de la administración pública: marco teórica", en Gobernanza democrática y fiscalidad: una reflexión sobre las instituciones. Madrid, 2010.

34 Villoria, Manuel. Ob. Cit.

el respaldo ciudadano suficiente para disponer de legitimidad y adecuados niveles de aprobación[35].

6.3. Principales beneficios

Es en mérito a los señalamientos efectuados que se entiende pertinente considerar cuáles son los principales beneficios que el gobierno abierto aporta. En este sentido y sin pretensión de taxatividad, se señalan los siguientes:

- Restablecimiento de confianza en el gobierno. Esta es el resultado esperable luego del reforzamiento de algunos otros aspectos vinculados, en la medida que las personas confíen reforzarán su desempeño en sus diferentes áreas de influencia.
- Garantía de mayores resultados a menor costo. Esto se debe a la coparticipación y coejecución de programas y servicios con las personas y la sociedad civil en su conjunto.
- Elevación de los niveles de cumplimento por parte de las personas en relación con las decisiones que se adoptan en la medida que son incorporadas por así ser percibidas como legítimas.
- Seguridad de la equidad de acceso en la formulación de políticas públicas a través de la reducción de los requerimientos para incorporarse en los procesos de participación.
- Fomento de la innovación y de otras actividades de tipo económico, siendo que cada vez con mayor fuerza son reconocidos éstos como motores de la innovación y creación de valor tanto para el sector público cuanto para aquél privado.
- Mejoramiento de la eficacia a través del aprovechamiento de conocimiento y recursos de las personas que pudieren estar enfrentando barreras para su participación. Esto facilita la especificidad de las políticas públicas

6.4. Características fundamentales

De acuerdo con lo establecido es posible indicar que las principales características a los efectos de la existencia de un Gobierno con calificación de abierto son las siguientes:

- Transparencia, esto es, las acciones y las personas responsables de éstas deben estar sujetas al escrutinio público y pudiendo ser éstas impugnadas por otro lado siendo pasible de exigencias de información.
- Accesibilidad por parte de cualquier persona, en todo momento y lugar, por lo que puede afirmarse que los servicios públicos y la información sobre éstos deben estar fácilmente accesibles para los ciudadanos.
- Receptividad, a las ideas, reclamos y criterios de las personas en el iter de la decisión
- Apertura en sentido amplio. Es importante considerar que la condición de apertura es más abarcativa que la transparencia, en la medida que implica tanto a la accesibilidad como a la capacidad de respuesta, esto es accesibility más responsiveness, lo que tiene por finalidad incluir más cualidades en la interacción entre gobierno y ciudadanía.

A lo antedicho se debe adicionar que indudablemente el Gobierno abierto fortalece la democracia al permitir el escrutinio público, generando un baluarte contra la acumulación excesiva de poder brindando mayores oportunidades para la
participación de la ciudadanía.

Múltiples políticas que se impulsan para una mayor apertura reconocen en forma explícita la contribución que estas medidas tienen en la mejora de la gobernanza democrática.

En algunos países se reconoce que un gobierno abierto es incluso una condición siempre necesaria aunque no suficiente para el fortalecimiento del buen gobierno.

35 Rainie, Lee y Purcell, Kristen. "How the Public Perceves community Information Systems". Pew Internet Research Institute. Disponible en: http://www.pewinternet.org/~/media//Files/Reports/2011/Pew_Monitor_Communityinfo.Pdf (Página visitada el 27 de agosto de 2013).

Sabido es que precisamente la obtención del buen gobierno implica incluso la aplicación de medidas transversales que fortalezcan la capacidad que la sociedad civil tiene para el aprovechamiento de este nuevo contexto.

En términos económicos los beneficios de un gobierno abierto parecen casi obvios. Sabido es que los países con los mayores niveles de transparencia y contralor parlamentario efectivo disfrutan de los mayores niveles en términos de calidad de vida de sus ciudadanos; la mayor apertura tiene un impacto fuertemente positivo en el rendimiento de las políticas públicas aplicadas en las áreas sustanciales de gobierno como pueden ser aquéllas vinculadas con las actividades regulatorias, presupuestarias o de gestión del gasto público.

En términos institucionales también es central la importancia del gobierno abierto, ya que las estipulaciones legales y su cumplimiento efectivo en la implementación de las políticas públicas con asiento en la institucionalidad democrática genera seguridad jurídica y fortalece la gobernabilidad democrática, consolidando una cultura favorable a la apertura en el sector público que se trasunta incluso hacia el sector privado.

7. Datos abiertos

Es posible establecer que todos los datos producidos por las entidades públicas, son datos públicos – de principio – y solamente serán realmente tales si son puestos a disposición en línea en formatos abiertos, usables, reutilizables y bajo licencias abiertas.

A esto refiere el nuevo paradigma de los datos abiertos, el que consiste en ubicar todos aquellos datos públicos que no impliquen afectación a derechos fundamentales en disposición de ser reutilizados por la ciudadanía, las organizaciones sociales, o las empresas de forma tal que sea posible la generación de una efectiva transparencia en las entidades e inclusive riqueza y puestos de trabajo en el incipiente sector infomediario.

Con la publicación de datos abiertos, los gobiernos son más capaces de centrarse en aquello para lo que mayor expertisse poseen, esto es, recopilar y gestionar registros fidedignos acerca de actividades públicas claves, permitiendo que otros colaboren y compitan para avanzar en la concreción del resto de las acciones. Las personas, las empresas y las organizaciones que trabajan para lograr que los datos gubernamentales sean más útiles y más accesibles, en general tienen una gama amplia de opciones, recursos y capacidades que supera a aquélla que poseen los gobiernos por sí.

Desde el punto de vista tecnológico el basamento del tema consiste en publicar los datos en un formato electrónico que a todos les resulte de sencilla utilización. Algunos de dichos formatos – como por ejemplo las imágenes escaneadas de documentos – son de simple creación, pero presentan dificultades para el análisis, el mapeo y la combinación para con otra información siendo que además tampoco es sencillo el desenvolvimiento de búsquedas en su interior. Formatos tales como una hoja de cálculo o una base de datos aparecen como de mayor simplicidad al momento de su reutilización en mérito a que su manipulación es más fácil en los diferentes software - datos estructurados - .

Si se colocan datos en formatos estructurados, el Gobierno puede capacitar a todos los sectores para que agreguen valor a los datos, creando en su entorno nuevas interfaces y herramientas, contribuyendo a que el Gobierno obtenga en mejor forma sus propios objetivos. Generalmente, cuando los gobiernos recopilan o crean información, lo hacen con una motivación unida a una particular utilización que se le dará a los datos.

Publicar datos abiertos activa un motor innovador, capacitando las empresas privadas, los grupos de la sociedad civil, las personas en general, para la obtención de un nuevo valor de la información que el gobierno reúne con dedicación a otros usos hasta ahora tan inesperados como valiosos.

Toda esta nueva movilización a favor de los datos abiertos de gobierno se encuentra todavía en sus primeros desarrollos, de tal forma que los líderes de gobierno que sean capaces de aprovechar las oportunidades que ésta genera tendrán la chance de creación de beneficios múltiples transformándose a su vez en líderes en un tema absolutamente emergente. En los diferentes niveles de gobierno se está avanzando – tal vez sin prisa pero sin pausa – de forma tal de concretar el uso de las tecnologías para el mejoramiento de la entrega de servicios de calidad, incrementando la participación, facilitando el fomento de la responsabilidad, estimulando la innovación y el emprendedurismo.

Ahora bien, es importante también tener en cuenta que el hecho de proporcionar datos abiertos no genera su propia demanda. En efecto, los proyectos vinculados con datos abiertos que son exitosos son los que están orientados a dar satisfacción a la demanda existente de información o donde el gobierno desarrolla un interés y compromiso con los interesados, en relación con los datos que por alguna razón decidió publicitar. Hablar de éxito efectivo en estos proyectos en general está vinculado con una fuerte asociación entre el gobierno y los actores de índole privada.

Las oportunidades se multiplican para los líderes de gobierno si son capaces de apropiarse en forma efectiva del verdadero significado de la apertura de datos, ya que mediante modificaciones simples se obtienen beneficios sustanciales con la tecnología disponible. Pero para obtener un beneficio pleno, es imprescindible darle impulso a esta nueva formulación desde la lógica organizacional y cultural mucho más que desde aquélla tecnológica. Toda esta concepción vinculada con la necesidad de invertir en datos abiertos implica una realineación fuerte pero gradualista dentro de la estructura burocrática gubernamental lo que implica que deben examinarse las plataformas tecnológicas a los efectos de la publicación de los datos gubernamentales, determinando a su vez, modificaciones en los procedimientos administrativos que incentiven a los funcionarios a que utilicen estas plataformas.

Ahora bien para evitar frustraciones es importante tener presente que "los datos gubernamentales se pueden haber vuelto más abiertos, pero el Gobierno en sí, no."[36]

Esto significa que la tecnología no sustituye ni da garantías al incremento significativo de la transparencia gubernamental más allá del punto de partida antes del inicio de los proyectos de apertura de los datos. Estas modificaciones implican cambios importantes en las bases mismas de las políticas que se instrumentan, los que sin lugar a dudas exacerban el alcance de la tecnología.

Así es que cuando la información gubernamental ya es pública, un determinado software de datos abiertos puede hacer de la información algo mucho más utilizable y valioso. Sin embargo, el requerimiento relativo a qué datos se deben publicar – esto es qué cuestiones vinculadas con los trabajos internos del gobierno se deben revelar sin cortapisas al público – es una determinación que el sistema político en su conjunto debe acordar y responder.

Es importante de todas formas no confundirse, los datos abiertos no son una panacea y no siempre son de instrumentación simple.

36 Ramírez Alujas, Alvaro.- "Innovation in Public Management and Open Government: An old new idea...", en Revista Buen Gobierno para pensar en la Democracia. México, 2010.

8. Otro elemento a no perder de vista

Es la importancia creciente de la consideración de pública de la información, los códigos abiertos y la colaboración.

"En la era de la información, la sostenibilidad del sector público dependerá también de que asuma una cultura laboral de la innovación basada en la pasión creativa en red y en una relación más flexible con el tiempo, algo que sólo es posible si se efectúa un cambio consciente de la cultura de la administración pública. Solamente a través de tales mejoras de la productividad basadas en la innovación podrá el sector público continuar suministrando una base sostenible para la era de la información global y no será eliminado por obsoleto".[37]

8.1. Open Source Governance y Wiki Government.

En esta lógica de gobierno de la información, apertura de datos y gobierno abierto así como las modificaciones que se han venido verificando en el entorno de Internet, es que se han desenvuelto otros criterios que van desde el acceso a la información hasta los mecanismos de códigos abiertos y colaboración.

En efecto, se verifican desarrollos vinculados con la teoría de la Gobernanza de Código Abierto (Open Source Governance) que procura la aplicación de la filosofía del movimiento del Software Libre y de contenidos abiertos a los principios democráticos, a los efectos de habilitar que cualquier persona interesada en participar y estar más directamente implicada en – por ejemplo – el proceso legislativo, efectivamente pueda ejecutarlo.

En vínculo directo con la gobernanza de código abierto surge la aplicación del concepto de Wiki como herramienta colaborativa apareciendo otro neologismo en este nuevo escenario de los asuntos públicos en el siglo XXI: WikiGovernment, es un modelo de gobierno basado en los conceptos de código abierto y "Wiki"(...) El pináculo de esta teoría es que permite a miembros de la comunidad en cualquier jurisdicción el acceso directo a sus leyes.

Utilizando el estilo de edición Wiki, las personas pueden realmente editar – y procesar – sus demandas en las leyes"[38].

8.2. Open Politics

Finalmente, en esta lógica en la que a partir de las dimensiones del gobierno se añade la participación conjuntamente con la figura del gestor político aparece el concepto de "Open Politics". Éste combina aspectos centrales de los movimientos de software libre y contenidos abiertos, reclamando la promoción de mecanismos de toma de decisiones más abiertos, menos antagónicos, y con mayor capacidad para la determinación de lo que es el interés público con respecto a las cuestiones de política pública. En este ámbito, los criterios que lo sustentan son:

- Cualquiera puede participar, incluso anónimamente.
- Igualdad de los participantes, resolviéndose las eventuales controversias mediante la igualdad de las relaciones de poder.
- Accionamiento transparentes, y ninguno tiene más poder para revisarlas que cualquier otro.
- Registro y preservación de todas las contribuciones estando vedada la alteración de los mismos.

37 Himanen, Pekka. "La ética del hacker y el espíritu de la era de la información". Disponible en: http://eprints.rclis.org/bitstream/10760/12851/1/pekka.pdf (Página visitada el 27 de noviembre de 2013).

38 Ramírez Alujas, Alvaro. Ob Cit.

- Estructuración efectiva o eventual de los mecanismos de solución de controversias.
- Organización y reorganización de todos los contenidos será siempre carga de los participantes.
- Los accionamientos de tipo político tienen su límite dado por los formatos, las reglas establecidas y las leyes existentes en la comunidad de que se trata y que en mayor o menor medida se verá afectada por la decisión de tipo político.
- El contralor del foro podría idealmente, trasladarse a la mayoría de los usuarios de confianza.

9. ¿Apertura del gobierno o apertura de mentes?

Humberto Maturana ha establecido que "la noción de transformación contiene, en la evocación de lo que se hace, la atención a la dinámica relacional de su carácter sistémico como un proceso de cambio en torno a algo fundamental que no cambia sino que se conserva a través de los cambios". Así, lo fundamental en la noción de transformación es lo que se conserva, y lo que se conserva le da sentido a lo que cambia. "La noción de transformación, por lo tanto, trae consigo las preguntas ¿qué es lo que se quiere conservar? y sobre todo, ¿qué queremos conservar? Lo que nos deja de inmediato frente a la tarea de declarar nuestros deseos haciéndonos responsables de ellos"[39].

En caso de responder a estas cuestiones determinando las necesidades de nutrición, cuidado y desarrollo acordes para el bien común de las sociedades en que hoy se participa así como la conservación de una forma de vida y convivencia democrática, todas las modificaciones que se presenten no estarán necesariamente unidas al contenido de tipo tecnológico en tanto intermediario facilitador de la coherencia de las diferentes dimensiones de operación y relacionamiento sino que se necesita un involucramiento para con la nueva conciencia y corporalidad de las cosas, tanto en lo que refiere a las personas que las habitan como para la configuración de lo cotidiano.

Así esta apuesta por la apertura del gobierno puede perfectamente transformarse en una apuesta real para modificar lo público, para cambiar estructuras anquilosadas desde hace tanto y verificarse en un estado de la mente y el espíritu para todas las personas involucradas.

"El advenimiento de una nueva configuración paradigmática que aún no destila formas definitivas pero que entrega fugaces orientaciones sobre lo que podría ser el futuro de los asuntos públicos, y desde donde el Ogov puede perfectamente ser reconocido como una revolución silenciosa que podría ubicarse – de manera potencial – en el plano de las innovaciones de carácter sistémico o transformacional, cuyo efecto dominó genere un impacto profundo en la manera de entender, estar y actuar en nuestras democracias, sus prácticas constitutivas y las instituciones que la configuran"[40] es que surgen opciones, análisis y criterios superadores que se asocian directamente con la centralidad humanista de la acción política pública, para determinar diferentes opciones que enriquecen el debate de la apertura de datos y por ende los desafíos a que se enfrenta la sociedad de la información, en su mérito.

La información que se encuentra en poder de los gobiernos es una forma de infraestructura, tan fundamental como lo pueden ser otras centrales que han sido incorporadas a la cotidianeidad social y respecto de las cuales nadie duda de su condición de imprescindibles: transparencia, rendición de cuentas, o simplemente energía. Como resultado entonces de los flujos de información con los ciudadanos, la información les permitirá formular opciones de innovación, de participación y de actuación.

Ahora bien, los datos públicos del gobierno son elementos de gran valor siempre que sean compartidos bajo criterios de libertad y con formulaciones vinculadas a principios y estándares comunes. De esta forma, la información entendida bajo la lógica del nuevo paradigma de los datos abiertos de

39 Maturana, Humberto. "A ontología da Realidade". Belo Horizonte, 1997.

40 Ramírez Alujas, Alvaro. Ob. Cit.

gobierno deberá cumplimentar en primera instancia, requisitos tales como confiabilidad, facilidad de uso, actualización, consistencia y facilidad de interpretación, así como usabilidad, reutilización y redistribución. Esto sin lugar a dudas es obtenible a partir de la máxima apertura de los flujos de información que pueden fomentarse mediante la utilización de redes abiertas.

Ahora bien, el objetivo de este gobierno abierto no es únicamente la comunicación de información sino el traslado de poder efectivo a los ciudadanos como una forma de dar cumplimiento a los compromisos vinculados con la democratización de la información. Por lo tanto, el desafío fundamental está ubicado en la creación de estándares y el reconocimiento de las mejores prácticas que faciliten la adopción de regulaciones normativas y políticas públicas que estén acordes con los estándares y principios acordados por la comunidad internacional.

El adentrarse en las dinámicas del gobierno abierto en las tradicionales estructuras gubernamentales públicas es una tarea de tipo titánico. Lo primero a considerar debe vincularse con la remoción de las estructuras mentales prevalentes; es imprescindible una modificación cultural y emocional hacia la interna de la entidad de que se trate. Ahora bien, generar modificaciones en esos dominios de conductas relacionales así como las capacidades requeridas, implica tiempo y sustanciales esfuerzos, nada menores por cierto. Pero es posible un camino que puede implicar la reorientación de las distinciones partiendo del progreso para llegar a la innovación.

La gobernanza por su parte, en tanto forma de guiar a la sociedad para la mejor consecución de sus metas e intereses necesita de la fortaleza de un buen gobierno.

Éste en tanto institución, es su principal instrumento. La optimización de los mecanismos de toma de decisiones, la reordenación de los recursos humanos y financieros, facilitando la autorregulación en la toma de decisiones habilita que la gobernanza pueda definirse en forma independiente de la acción de gobernar y por tanto obtener el consentimiento de los gobernados.

La propagación de los programas de desarrollo de gobierno abierto ha venido asociada a campañas de lucha contra la corrupción, así como a la promoción del mejor aprovechamiento de las tecnologías de la información y la comunicación. Sin embargo, hay que tener presente que la mera existencia de portales web de los organismos públicos y privados, no determina la existencia o no de corrupción, sino que simplemente permite la difusión de información.

Hoy día el espacio electrónico es un espacio muy importante de acumulación de capital y por tanto y en función de las relaciones que se efectivizan por su intermedio es un espacio de mucho poder. "La globalización de los sectores económicos corporativos están en la red y son propietarios de ella y así como hay concentración de la economía global lo hay en las ciudades globalizadas. Esta hiperconcentración del espacio electrónico ha llevado a la segmentación entre espacio electrónico público y el privado. El espacio público no está en condiciones de enfrentar al espacio privado y es por ello que resulta cooptado. Con las desregulaciones y la industrialización del sector electrónico, los sistemas de comunicaciones nacionales están integrados a redes globales y los gobiernos nacionales pierden control."[41]

El gobierno abierto puede ser una herramienta muy fuerte para mejorar la calidad de vida de un país y su gente, porque modifica al gobierno en su conjunto, transformándolo en una entidad receptiva a sus ciudadanos. La idea es desarrollar buen gobierno y para esto, el centro debe ser servir a los ciudadanos que acceden y reciben servicios gubernamentales de todo tipo.

En definitiva entonces, la apuesta debe ser por un desarrollo basado en las tecnologías de la información y la comunicación y ésta debe estar en el centro del desarrollo de cualquier plan de crecimiento económico. Sin lugar a dudas uno de sus puntos fuerte deberá centrarse en los planes de gobernanza; ésta deberá estar basada en la consigna: crecimiento con equidad.

41 De Saskia, Sassen. "Los espectros de la globalización". Buenos Aires, 2003.

"Al presente la noción de gobernanza se asocia a las de buen gobierno y buena administración, aspirando a colocar en el centro del sistema a la persona y sus derechos fundamentales.

En la medida que el centro de la acción pública es la persona, el individuo humano no puede ser entendido como un sujeto pasivo, mero receptor o destinatario de las decisiones políticas. Como bien se ha destacado, "Definir a la persona como centro de la acción pública significa no sólo, ni principalmente, calificarla como centro de atención sino, sobre todo considerarla el protagonista por excelencia de la vida política. Aquí se encuentra una de las expresiones más acabadas de lo que entiendo por buen gobierno, por buena administración en el marco democrático ... Afirmar que la libertad de los ciudadanos es el objetivo primero de la acción política significa, en primer lugar, perfeccionar, mejorar los mecanismos constitucionales, políticos y jurídicos que definen el Estado de Derecho como marco de libertades. Pero en segundo lugar, y de modo más importante aún, significa crear las condiciones para que cada hombre y cada mujer encuentre a su alrededor el campo efectivo, la cancha, en la que jugar libremente su papel activo, en el que desarrollar su opción personal, en la que realizar creativamente su aportación al desarrollo de la sociedad en la que está integrado. Creadas esas condiciones, el ejercicio real de la libertad depende inmediata y únicamente de los propios ciudadanos, de cada ciudadano. El buen gobierno, la buena administración ha de mirar precisamente la generación de ese ambiente en el que cada ciudadano pueda ejercer su libertad en forma solidaria."[42]

Es una verdad inequívoca que como pocas cosas en el mundo, el gobierno electrónico está al alcance de todos tanto en el mundo en desarrollo cuanto en el desarrollado. La tarea de los líderes de gobierno es comprometerse y hacer real la frase de Carlos Reyles: "la vida nueva no saldrá de moldes viejos, sino que la vida nueva ha menester una nueva concepción de la vida".

42 Delpiazzo, Carlos. "Marco conceptual de la gobernanza con especial referencia a Internet". Ponencia preparada para el XII Congreso Iberoamericano de Derecho e Informática. Zaragoza, 2008.

CAPITULO VI

SMART DATA

Dra. Silvana Casciotti

SMART DATA

Dra. Silvana Casciotti

1. Introducción

Existen dos acepciones del concepto de Smart Data; hay quienes entienden el concepto de Smart Data como Big Data, al que se hará referencia en las próximas líneas, y otros que los diferencian entre sí.

El avance tecnológico que se ha generado en la última década ha llevado a que la información generada crezca de forma vertiginosa. Las nuevas generaciones aumentan permanentemente el volumen de los datos generados independientemente del dispositivo que estén utilizando (móviles, tablets, laptops, entre otros).

El concepto de **Big Data** aplica a toda aquella información que no puede ser procesada con los sistemas y herramientas tradicionales, ya sea debido a su volumen, variedad o velocidad de la misma. Las tecnologías **Big Data** surgen para dar solución al problema que tienen tanto empresas como administraciones públicas cuando la información que manejan excede la capacidad de almacenamiento, procesado y análisis de la organización.

Redes sociales como facebook, twitter y foros, nos permiten expresar y compartir momentos y emociones en tiempo real. En este sentido, la información que se puede obtener en el momento en que se comparte una foto, se realiza un comentario, o se hace una transacción, es amplia. Dentro de ésta se encuentra: información personal, redes de amigos, y conocer dónde se encuentra la persona en ese momento, es decir, se puede geo referenciar la ubicación de los usuarios.

Si recolectamos todo ese cúmulo de información para una ciudad o un país, a esta enorme masa de datos la podríamos llamar Big Data.

2. Concepto

Smart Data es el concepto de privacidad para el futuro, dejando a los datos o a la información que piense por ella misma y el programa que se adapte, siendo el contexto la clave. En privacidad resulta de suma importancia conocer el contexto y nadie sabe mejor que el propio usuario cómo deben usarse sus datos dependiendo del contexto.

A través de smart data se personifica el concepto de Privacy by Design. La razón por la cual Privacy by Design es una herramienta muy efectiva, es que es proactiva, previene y se anticipa a los daños que puedan afectar la privacidad.

El usuario lleva el control, el usuario conoce el contexto, da las instrucciones que se verán reflejadas en el mundo smart data.

Smart data está integrada por agentes virtuales que actuarán conforme a las instrucciones que les haya dado el usuario. La data vive en línea y refleja las preferencias de los usuarios en cuanto al uso y la divulgación de los datos personales**.**

Las personas no proporcionan voluntariamente sus datos personales y la revelación de información ocurre por varios factores:

- los seres humanos no siempre toman decisiones racionales. Las recompensas a corto plazo hacen que las personas tiendan a aceptar riesgos a largo plazo. Los beneficios del intercambio de información son por lo general mucho más evidentes
- Los comportamientos de protección de la privacidad consumen tiempo y conocimiento.
- Falta de conocimiento. El usuario no es consciente de la cantidad de datos personales que se recolecta y la manera en que dichos datos pueden ser analizados.
- Falta de alternativas. En muchas ocasiones el usuario está obligado a elegir entre privacidad y seguridad pública, entre privacidad y mejor servicio al cliente, por ejemplo.

Estos factores producen consecuencias negativas no sólo para los usuarios sino también para los proveedores de servicios. Para ser efectivos necesitamos tecnología para poder eliminar estos factores o las consecuencias de los mismos. Se pretende apoderar al usuario con herramientas tecnológicas, en particular con un representante o agente virtual que proteja sus datos personales.

Dicha tecnología debería permitir a los usuarios adoptar por defecto un comportamiento para proteger la privacidad; el agente virtual debe ser capaz de reducir el esfuerzo cognitivo requerido por el usuario para controlar sus datos personales; monitorear y proveer retroalimentación pertinente a los usuarios.

2.1. Smart Metering o Medidor Inteligente

No existe una definición estándar para el término "medidor inteligente", de hecho, el término ha sido aplicado a una variedad de dispositivos que incorporan funcionalidades diferentes. Hay, sin embargo, ciertas características básicas que tienen en común la mayoría de los medidores inteligentes actualmente desplegados. La más importante de estas cualidades es la medición digital del consumo de energía en los hogares en un nivel relativamente adecuado de granularidad - lecturas por horas de energía utilizada, por ejemplo. Esta granularidad permite la colección del "consumo por intervalo" de datos y permiten la posibilidad de que se facture por tiempo de uso.

Estos medidores inteligentes también pueden estar equipados con una memoria interna suficiente para permitir el almacenamiento de todas las lecturas para al menos un período de seis meses.

Por lo general, los medidores inteligentes están equipados con la funcionalidad de comunicación bidireccional. Esto permite utilidades para leer a distancia los contadores (a un costo significativamente reducido, en comparación con la lectura in situ realizada por un empleado de la empresa proveedora del servicio), y cada vez resulta más propicio para controlar el intervalo histórico de consumo a través de portales web en línea.

Algunos medidores inteligentes con capacidades de comunicación bi-direccional también pueden estar equipados con habilitación remota y desactivación de la funcionalidad de la oferta, lo que permite una utilidad para conectarse de forma remota o desconectar el consumidor. Esta característica permite a los servicios la posibilidad de habilitar el suministro de energía a las nuevas cuentas y desactivar el suministro de energía a las cuentas existentes sin tener que enviar a un técnico de servicio al sitio donde se encuentra la cuenta. También permite la aplicación de un sistema de tarifa pre-pago.

Finalmente, aunque la medición inteligente hasta la fecha se ha centrado en el consumo de energía eléctrica, se anticipa que los medidores inteligentes también pueden utilizarse para agua, gas, y calor. En consecuencia, algunos agentes inteligentes están siendo diseñados para apoyar la medición de utilidades múltiples con el fin de evitar la innecesaria duplicación de la infraestructura.

3. Problemas que presenta para la privacidad

Desde su lanzamiento, numerosos grupos y organismos reguladores se han centrado en la necesidad de proteger la privacidad de los consumidores en la red inteligente. Esta necesidad surge a partir del aumento de los flujos de datos en este sistema.

Este aumento en los datos de consumo eléctrico está emparejado con la lectura remota y la recogida de los datos, que plantean plantear cuestiones en relación con la transparencia y el control de consumo de datos.

La investigación sugiere que a medida que la red inteligente madure, los estilos de vida del consumidor podrían deducirse perfectamente de la información generada. A través las inferencias sobre el tiempo de uso y otros factores, puede ser posible determinar si los individuos tienden a cocinar las comidas para microondas o comidas en el horno, si toman el desayuno, la hora en la que los individuos están en su casa, si una casa cuenta con un sistema de alarma y la frecuencia con que se activa, cuando los ocupantes generalmente toman una ducha, cuando la TV y / o el ordenador está encendido, si los aparatos están en buenas condiciones, el número de aparatos en el hogar; si la casa tiene una lavadora y secadora y la frecuencia con que se utilizan, ya sea las luces y aparatos se utilizan en las horas impares, como en el medio de la noche, y / o si y con qué frecuencia utilizan equipos tales como una cinta de correr.

En combinación con otra información, que se puede derivar, por ejemplo, que el dueño de casa tiende a llegar a casa tarde, el individuo posee sueño inquieto o falta de sueño, el ocupante sale tarde al trabajo, el dueño de casa rara vez se lava las / sus ropas, la persona deja a sus niños solos en la casa, entre otros. Aunque el uso de electricidad no se registra minuto a minuto, la vigilancia constante del consumo de electricidad puede revelar el número aproximado de ocupantes en un hogar, cuando están presentes, así como cuando está despierto o dormido.

Esto puede poner en peligro la noción de la "Intimidad del hogar", donde esos detalles íntimos de la vida diaria no debe ser accesible sin el conocimiento del ocupante (s), existiendo el riesgo de que la información de identificación personal sea utilizada para fines distintos que para los que originalmente fueron recogidos.

4. Smart metering y Privacy by Design

En febrero de 2011, el Grupo de Expertos de la Comisión Europea 2 (EG2) afirmó que "en Europa el robo de energía y la privacidad son las preocupaciones más importantes relacionadas con la implementación de la red inteligente Smart Grid.

Se ha sugerido que "el dilema del sector de la energía tiene que ser abordado por adelantado ya que es la mejor manera de entregar niveles apropiados de seguridad y privacidad, y son esenciales para facilitar el consumo de buy-in ".

En particular, una recomendación clave del informe de los EG2 detalla la necesidad de los pilotos adicionales en el manejo de los datos para proponer una lista de principios de primer nivel con destino al entorno de las redes inteligentes, donde los operadores de la misma puedan diseñar sus sistemas y procesos.

Los estándares de la protección de la privacidad desde el diseño ha devenido un sello de calidad de privacidad y seguridad de la red y medidores inteligentes. Por ejemplo, en setiembre de 2011 el Grupo Internacional de Trabajo de Protección de datos y Telecomunicaciones adoptó un documento llamado: Privacidad en el diseño y Medidores inteligentes: Minimizar la información personal para mantener la privacidad.

Recomendaciones de la Privacidad en el diseño para los Smart Meters:

- En las iniciativas de medición inteligente deberían figurar los principios de privacidad en la gestión global del proyecto marco y proactivamente incorporar los requisitos de privacidad en su diseño, con el fin de evitar eventos de invasión de privacidad.

Los servicios públicos deben llevar a cabo Evaluaciones de Impacto de Privacidad o tipos similares de evaluaciones como parte de los requisitos y las etapas de diseño de las iniciativas de medición inteligente. Dentro de esta evaluación, deben realizarse dos consideraciones. En primer lugar, los servicios públicos deben determinar que tipo de información de los medidores inteligentes se requiere para cumplir con los objetivos. Se deberán poner a disposición mecanismos que permitan a los consumidores mantener el control sobre la información disponible y que quizá, no sea necesaria. En segundo lugar, se debe obtener la menor información posible en del hogar del consumidor a través del medidor inteligente. Se debe lograr que el el flujo de datos sea lo menos personal posible y que los servicios públicos pueden utilizar técnicas como la disociación, uso de seudónimos, o la agregación de datos.
Los contadores inteligentes deben proteger la privacidad por defecto, sin necesidad de acción alguna por parte del consumidor. Con el fin de asegurar su presencia, la privacidad siempre debe ser protegida como la condición predeterminada. La intimidad debe estar en modo: "no se requiere acción".

Deben realizarse dos consideraciones. En primer lugar, en caso de presentarse múltiples opciones (en relación con ya sea el tipo de metro o de sus valores iniciales) al consumidor, la opción por defecto debe ser la que garantice mayor privacidad. En segundo lugar, aún cuando los consumidores han optado por tener información detallada del consumo que hayan sido recabados por el medidor inteligente, se deberá obtener el consentimiento informado y positivo de las personas antes de cada uso independiente o de la divulgación de esta información para propósitos distintos que escapen al servicio.

La privacidad debe ser un elemento esencial para el diseño y prácticas de sistemas de medidores inteligentes. Iniciativas de medidores inteligentes se han visto incrementadas en muchas jurisdicciones de todo el mundo. Se están desarrollando mejores prácticas y requerimientos legislativos para reforzar los esfuerzos de las empresas de servicios públicos y de terceros para crear prácticas amigables de recolección, uso y divulgación de la información de los medidores inteligentes.

Sin embargo la privacidad no puede depender únicamente del Poder Legislativo, sino que debe estar diseñada en la propia tecnología. Por consiguiente, subyacente a los requisitos de la privacidad desde el diseño, es el concepto de minimización de los datos, esto es, la idea de que la recopilación, uso, divulgación y retención de información personal debe ser minimizado en cualquier lugar, y en la mayor medida posible.

Las iniciativas de medición inteligente deben evitar innecesarias concesiones entre privacidad y otros objetivos legítimos.

Cuando la intimidad se encuentra en conflicto con la funcionalidad del sistema, las organizaciones se encuentran ante disyuntivas innecesarias, respecto a las protecciones que se describen en términos de "en lugar de" más que "además de", llegando a presentar a los consumidores opciones entre su vida privada y la eficiencia energética / conservación. Estos enfoques van directamente en contra de la filosofía de la privacidad desde el diseño, que asegura que todos los objetivos legítimos se cumplen en iniciativas de medición inteligente. Los medidores inteligentes y su más amplia infraestructura deben ser diseñados tanto para garantizar la privacidad y la seguridad, a niveles que estén en línea con los riesgos que corren los interesados, así como garantizar la consecución de los beneficios potenciales de dichos medidores.

Las Iniciativas de medición inteligente deben estar diseñadas para respetar la privacidad de los consumidores.

Los consumidores deben estar provistos de toda la información necesaria, las opciones y controles para que puedan gestionar su consumo energético y su privacidad. Por ejemplo, el ERGEG **(European Regulators Group for Electricity and Gas)** ha declarado en su Documento de Mejores Prácticas que, "siempre es el cliente quien elige de qué manera se utilizarán los datos de medición".

El Supervisor Europeo sobre Protección de Datos (SEPD) ha adoptado el Dictamen **2012/148/UE: Recomendación de la Comisión, de 9 de marzo de 2012**[1]**, relativa a los preparativos para el despliegue de los sistemas de contador inteligente.** El objetivo de la Recomendación es proporcionar orientaciones a los Estados miembros sobre los preparativos para el despliegue de los sistemas de contador inteligente en Europa. El despliegue está previsto para 2020 tanto para el mercado de la electricidad como para el mercado del gas y está sujeto a una evaluación económica de costos y beneficios. Dicha evaluación deberá ser realizada por cada Estado miembro a más tardar el 3 de septiembre de 2012

Si bien el despliegue de los sistemas de medición inteligente puede aportar beneficios importantes, también permitirá la recolección masiva de datos personales al realizar un seguimiento de lo que los miembros de la familia hacen en la intimidad de sus hogares. Estos modelos pueden ser útiles para el análisis de consumo para el ahorro de energía, pero en correlación con los datos procedentes de otras fuentes, el potencial para una **explotación de datos con otros fines** es muy importante. Los modelos y perfiles de consumo se pueden utilizar para muchos otros fines, incluidas las campañas de marketing, la publicidad y la discriminación de precios por parte de terceros.

El SEPD aprecia los esfuerzos de la Comisión para utilizar las nuevas propuestas de conceptos como la protección de datos desde el diseño y los instrumentos prácticos como las evaluaciones del impacto sobre la protección de datos y las notificaciones de violaciones de la seguridad. El SEPD, en particular, apoya el plan de la Comisión de preparar un modelo de evaluación del impacto sobre la protección de datos y presentarlo al dictamen del Grupo de Trabajo del Artículo 29.

Asimismo, lamenta que la Recomendación no haya ofrecido una orientación más específica y práctica en materia de protección de datos. Sin embargo, considera que todavía pueden proporcionarse orientaciones al modelo que está siendo elaborado actualmente. Por ello, el dictamen realiza recomendaciones sobre el modelo y hace hincapié en que el mismo debe ofrecer orientaciones específicas y prácticas: una recopilación de las mejores prácticas y de las «mejores técnicas disponibles». También resulta crucial que el modelo siga una metodología sólida y, entre otros, que relacione de forma clara cada riesgo con un control adecuado.

Además, el dictamen pide a la Comisión que evalúe si resulta necesaria una mayor acción legislativa a nivel europeo y ofrece recomendaciones para dicha posible acción legislativa. Algunas de dichas recomendaciones ya pueden ser aplicadas a través de una modificación de la Directiva sobre eficiencia energética, que está siendo estudiada por el Consejo y el Parlamento. Dichas recomendaciones deberían incluir como mínimo el requisito obligatorio para los responsables del tratamiento de llevar a cabo una evaluación del impacto sobre la protección de datos y una obligación de notificar las violaciones de datos personales.

1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:ES:PDF (Página visitada el 27 de agosto de 2013).

El SEPD recomendó asimismo[2]:

- Una mayor orientación sobre la base jurídica del tratamiento y las opciones de que disponen los interesados: en particular, una distinción clara entre los objetivos para los que los datos sobre el uso de la energía pueden ser tratados sin el consentimiento del cliente y los objetivos para los que resulta necesario contar con el consentimiento del cliente (apartado 4.2),
- La aplicación obligatoria del «Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad» y otras «mejores prácticas disponibles» para la minimización en la recogida de datos (apartado 4.3),
- Aclaración de las funciones y responsabilidades de los distintos actores desde el punto de vista de la protección de datos (apartado 4.4),
- Mayor orientación sobre los períodos de conservación; en principio, los datos de consumo de grano fino de los hogares únicamente serán permitidos hasta el final del período durante el que pueda impugnarse legalmente la factura o exigirse el pago y sólo para el nivel de granularidad exigido con fines de facturación (sin perjuicio del derecho del consumidor a un período más largo basado en el consentimiento, por ejemplo, para obtener un asesoramiento específico sobre energía) (apartado 4.5),
- Acceso directo de los consumidores a sus datos sobre el uso de energía y los métodos eficaces de informar a los interesados sobre el tratamiento de sus datos; esto debería incluir, en el caso de la extracción automática de datos, la publicación de los perfiles de las personas físicas y la lógica de todos los algoritmos utilizados para dicha extracción; debe ofrecerse una información global sobre la existencia de todas las funcionalidades de activación y desactivación.

5. Proyecto de George Tomko

George Tomko define Smart data como: un agente inteligente basado en web, que sirve de representante del titular de los datos, para asegurar y controlar la emisión y usos de sus datos personales, en función del contexto y las preferencias del interesado.
Es autónomo y aprende de la experiencia, respondiendo correctamente a situaciones nuevas, va a funcionar en un mundo 3-D virtual cuando éste se convierta en la próxima evolución de la web.

Es una tecnología basada en la Web que permite a la persona interesada estar en completo control de los usos de sus datos personales todo el tiempo.

Plantea la Fantasía Científica de que cada uno tiene información en su cabeza que quiere mantener en privacidad, entonces cada individuo es la versión humana de smart data. Propone imaginar la digitalización de nuestro cuerpo y mente en un sistema binario y luego almacenarlo en la nube, e imaginar además, que cuando alguien tiene una solicitud acerca de nuestros datos personales, se pudiera descargar un sistema binario en una máquina de clonación, y que ésta máquina pudiera reconstruir una copia de nosotros, un clon. Dicho clon representaría nuestro interés en cuanto a la privacidad de nuestros datos. O sea que si alguien le solicita al clon determinada información, éste se la entregará únicamente si reunió los criterios adecuados.

Además, la idea es que sea un clon dinámico, que observe lo que se hace con los datos personales, que controle que no se haya hecho nada incorrecto, por ejemplo que se haya enviado datos a personas que no se tuvo intención en enviar.
Su idea es sustituir al clon por un agente inteligente, a ese agente lo llamaría: Smart Data. Luego, sustituye la máquina de clonación por un procesador, de manera que cuando sea descargada la cadena binaria en un dispositivo se configura y activa un agente inteligente de datos.
En cuanto a la seguridad, los datos personales estarán divididos, anónimos, encriptados y ubicados

2 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_ES.pdf (Página visitada el 27 de agosto de 2013).

en cajas bloqueadas almacenadas en la nube.
Smart Data controlará quien está autorizado a acceder a los datos, que pueden hacer con ellos y cuando y donde pueden acceder a los mismos.

6. Conclusiones

Las empresas registran cada vez más información de sus clientes, proveedores y empleados, establecen perfiles con gustos y necesidades similares. Pero no solo es que haya más cantidad de datos, sino que son datos totalmente nuevos, y ello exige que las herramientas informáticas para extraer el conocimiento sean cada vez más avanzadas, lo que dificulta una adecuación paralela de la regulación normativa en materia de privacidad y seguridad.

La información se ha convertido en una materia prima de gran valor, siendo los datos una nueva especie de activo económico, como la moneda o el petróleo. El almacenamiento masivo de datos y las nuevas fuentes de obtención de los mismos, afectan el mundo de los negocios, el ámbito académico y las administraciones públicas.

Para lograr confianza en el uso de las nuevas tecnologías, por parte de los usuarios finales, es imprescindible que existan políticas de privacidad asequibles, claras y visibles, en las que el consentimiento de los usuarios sea en toda ocasión, específico para el tratamiento concreto que se va a realizar de sus datos personales.

Según dijo Sir Tim Berners-Lee (inventor de la World Wide Web), estamos en la era de "The Data Revolution", en la que, refiriéndose a los gigantes de Internet: "They have the data and I don´t"[3] (ellos tienen mis datos personales y yo no). Smart Data es un avance extraordinario, pero debe armonizarse siempre con el control por los usuarios sobre sus propios datos. Ese será el próximo desafío.

3 http://www.guardian.co.uk/technology/2012/apr/18/tim-berners-lee-google-facebook (Página visitada el 27 de agosto de 2013).

CAPITULO VII

DATOS BIOMÉTRICOS

Dr. Marcelo Bauzá

DATOS BIOMÉTRICOS

Dr. Marcelo Bauzá

1. Conceptos técnicos preliminares

1.1. Definición y consecuencia jurídica

La Biometría es una ciencia que estudia aquellos elementos que permiten identificar un individuo a partir de características muy certeras. En base a ella se llega a los denominados datos biométricos, definidos como "propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican cierto grado de probabilidad".[1]

En las aplicaciones que hace la técnica de esta disciplina, se aprovecha la existencia de datos irrepetibles de un individuo a otro, que lo acompañan a lo largo de su vida sin alteraciones ostensibles. Ambos rasgos, irrepetibilidad y permanencia, resultan valiosos argumentos al momento de una identificación precisa, permitiendo también una trazabilidad del sujeto portador de tales rasgos, en circunstancias tempo-espaciales diversas.

Por sus características que afectan las zonas más fuertes de la privacidad e intimidad del individuo, estamos ante datos sensibles, merecedores como tales de regulación y controles especiales.

1.2. Clases y especies de datos biométricos

Se habla de una **Biometría estática** para referir a las técnicas que se apoyan en la mensura de la anatomía del usuario, mientras que la **Biometría dinámica** agrupa las que miden el comportamiento del usuario.

Actualmente, y de acuerdo al estado de la técnica, existen los siguientes sistemas biométricos:

A) Biometría estática:

a) Verificación de huellas dactilares: tradicionalmente reconocido como uno de los mejores patrones identificatorios, ya que no está probado científicamente que no haya dos improntas iguales; se basa en la lectura de la huella individual y su comparación con las existentes en el banco de datos.

b) Verificación de patrones de la mano: comparación de la imagen tomada con patrones almacenados, a través de modelos matemáticos.

c) Termografía corporal: mide la temperatura corporal (ej. facial), a través de los patrones de rayos infrarrojos que emite un cuerpo debido al flujo de sangre bajo su piel.

d) Verificación de patrones oculares: De los métodos más efectivos (retina e iris) por la misma razón que la huella dactilar. No goza de buena aceptación de parte de los usuarios, por su carácter invasivo (escaneo del ojo) y por la posibilidad de dejar al descubierto cuestiones íntimas o privadas (consumo de drogas o alcohol, padecimiento de alguna enfermedad).
e) Venas del dorso de la mano: El sistema de identificación en este caso proviene de la interpretación

1 Grupo de Trabajo del Artículo 29. Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio de 2007. 01248/07/ES WP 136.

de la geometría del árbol de venas del dedo o la mano.

f) Reconocimiento facial: Es una aplicación dirigida por un programa informático para identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales, a partir de una imagen digital o un fotograma de una fuente de vídeo. Una de las maneras de hacer esto es mediante la comparación de determinados rasgos faciales de la imagen facial y una base de datos.

B) Biometría dinámica:

a) Verificación de la voz: requiere de sala especial, ajena a ruidos y con buena acústica. El usuario se autentifica a través de un texto pre definido o independiente.

b) Verificación de escritura manuscrita o firma: se basa en aspectos dinámicos (presión del lápiz sobre el papel, ángulo de los trazos, tiempo utilizado para firmar).

c) Dinámica de tecleo: recoge la información de tiempo detallado que describe exactamente cuándo cada tecla es presionada y soltada por una persona cuando escribe en un teclado de computadora, permitiendo expresar un patrón de tecleo personal de cada usuario.

d) Cadencia del paso: en tanto resulta ser también un modo peculiar de cada individuo, mensurable.

e) Análisis gestual: similar funcionalidad que la anteriormente referida.

1.3. Propiedades de los datos tratados biométricamente

Se trata de datos invariables al menos durante un largo período de vida del individuo (se produce un cierto descaecimiento o cambio de figuración, a medida que el sujeto envejece, o bien por accidentes que sufra).
Como se expresara antes, son mensurables con precisión, y por ello unívocos, es decir no susceptibles de ser puestos en duda.

Un rasgo que podríamos denominar de contención jurídica, viene dado por la confrontación con el respeto de la dignidad humana. Es por ello que se tomarán como aceptables en su uso, solamente aquellas técnicas biométricas que excluyan técnicas invasivas.

Otra característica de este tipo de datos, es que son reducibles a resultados de fácil contralor, a través de dispositivos de captura de tales datos en estado analógico, convertidos mediante el software adecuado en información legible digitalmente.

1.4. Fases de un procedimiento biométrico y resultados posibles

Existe una **fase de registro** donde el sujeto entr4ega al sistema un elemento biométrico, del cual se extrae el "template" o "modelo", o una representación matemática de los datos a tratar.

Luego está la **fase de verificación** en la que el dato biométrico ya adquirido por el sistema, es confrontado con el dato sometido a análisis, con miras a una autenticación o identificación.

La aplicación de una técnica biométrica, según los casos, puede arrojar tres resultados diferentes:

Autenticación : ¿soy yo realmente el que declaro ser?
Verificación uno con uno : ¿quién soy yo?
Verificación uno contra muchos : ¿es o está presente la persona supuesta?

2. Los principios jurídicos aplicables

2.1. La aplicación del régimen general

La recolección y tratamiento de datos personales cualquiera sea el soporte o técnica en la que se funden y organicen, son actividades que deben enmarcarse dentro de los referentes mayores del derecho fundamental de la protección de datos personales, para considerarse lícitos y ajustarse en un todo a derecho.

Los datos biométricos no escapan a la enunciada regla. Se destaca para el caso en examen la necesidad de aplicación y cumplimiento de una serie de principios, con sus especificidades atendiendo a las características particulares de este tipo de datos. Es indudable que se deben establecer marcos legales y tecnológicos para proteger a los individuos, para que la tecnología no se limite a procesar a la gente reduciéndola a datos reportables.

Por tanto, toda vez que se proyecte poner en práctica un nuevo sistema biométrico, las empresas o entidades responsables deberán tener presente la relación de tal propósito con la privacidad y la protección de datos personales.
La aceptación de estos sistemas depende de si se adecúan a los propósitos perseguidos, si son necesarios y no invasivos. En este punto se debe valorar el impacto en la privacidad tomando en cuenta las siguientes notas:

- Cuál es el objeto de la recolección.
- Cuántas personas serían las afectadas.
- Evaluar la vulnerabilidad de estas personas.
- Si los datos biométricos se transmiten a terceros.
- Qué tipo de medidas de seguridad se implementan.
- Si existe riesgo de robo de identidad.
- Por cuento tiempo se conservan los datos.

2.2. El principio de licitud

En los últimos decenios los sistemas biométricos han estado expandiéndose a múltiples efectos. La globalización de las relaciones humanas, con el incremento considerable de los desplazamientos de las personas, el avance en las facilidades y prestaciones que ofrece la técnica para agilizar los controles fronterizos, y el aumento superlativo de las medidas de policía y seguridad adoptadas por los Estados para frenar la escalada del terrorismo y la delincuencia internacionales, son otros tantos factores que han determinado que entidades internacionales y Estados se hayan ido abriendo cada vez más al uso de este tipo de técnicas, como forma de identificación, seguimiento y/o control de individuos, sus movimientos y actividades.

Sin embargo, dado que se trata de técnicas que ponen a prueba el sistema jurídico de los DD.HH., es necesario que los mismos cuenten con previsión legal expresa, lo cual supone hacerlos compatibles con la regla de derecho, vale decir que no sean violatorios de derechos humanos, ni contrarios a las leyes o a la moral pública.

Los desafíos mayores son justamente aquellas acciones que contravienen el núcleo duro de la licitud en tanto valor jurídico supremo: la recolección subrepticia, los cambios de finalidad ampliando el uso previsto inicialmente sin nueva norma habilitante, la recolección de informaciones secundarias.

2.3. El principio de necesidad

Un sistema de esta naturaleza debe pasar el test de necesidad para resultar legítimo. Ello supone que, en la medida que existan otros procedimientos, incluso técnicas, que produzcan una menor afectación al derecho fundamental de protección de datos personales, deberán ser preferidos antes que implantar un sistema biométrico.

La implantación de este tipo de sistemas debe realizarse, pues, con razonabilidad y mesura, incluso prefiriendo dentro del conjunto de sistemas biométricos susceptibles de elección, aquéllos menos invasivos. Existe una gradación en este punto, que va en directa proporción a la necesidad perseguida según los casos, y ello habrá también de respetarse. Los sistemas menos invasivos serán los que se limitan a verificar la identidad del individuo mediante simple cotejo de los datos tratados, sin contenerlos o registrarlos en otro tipo de soportes, ni compararlos con los de otros individuos.

2.4. El principio de dignidad

Como toda tecnología relacionable con la identificación y seguimiento de las personas, la Biometría presenta riesgos de vulneración de los derechos y libertades fundamentales. La integridad del cuerpo humano, la manera en que se lo utiliza a fines técnicos, son cuestiones que se relacionan directamente con la dignidad humana. Por lo tanto, la adopción de este tipo de sistemas, su instrumentalización, el personal afectado a ello, conlleva aspectos éticos y jurídicos de cuidado y requerida consideración.

El tema conecta directamente con la Ética y los Derechos Fundamentales. Como bien se ha sabido expresar, "La biometría alentará debates sobre las aplicaciones éticas de la tecnología. Se puede sonreír ante la ocurrencia de una discoteca de Barcelona, España, que hace tres años motivó a sus clientes a implantarse una etiqueta RFID para facilitarles la entrada y pagar los tragos en el bar, pero difícilmente se puede sonreír de la misma manera ante la propuesta del gobierno colombiano de instalar tales implantes en todos sus ciudadanos que viajan a Estados Unidos para facilitarle al gobierno estadounidense el trabajo de rastrearlos. Como con toda aplicación tecnológica, es el respeto a la dignidad humana lo que debe guiar la evolución de la biometría, para evitar que su reinado se convierta en una pesadilla."[2]

2.5. El principio de proporcionalidad

A lo que debe apuntarse es a no solicitar ni emplear datos excesivos (o sea desconectados de la finalidad propuesta) al servicio de la nueva modalidad proyectada. Las leyes nacionales de protección de datos personales, refieren a este punto bajo la expresión "ecuánimes, no excesivos".

Desde otro punto de vista, el enunciado principio engloba una serie de pasos a considerar para la implantación de este tipo de sistemas: 1º) Necesidad de la medida. 2º) Idoneidad de la misma. 3º) Propiamente la ponderación, que a su vez se verifica en otros tres pasos, consistentes en (i) identificar el derecho-interés en baja, (ii) identificar el derecho-interés en alza, y (iii) comparar la importancia de satisfacer unos y otros derechos-intereses.

Superados estos tests, existen igualmente otro tipo de medidas complementarias a cumplir, a saber:
1º) Registrar datos resumidos en vez de datos brutos.
2º) Preferir la simple verificación por sobre la identificación.
3º) Preferir los almacenamientos locales por sobre las bases de datos centrales.

2 Martínez García, Juan Carlos. "El reinado de la biometría", en http://www.comoves.unam.mx/numeros/articulo/104/el-reinado-de-la-biometria (Página visitada el 8 de setiembre de 2013).

2.6. El principio de finalidad

Alude a la justificación y finalidad que deben existir, y respetarse en todo el transcurso de existencia de estos tratamientos, a los efectos de avalar o legitimar la utilización de este tipo de datos, y sus tratamientos consiguientes que modifican los sistemas tradicionales imperantes hasta el momento.

2.7. El principio de seguridad

Se debe preservar la integridad de los datos obtenidos, a través de técnicas de seguridad que deberán ser de las más altas atendiendo el tipo de tecnología e información en juego, volumen y fines de interés público que justifican el tratamiento.

La importancia de este principio se relaciona igualmente con la existencia inexorable de una "tasa de fallos" a contener o acotar. La experiencia muestra que estos sistemas presentan debilidades producto de asociaciones erróneas u omitidas, y malas capturas de datos. Se debe considerar el impacto de esta tasa sobre el éxito del proyecto o implantación del sistema biométrico.

3. Experiencias traídas a comentario durante la 34ª Conferencia[3]

3.1. Cuestiones tratadas

En esa oportunidad se trataron tres aspectos fundamentales: libertad, seguridad y privacidad, a la luz del estado actual de esta técnica biométrica.

Las preguntas propuestas a los panelistas fueron las siguientes:

- Implicancias jurídicas para la PDP, de la captura, almacenamiento y eventual publicación de imágenes en lugares públicos.
- Exigencias para el tratamiento de la información biométrica destinada a seguridad pública.
- Etiquetado automático de fotos, recolección y utilización de datos biométricos por Facebook, como opciones opt-out.

3.2. El reconocimiento facial en redes sociales

Lillie Coney de EPIC-Public Voice indicó que hace años que la tecnología permite distinguir una cara de otro objeto, pero lo que encuentra preocupante es que la cara actualmente pueda ser asociada únicamente a una persona. De todas maneras la tecnología del reconocimiento facial ya existe y habrá que lidiar con las políticas respectivas.

Explicó que en 2011 Facebook lanzó una aplicación de reconocimiento facial basada en las fotos subidas por usuarios y fotos etiquetadas, y si bien es la base de datos más grande de fotos no es la única. El problema es que estas aplicaciones son creadas sin consentimiento y sin la opción "opt out". Actualmente oímos hablar de la **nube** y de **big data** por lo que debemos tomar en cuenta que estos servicios toman fotografías de redes sociales o de cualquier foto que entreguemos para algún tipo de tratamiento. Eso es algo que la sociedad civil debe investigar ya que se trata de miles de millones de

3 La 34ª Conferencia Mundial de Autoridades de Protección de Datos y Privacidad se llevó a cabo en Punta del Este (23 y 24 de octubre de 2012) con la participación de personalidades y expertos de los cinco continentes. El Panel H sobre "Biometría" contó con la presencia de Wojciech Wiewiorowski (Polonia) en calidad de Moderador, y los siguientes panelistas: Gus Hosein (Reino Unido), Sigrid Arzt (México), Lillie Coney (Estados Unidos), y Ruben Amato (Uruguay).

fotografías que permiten identificar y asociar a un perfil personas que pueden ser objeto de acoso. Inclusive esta identificación puede atentar contra derechos constitucionales tales como libertad de asociación, de asamblea, de movimiento.

Se pierde el control sobre la imagen y además esa información puede ser usada para influenciar los hábitos de compra. Por eso, concluye que el mayor reto para la Federal Trade Comission (FTC) es lograr transparencia para que los consumidores sepan cómo son tratados sus datos.

3.3. La inversión en este campo y sus beneficiarios

Gus Hosein de Privacy International da cuenta del proyecto que lleva adelante su organización, denominado Big Brother Inc.

El proyecto consiste en determinar cuáles empresas venden sistemas de vigilancia en cuales países. Por ejemplo, indica que en varios países de África son utilizados como forma de identificación rasgos biométricos que en el mundo occidental generan problemas con la privacidad.

El PNUD financia registros biométricos de votantes en Benin, Cabo Verde, Comoros Islands, Congo, Sierra Leona, Togo y Zambia. El Banco Mundial lleva un registro biométrico de pobres en Benin y Kenya. El USAID financia sistemas de identificación basados en la biometría en Malawi y Guinea.

Los costos de estas políticas son considerables: En Mozambique el costo de implementar tarjetas de identificación fue de U$S 15 millones. En Uganda el costo del contrato con el grupo Mühlbauer, también por tarjetas de identificación fue de 64 millones de euros. El costo de PNUD por el registro de votantes de Sierra Leona fue de U$S 60 millones. En Congo el costo del proceso de registración fue de U$S 101 millones y hubo más de 700.000 registros dobles.

Lo irónico, indica Hosein, es que se crean fondos para países que lo necesitan pero el dinero termina revirtiendo por contrato a empresas europeas.

Los sistemas de control más invasivos son los diseñados por empresas inglesas y alemanas según el expositor.

La solución planteada es hablar con las fundaciones para informar como los fondos van a las empresas. Además se deben establecer marcos legales y tecnológicos para proteger a los individuos, frente a la tentación de hacer de todo individuo un conjunto de datos reportables.

3.4. Experiencia de México

Sigrid Arzt Colunga, Comisionada de la Autoridad de Protección de Datos de México informó que en la ley mexicana sobre los datos que recolecta el Estado existe el derecho de acceso y corrección, pero no el de oposición.

Luego detalló una investigación llevada a cabo en México por la empresa Unisys en marzo de 2012. Según los datos obtenidos, un 64% de la población está dispuesta a entregar sus huellas digitales como forma de identificación; un 62% su fotografía para ser usada por tecnologías de reconocimiento facial; un 61% la voz como forma de identificación; un 60% el iris y un 59% el patrón de circulación de sangre por la venas de los dedos. Incluso más de un 20% está dispuesto a entregar datos biométricos para identificación, si éstos facilitan el acceso a espectáculos deportivos. Sólo un 23% de los encuestados se oponen a medidas invasivas.

En el IFAI se han publicado unos lineamientos para el registro de las bases de datos según el tipo de tratamiento, ya que todas las medidas impactan en la privacidad. Como ejemplo indica que en el caso del personal de seguridad se recolectan varias clases de datos, entre ellos el ADN, por lo que

hay que justipreciar si existe proporcionalidad, y por cuento tiempo son guardados los datos una vez que la persona deja de pertenecer a la corporación.

3.5. Experiencia de Uruguay

Ruben Amato, Director de la Dirección Nacional de Identificación Civil (DNIC) sostuvo que se ve a la recolección de datos en pro de la seguridad, pero pocos ven la identificación desde el punto de vista de la gobernabilidad democrática.

El Estado necesita saber quiénes son los ciudadanos para implementar con efectividad las políticas sociales, para saber cómo se ubica la población, para fines presupuestales. Los métodos de identificación biométrica, tienen que ser aceptados a tal propósito, no obstante lo cual los invasivos no deben serlo.

Es preciso preguntarse hasta donde se justifica el uso de un dispositivo de biometría para un documento de identidad, de viaje, o para ingresar a un trabajo; y qué clase de ellos según los casos.

El iris, el ADN, el estudio de la venas, son métodos invasivos y pueden mostrar elementos que no se quieren sacar a la luz, como patologías o consumo de drogas.

Uruguay dispone de documento de identidad con inclusión de elementos de biometría desde 1978: huella digital, foto y firma, dos métodos estables y uno dinámico. Asimismo tiene el sistema AFIS de identificación automatizada de huellas dactilares, donde el dato se puede chequear al instante.

Se concluye por el panelista que los motivos de seguridad y defensa no significan que esté todo permitido. La ley de protección de datos personales excluye de su ámbito de actuación a las bases de seguridad y defensa, pero si los datos tomados se desviasen de ese objetivo, se cae en la ilegalidad.

3.6. Intervenciones a pedido del público

Las preguntas y comentarios del público dieron oportunidad para que los expertos aportaran sus reflexiones acerca de tópicos variados, relacionados siempre con el tema expuesto.

La primera reflexión provino de quien manifestó estar interesado por sistemas más avanzados de identificación como los que se usan en aeropuertos, y no tanto por las huellas dactilares.

Coney contestó que caminar por un aeropuerto es como ir a un laboratorio donde no siempre sabemos que datos están tomando. De todas maneras ella considera que es más preocupante la cantidad de fotos desde varios ángulos subidas en redes sociales que el hecho de escanear el iris en un aeropuerto.

Por su parte Hosein, explicó que cada smartphone tiene un único número identificador, por lo que en los aeropuertos se utiliza un dispositivo para controlar el paso.

Amato sostuvo que el método biométrico debe ser razonable, ajustado a la finalidad y al país. Por ejemplo en nuestro país la gente pasa por las fronteras en auto y el reconocimiento facial no es acertado pero las huellas biométricas sí pueden serlo.

La segunda consulta es acerca del uso de datos biométricos con fines comerciales.

Contesta Coney que el sector comercial está muy interesado en recolectar rasgos biométricos.
Es como tener una llave de acceso y esa llave es el perfil ligado al reconocimiento facial. Incluso las Agencias de Inteligencia pueden usar esos perfiles para saber si se debe permitir a la persona subir a un avión o un subterráneo.

También existe tecnología que detecta las emociones y es usada para inducir a la compra de determinados productos.

La siguiente intervención es un comentario respecto a la exposición de Arzt, en el sentido que puede resultar más barato conservar los datos que eliminarlos, lo que se debe tomar en cuenta cuando se trata de agencias con recursos limitados.

La comisionada Arzt responde que la postura del IFAI es consultar al sector seguridad sobre la calidad y sostenibilidad de la conservación de los datos.

La siguiente consulta es sobre si hay una evaluación imparcial de las tecnologías que toman rasgos biométricos.

Responde Arzt que cada vez que sale una nueva aplicación el IFAI pide un estudio de impacto realizado por una consultora independiente. Por ejemplo el Ministerio del Interior lanzó una tarjeta de identificación para la que se recolectaron datos del iris de niños, y en este caso el IFAI recomendó instruir a los padres.

Coney contesta que parte del trabajo de EPIC es relevar la tecnología emergente y para ello trabajan junto a los investigadores de la Universidad de Carnegie Mellon.

Según Hosein se debe hablar de usos específicos ya que cada aplicación es creada para determinado ambiente específico, lo que puede funcionar en un aeropuerto no funciona en la calle.

Finalmente se plantean cuatro consultas seguidas para que luego los panelistas respondan.

La primera consulta es si las especificaciones técnicas y legales están alineadas, ya que los Estados no ponen mucha seguridad en la recolección de datos que generalmente se encarga un tercero.

La segunda consulta es para Coney, acerca de si considera que hay un uso positivo de la biometría y los perfiles de los consumidores.

El tercero es un comentario acerca de que la biometría es crítica para identificar a criminales que cruzan fronteras, y por eso en Reino Unido se usan las huellas dactilares. De hecho el 50 % de las personas arrestadas en Londres no son nacionales. Finalmente se indica que el gobierno va a utilizar todos los medios de vigilancia posibles como los circuitos de CCTV, para evitar el crimen.

La última pregunta consulta que tan comprometidas con la privacidad están las empresas que venden sistemas de identificación en África.

Para Coney el principal problema es la falta de transparencia en el tratamiento de los datos. Según Hosein las empresas no se comprometen, ya que no envían ingenieros sino vendedores, por eso es muy importante que la privacidad esté implicada en el diseño. Por su parte, Arzt indica que el IFAI siempre busca técnicos que puedan explicarles todas las aristas para realizar las recomendaciones. Asimismo menciona que gracias a las huellas dactilares se pudieron identificar a 72 inmigrantes víctimas de la masacre de San Fernando. Amato opina que en materia policial se pueden recolectar datos, pero deben cancelarse a la primera oportunidad de cumplido el cometido. El equilibrio entre tecnología y privacidad es responsabilidad de los responsables de bases de datos.

Para finalizar Wiewiorowski concluye que las técnicas utilizadas por la policía son luego usadas por el mercado, la pregunta es si permitimos las mismas técnicas.

CAPITULO VIII
E-SALUD

Dra. Flavia Baladán

E- SALUD

Dra. Flavia Baladán

1. Introducción

El presente capítulo tiene como objetivo estudiar la E-Salud en relación con los datos personales, empezando por una visión más global hasta llegar a un estudio más pormenorizado de su incidencia en materia de protección de datos.

1.1. Introducción a la E-Salud

Para comenzar es necesario definir que se entiende por "E- Salud". Según el Informe ANUA sobre el desarrollo de la Sociedad de la Información en España, la E- Salud se define como la aplicación de las Tecnologías de Información y Comunicación en el amplio rango de aspectos que afectan el ciudadano en la salud, desde el diagnóstico hasta el seguimiento de los pacientes, pasando por la gestión de las organizaciones implicadas en estas actividades.

En el caso concreto de los ciudadanos, la E – Salud les proporciona considerables ventajas en materia de información; inclusive favorece la obtención de diagnósticos alternativos. En términos generales, la E- Salud implica una mejora en el acceso a información relevante sobre los datos de salud de las personas.

En conclusión, se trata de formas diferentes de prestar servicios ordinarios buscando que éstos sean más eficientes y eficaces, así como también implica una reducción en los tiempos, ahorro de costos, entre otros.

1.2. Salud 2.0

A nivel internacional se ha considerado que el término "Salud 2.0" refiere al nuevo enfoque existente sobe la sanidad. Se trata de una visión integral y superior de la salud. Es dotar a los profesionales sanitarios y a la personas de la posibilidad de gestionar sus propias historias clínicas mediante distintos dispositivos y compartir con el profesional que elijan su historial clínica, sin importar el lugar donde se encuentren. [1]

Generalmente, cuando se habla de Salud 2.0 se hace referencia a ciertas características, a saber: movilidad, personalización, monitorización y localización. En relación con la movilización, se indica que las personas pueden compartir su información médica no importando la distancia a la cual se encuentren. Cuando se habla de personalización se quiere decir que las características propias de cada paciente determinan el tipo de servicios que necesita y cómo deben usarlos. La monitorización refiere a lograr mayor independencia del paciente, y tranquilidad para la supervisión médica al tener una información continua. Además, permite reaccionar rápidamente ante problemas derivados de cualquier síntoma. Por último, la localización es un instrumento que permite identificar el lugar donde se encuentra cada paciente de forma de poder localizarlo en cuanto sea necesario.

1 www.wikipedia.org/wiki/Salud_2.0 (Página visitada el 19 de febrero de 2013).

1.3. Salud 3.0

Los nuevos desarrollos tecnológicos también implican cambios en la salud. Por ejemplo, a nivel mundial se habla del surgimiento de la web semántica. Se entiende que la web semántica es "una Web extendida, dotada de mayor significado en la que cualquier usuario en Internet podrá encontrar respuestas a sus preguntas de forma más rápida y sencilla gracias a una información mejor definida. Al dotar a la Web de más significado y, por lo tanto, de más semántica, se pueden obtener soluciones a problemas habituales en la búsqueda de información gracias a la utilización de una infraestructura común, mediante la cual, es posible compartir, procesar y transferir información de forma sencilla. Esta Web extendida y basada en el significado, se apoya en lenguajes universales que resuelven los problemas ocasionados por una Web carente de semántica en la que, en ocasiones, el acceso a la información se convierte en una tarea difícil y frustrante". [2]

En el ámbito de la salud "quiere decir que si un paciente hiciera una búsqueda en Internet sobre algún aspecto relacionado con su salud, el sistema devolviese los **resultados que ese paciente necesita ordenados en función de su relevancia**, eliminando todos aquellos clasificados como ineficaces o perjudiciales para su salud (...). Esto implicaría que el sistema conociese las búsquedas anteriores de esa persona, sus referencias sanitarias en su círculo social relacionado con la salud y además, cuáles de los contenidos relacionados con la búsqueda son los más útiles o más valorados por el resto de los usuarios. Y no solo eso, sino que el algoritmo será capaz de ir aprendiendo con las búsquedas de los usuarios y refinando cada vez más los resultados". [3]

Es fácil llegar a la conclusión de que esto tiene una clara incidencia sobre el derecho de la privacidad, en virtud de que las búsquedas que nosotros realizamos las hacemos por medio de herramientas privativas. Quiere decir que le brindamos datos sensibles a terceros. Cabe preguntarse sobre el balance entre entregar este tipo de información por obtener información sanitaria específica de relevancia para el titular de los datos.

1.4. Salud en dispositivos móviles

También, actualmente las Tecnologías de la Información permiten que mediante el uso de dispositivos móviles, tales como celulares o tablets, el paciente pueda acceder a información sobre su salud.

En este aspecto, uno de los puntos más discutidos es la posibilidad de llevar la historia clínica en algunos de los soportes electrónicos del tipo de los mencionados. Los problemas relacionados con la privacidad en este campo surgen sin mayores dificultades.

Por ejemplo, determinar los peligros para la seguridad de los datos sensibles como son los de salud cuando se llevan éstos en forma personal. Cabe preguntarse aquí qué sucede con información personal en caso de pérdida de estos dispositivos. En virtud de ello, es necesario conocer qué medidas de seguridad ofrecen.

Otro ejemplo, es la utilidad o no que lleva la encriptación de la información como forma de asegurar los datos. En este último caso, se discute cuál es la utilidad que puede tener poseer datos de salud en casos de accidente de tránsito si la información se encuentra encriptada. El profesional de la salud no podría acceder y, por tanto, no serviría como fuente de información. Este punto será abordado más adelante en este trabajo.

2 http://www.w3c.es/Divulgacion/GuiasBreves/WebSemantica (Página visitada el 21 de febrero de 2013).

3 http://saludconectada.com/salud-3-0/ (Página visitada el 21 de febrero de 2013).

1.5. Sistemas de tarjeta sanitaria electrónica

Otro medio electrónico disponible que se ha ido expandiendo es la tarjeta sanitaria que supone el complemento indispensable para que la información sanitaria se lleve con eficacia y que no daría lugar a los problemas antes mencionados.

Existen diferentes tipos de tarjetas sanitarias: las que solamente identifican al paciente, las magnéticas, que sirven de llave para la información del paciente, las tarjetas electrónicas de memoria que almacenan datos pero no contienen microprocesadores, y las tarjetas electrónicas inteligentes que además de almacenar datos, contienen un microprocesador. [4]

Estas últimas, las que incorporan información sobre la salud de las personas crean incertidumbre sobre la confidencialidad de la información que contienen. Se estima que plantean más riesgos que las tarjetas sanitarias tradicionales, sin embargo, desde el punto de vista técnico se consideran relativamente aceptable. Se estima necesario contar con una norma que determine qué información pueden contener estas tarjetas, la finalidad con la que se puede emplear la misma, quiénes pueden acceder, etc.

1.6. Historia clínica electrónica

Para la Organización Mundial de la Salud, la Historia Clínica Electrónica es un registro en formato electrónico (por oposición a la ficha en papel) de la historia clínica de un paciente. Comprende aquella información sobre resultados de pruebas y tratamientos farmacológicos, así como la historia clínica en general. Las TIC permiten poner ésta rápidamente a disposición del personal autorizado que esté atendiendo al paciente. [5]

Desde el punto de vista de la protección de datos, el Grupo de trabajo sobre protección de datos del artículo 29 define la historia clínica electrónica como un historial médico completo o una documentación similar del estado de salud física y mental, pasado y presente de un individuo, en formato electrónico, que permita acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados. [6]

Sobre este punto en particular, existe mucha información desde el punto de vista de la protección de datos que resulta excesivo para los objetivos de este trabajo. Es, sin embargo, de destacar la opinión que emite el referido Grupo de Trabajo en el sentido de entender que "los sistemas de historia clínica electrónica tienen el potencial para lograr una mayor calidad y seguridad en la información médica que las formas tradicionales de documentación electrónica". Sin embargo, ellos opinan que desde el punto de vista de la protección de datos hay que subrayar el hecho de que tienen más potencial para tratar más datos personales y para hacer que los datos sean más fácilmente accesibles para un número mayor de destinatarios, lo cual da lugar a problemas con la confidencialidad de los datos y requiere la determinación de niveles de acceso. [7]

4 http://www.ehu.es/argitalpenak/images/stories/tesis/Ciencias_Sociales/ABERASTURI%20GORRI%C3%91O.pdf (Página visitada el 18 de febrero de 2013).

5 http://www.who.int/goe/data/Global_eHealth_Survey-Glossary-SPANISH.pdf (Página visitada el 28 de agosto de 2012).

6 Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), WP 131 del Grupo de Trabajo sobre protección de datos del artículo 29, 15 de abril de 2007, pág. 4.

7 http://www.ehu.es/argitalpenak/images/stories/tesis/Ciencias_Sociales/ABERASTURI%20GORRI%C3%91O.pdf (Página visitada el 18 de febrero de 2013).

2. La seguridad en la E – Salud

Todos los nuevos dispositivos móviles, cloud computing, dispositivos móviles, tarjetas sanitarias electrónicas, entre otros, así como el uso de la historia clínica electrónica, llevan a que se planteen problemas con la seguridad de los datos. La problemática en materia de salud se basa fundamentalmente en determinar quiénes y a qué información se accede. Se entiende que los profesionales del ámbito de la salud deben tener un amplio acceso a la historia clínica del paciente para brindar un correcto tratamiento. Por su parte, las demás personas que se desempeñan en el ámbito de la salud deben tener accesos limitados de acuerdo a las necesidades de las funciones que desempeñen. Evidentemente, aquellas personas que no tengan una razón legítima para acceder a la información deben tener completamente vedado el acceso a estos datos.

En lo que se refiere al tipo de medidas de seguridad, una herramienta que frecuentemente se utiliza es la encriptación de la información, tanto para el almacenamiento de datos como para su transferencia. Igualmente, como se ha dicho, una duda que surge en este ámbito es qué sucede cuando en caso de emergencia se requiere acceder a información que se encuentra encriptada. Más allá de esta discusión, no existen dudas acerca de la necesidad de que se adopten medidas que garanticen en forma fehaciente la seguridad de los datos.

En cuanto al alcance que deben poseer esas medidas de seguridad, se estima que es pertinente hacer referencia a los ítems que menciona el Grupo de Trabajo sobre protección de datos del artículo 29 en el Documento de Trabajo WP 131. Estas medidas refieren a:

- Contar con un sistema fiable y eficaz de identificación y autenticación electrónicas que posea registros actualizados en forma permanente,
- Registro y documentación exhaustivas de todas las fases del tratamiento,
- Mecanismos eficaces de copia de seguridad y de recuperación,
- Imposibilidad de acceso no autorizado o de alteración de los datos,
- Instrucciones claras y documentadas a todo el personal autorizado sobre cómo utilizar correctamente los sistemas de historia clínica y cómo evitar riesgos y fallos de seguridad,
- Distinción clara de las funciones y competencias,
- Controles internos y externos regulares en materia de protección de datos. [8]

3. El ejercicio de los derechos.

La protección de la intimidad se regula estrictamente en el ámbito de la salud. Dentro de los derechos reconocidos al paciente se encuentra la confidencialidad de la consulta así como lo que en algunos lugares se denomina la autonomía progresiva de los pacientes. Esto es, el derecho de todo usuario o paciente, por sí o a través de representantes debidamente acreditados, a la confidencialidad de todo el proceso de sugerencias, iniciativas, consultas, peticiones o reclamos.

También en algunos lugares se regula el derecho de todo usuario de conocer la nómina de profesionales que se desempeñan en el servicio de salud.

En aplicación de los principios de la protección de datos, uno de los principales derechos es el de otorgar el consentimiento informado. En general, se indica en forma expresa las excepciones al consentimiento informado y el carácter personal del consentimiento informado así como los datos que necesariamente deben figurar en el documento donde consta éste.
Otro derecho consagrado en algunas normativas es el derecho a no saber. En virtud de éste, el paciente no quiere conocer el diagnóstico médico al cual se arriba. Para ello, el paciente debe

8 http://www.ehu.es/argitalpenak/images/stories/tesis/Ciencias_Sociales/ABERASTURI%20GORRI%C3%910.pdf (Página visitada el 18 de febrero de 2013).

otorgar el consentimiento por lo que recibe el tratamiento pero sin conocer los procedimientos que se les están brindando. En nuestro país, este derecho se encuentra regulado en la Ley Nº 18.335, de derechos y obligaciones de los pacientes y usuarios de los servicios de salud. Según esta norma, dicho derecho puede ser relevado cuando a juicio del médico, la falta de conocimiento pueda constituir un riesgo para la persona o la sociedad. En forma complementaria, el Decreto aclara que si la falta de consentimiento implica un riesgo para el paciente se debe dejar constancia de ese hecho en su historia clínica.

Vinculado con el anterior, se encuentra el derecho a negarse a recibir atención médica donde es necesario que el profesional deje constancia en la historia clínica con la firma de ambos. Al igual que el anterior, este derecho se encuentra limitado cuando exista un riesgo para la sociedad en su conjunto.

No se debe dejar de mencionar la posibilidad de que se emita la voluntad anticipada. Llevado a Uruguay, la Ley Nº 18.473 regula el derecho del paciente terminal de ser atendido o de oponerse a alargar su vida mediante la aplicación de tratamientos y procedimientos médicos, salvo que pueda afectar la salud de terceros. Este derecho es aplicable a aquellas personas que tienen una enfermedad terminal incurable o irreversible. Este consentimiento debe figurar en la historia clínica del paciente.

4. La E – Salud en los casos de emergencia

Una de las grandes problemáticas en la materia es el acceso a la información sanitaria durante los casos de emergencia.

Cuando se da un caso de emergencia, en general no se cuenta con el tiempo necesario para recabar el consentimiento informado de la persona accidentada. Puede suceder que el paciente esté inconsciente o incapacitado para comunicarse. En estos casos, el consentimiento puede considerarse implícito con el fundamento de que si la persona estuviere consciente hubiese prestado el consentimiento.

Si lo viéramos desde la perspectiva de Uruguay, el consentimiento del titular es caracterizado como libre, previo, expreso e informado, el que debe documentarse. Y su tratamiento se considera lícito cuando se hubiese recabado. Ahora bien, la normativa vigente prevé que no es necesario recabar el consentimiento para la comunicación de datos cuando se trate de datos de salud y se trate de razones sanitarias. Se prevé que en estos casos se preserve la identidad de los titulares mediante la disociación de datos. [9]

Esta misma solución es adoptada en otras normativas como la española, que establece que no es necesario el consentimiento para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. [10]

9 Artículo 17 de la Ley Nº 18.331, de 11 de agosto de 2008.

10 Artículo 11, numeral 2, literal f) de la Ley Nº 15/1999, de 13 de diciembre de 1999.

5. La E – Salud y las transferencias internacionales

Una de las grandes problemáticas en materia de salud es la transferencia internacional de datos. Éstos se plantean cuando los datos son transferidos a países que no poseen un nivel adecuado de protección. En la sociedad en la que vivimos donde las tecnologías de la información permiten una fluida transferencia de datos, el peligro que los datos de salud, reconocidos a nivel mundial como datos sensibles, y por ende especialmente protegidos, viajen a lugares donde puedan ser utilizados con fines no lícitos, es alta.

También debemos ver el aspecto positivo de las transferencias internacionales. Sin lugar a dudas, el hecho de que las historias clínicas se encuentren disponibles, puede mejorar considerablemente las facilidades de diagnóstico o de tratamiento "permitiendo el recurso a conocimientos médicos disponibles solamente en instituciones médicas extranjeras". Para ello, se considera que la información debe ser remitida en forma anónima o utilizando seudónimos. Esta solución no requiere del consentimiento del titular. [11]

El Grupo de Trabajo del Artículo 29 para la Unión Europea considera que solamente se pueden transferir datos a países que tengan un nivel adecuado de protección de datos. [12] También se considera que en estos casos, se debe prestar especial atención a los aspectos de seguridad de la transmisión de estos datos.

6. E – Salud y Gobierno Electrónico

Si entendemos por Gobierno Electrónico "el uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público (...)", no se puede dejar de pensar que la salud es un aspecto que se encuentre incluido en él. [13] Es así que las Entidades Públicas debe procurar el desarrollo de la E – Salud mediante la adopción de las tecnologías necesarias y brindando un marco normativo suficiente y adecuado.

7. Conclusiones

Más allá de los beneficios que implica el uso de las TIC, es totalmente aplicable aún la finalidad de la salud en general, entendida ésta como la de facilitar la asistencia sanitaria a las personas concretas que, por una u otra causa, hayan sido objeto de las prestaciones realizadas en el marco de su actividad asistencial, la E - Salud debe ser considerada como otro aspecto de la prestación de los servicios de salud que persigue idéntica finalidad. [14]

Por tanto, todos los involucrados deberán analizar todas aquellas mejoras que surjan en virtud de las TIC, tomando en cuenta la protección de este tipo de datos, los derechos involucrados, etc.

El desarrollo de las TIC que permiten actualmente que el acceso clínico de los datos de salud desde

11 http://www.ehu.es/argitalpenak/images/stories/tesis/Ciencias_Sociales/ABERASTURI%20GORRI%C3%91O.pdf (Página visitada el 18 de febrero de 2013).

12 Artículo 17 de la Ley Nº 18.331, de 11 de agosto de 2008.

13 http://www.agesic.gub.uy/innovaportal/v/803/1/agesic/carta_iberoamericana_de_gobierno_electronico.html (Página visitada el 27 de febrero de 2013).

14 http://www.iee.es/pages/bases/articulos/hemeroteca/derint022.html (Página visitada el 26 de febrero de 2013).

casi cualquier punto del planeta debe verse en forma positiva. Se accede a una amplia gama de bases de datos automatizadas, recuperando la información sanitaria para su tratamiento. Este acceso a los datos permite una mejora en el tratamiento de los datos de salud porque al conocer con mayor exactitud los datos, el tratamiento va a ser de mejor calidad.

Desde el punto de vista jurídico, se deben acompasar estos cambios proveyendo de una normativa que brinde las seguridades suficientes para su desarrollo y expansión.

CAPITULO IX
HERRAMIENTAS FORENSES

Dra. Rosario Ierardo

HERRAMIENTAS FORENSES

Dra. Rosario Ierardo

1. Introducción

Por un momento pensemos cuantas comunicaciones electrónicas, documentos electrónicos y archivos multimedia almacenamos en diversos dispositivos. Las herramientas forenses como el E-Discovery permiten identificar, colectar, preparar y preservar información electrónica, en el marco de un proceso legal.

2. Definición de e– Discovery[1]

El E- Discovery es el proceso mediante el cual se puede identificar, colectar, preparar y preservar información electrónica, en el marco de un proceso legal.

Implica la solicitud de información electrónica almacenada o ESI (Electronically Stored Information) para su uso en juicio. Generalmente refiere a: correos electrónicos, historial de la navegación, transacciones en línea, documentos de procesadores de textos, fotografías, mensajes grabados.

Los datos objeto de E- Discovery pueden provenir de cualquier dispositivo electrónico, inclusive aquéllos que son portátiles tales como smartphones o PDA.

Así es como que el E- Discovery incluye, pero no se limita, a toda información almacenada electrónicamente en medios ópticos o magnéticos, cualquier archivo electrónico borrado pero recuperable, fragmentos de archivos y fragmentos de datos guardados en la memoria del dispositivo.

Atento a que el objeto de la información solicitada es su presentación en un juicio, la información tiene que ser relevante para la parte y debe especificarse el criterio de búsqueda.

Es decir, en caso de necesitarse, por motivos judiciales, acceso a la información protegida, debe garantizarse que la extracción de la información sea posible de una manera rápida y acorde a directrices de conservación aséptica, de modo que los hipotéticos procesos judiciales que requieran la información no se vean entorpecidos, propiciando además garantías de que la información se extrae del sistema conservando plenamente su integridad.

La proliferación de los Sistemas de la Información y de la dependencia de los mismos ha ocasionado que en Estados Unidos, se hayan acordado sanciones muy fuertes a las compañías que no respondan rápida y efectivamente a las peticiones de extracción de información. En EEUU, se está aplicando de un modo particularmente específico a las directrices relativas a información médica personal, a las prescripciones de seguridad en el trabajo, y a las regulaciones orientadas a la protección de los inversores, la integridad de mercados financieros y a formación de capital.

1 La definición está tomada del diccionario legal en línea http://definitions.uslegal.com/ (Página visitada el 3 de julio de 2010).

3. Leading case Da Silva Moore vs Publicis Groupe[2]

El juicio de Monique Da Silva Moore vs Publicis Groupe es la primera vez que un tribunal aprueba el uso de un sistema informático para realizar la revisión de la información almacenada electrónicamente (ESI).

En el presente caso se reclama por un despido donde se alega discriminación de género (despido de una trabajadora en estado de gravidez). Como prueba, estaban involucrados más de 3 millones de documentos. Si bien ambas partes habían acordado usar una revisión automatizada, los demandantes controvirtieron el protocolo de los acusados alegando que no era tan transparente como debe ser.

En audiencia el juez instó a las partes a presentar un protocolo común. De todas maneras, se explicita en audiencia que el E- Discovery no es la panacea y sólo debe aplicarse en juicios adecuados, en el presente casoel juez aprobó el uso del E- Discovery por las siguientes cinco razones:

- Existió un acuerdo entre partes para usar este método,
- Estaba involucrado un gran volumen de información,
- En audiencia fue considerado incluso más exacto que la revisión manual,
- Los costos son más reducidos que los costos de pagar un analista humano,
- El software tiene una alto grado de transparencia, lo que es fundamental durante un proceso judicial.

Sin embargo, si la cantidad de información almacenada electrónicamente fuera poco significativa, no se justifica el tiempo y dinero gastado en "entrenar" a un sistema.

Asimismo opinó que la revisión asistida por ordenador es una herramienta disponible y debe ser considerada seriamente para su uso en los casos de gran volumen de datos donde se puede ahorrar una cantidad significativa de los gastos legales en la revisión de documentos.

De hecho el Tribunal consideró la revisión manual usando palabras claves "sobre inclusiva y poco efectiva", comparándola con un juego de niños donde se trata de adivinar la carta que tiene el otro jugador.

A partir estas consideraciones vertidas en el presente caso, los mecanismos de E- Discovery fueron admitidos en diversos juicios.

3.1. Funcionamiento de la Predicción por Codificación (predective coding) y el Reconocimiento óptico de Caracteres (OCR)

El sistema utilizado para la búsqueda de documentos relevantes en el leading case reseñado es la Predicción por Codificación(o predictive coding).

El "Predictive Coding" es un software que, mediante el uso de algoritmos, permite a la computadora reconocer los documentos relevantes para presentar como prueba en determinado juicio, ahorrando el tiempo y los costos que acarrearía una revisión manual.

Como primera medida, el analista humano (en este caso un abogado) evalúa un número limitado de documentos seleccionados al azar del universo de documentos a analizar, a los que adjudica un código que indica su relevancia.
Este subgrupo de documentos recibe el nombre de "seed set", el abogado va codificando como relevante y no relevante los documentos que integran el subgrupo. En base a este "seed set" comienza

2 La opinión del Juez Peck puede consultarse en el link http://www.ediscoverylaw.com/uploads/file/Peck%20Recusal%20Opinion.pdf . (Página visitada el 17 de julio de 2012).

un proceso iterativo de entrenamiento del sistema, que implica múltiples revisiones y pruebas. Luego, el sistema examina las decisiones tomadas por el analista e identifica las propiedades de los documentos codificados, ya que el objetivo es que el sistema tome decisiones propias automatizadas.

A medida que el analista humano continúa adjudicando códigos a la documentación, el sistema es capaz de predecir que documentos serán codificados por el analista. El sistema utiliza algoritmos para analizar el "seed set" y predecir la relevancia de otros documentos en base a lo aprendido.

En el leading case Da Silva Moore, luego de la creación del "seed set" de documentos, el sistema fue "entrenado" con siete grupos de 500 documentos cada uno, antes de comenzar a predecir automatizadamente.

Una vez que la codificación del analista y la predicción del sistema coinciden, el sistema ha aprendido lo suficiente para comenzar a predecir por sí. Es importante tomar en consideración que los abogados que realicen la codificación van a ser los últimos ojos que analizarán la documentación que podrá ser presentada ante la justicia. Es por ello que la tarea de los analistas que realicen la codificación de documentos debe ser minuciosa y sistemática.

Además del software de "predictive coding" existe otra herramienta que permite el análisis de documentos por parte de un sistema experto. Se trata del Reconocimiento óptico de Caracteres (OCR, por sus siglas en inglés).

El OCR es un software que permite identificar automáticamente símbolos o caracteres que pertenecen a un determinado alfabeto, a partir de una imagen. Esto permite ingresar los caracteres al sistema sin tener que utilizar el teclado para su entrada.

Este tipo de sistemas resuelven problemas de segmentación en bloques lógicos, tablas, títulos, gráficos. Generalmente el lenguaje utilizado para completar formularios es fácilmente estandarizable y pueden restringirse opciones (tal como invalidar rangos numéricos en una fecha), por lo que fácilmente puede ser utilizado este elemento.
El rango de exactitud de conversión depende del documento a trasladar. Una página de texto se estima que tiene 2000 caracteres así que aunque el software de OCR tenga una exactitud del 90%, el documento creado tendría unos 200 errores.

4. Proceso del e- Discovery

La aplicación del E- Discovery implica varios pasos a seguir. Primeramente debe preexistir un juicio, donde será implementado el mecanismo de E- Discovery.

Como segunda etapa, los sistemas de información tienen que ajustarse para retener la información relevante.

Luego, las partes en juicio definen la información relevante, así como el objeto de la prueba.

Se procede entonces a las consideraciones iniciales acerca de la información disponible y cuál información electrónicamente almacenada no es razonablemente accesible.

Una vez finalizadas estas instancias previas, es que se procede a recolectar la información relevante almacenada en los sistemas de información. Si no fue solicitado un formato con anterioridad, la misma deberá colectarse en un formato usable.

En este punto, puede presentarse una etapa de test sobre la posibilidad o no de accesibilidad razonable respecto a información contenida en el sistema de información de la parte contraria.

Sobre la información colectada procede un análisis por parte del técnico, que será presentado en el juicio como prueba.

4.1. Orden modelo en los casos de patentes[3]

En setiembre de 2011, también en Estados Unidos, se adoptó un modelo de orden con las pautas para utilizar E- Discovery en casos relativos a patentes de propiedad. Este modelo se centra en la recolección de correos electrónicos y fue creado por el Federal Circuit Advisory Council. El correo electrónico es el medio más utilizado para ventilar los temas litigiosos.

Los correos electrónicos deben ser solicitados de manera separada del resto de la ESI.

No se permite la presentación de solicitudes generales referidas a correos electrónicos. Las solicitudes deben contener la identificación del custodio (que es la persona que tiene el correo electrónico en su inbox), los términos y el marco temporal de búsqueda. En cada búsqueda se puede solicitar información en poder de cinco custodios.

Independientemente a lo establecido, por acuerdo de partes se puede acordar la modificación de los términos de búsqueda y de la cantidad de custodios a requerir. En estos casos los costos deben ser solventados por la parte que solicita los datos.

4.2. Protocolo para los documentos almacenados electrónicamente "ESI Protocol"[4]

En febrero de 2012 el Departamento de Justicia de EEUU aprueba un documento denominado "ESI protocol" que contiene las pautas para la producción de prueba informática en casos criminales.

Este documento plantea principios, tales como que los abogados tienen la responsabilidad de tener un entendimiento adecuado del E- Discovery; las partes deben tener suficientes conocimientos técnicos; la necesidad de pactar el volumen, naturaleza y mecanismos de producción de E- Discovery; los formatos elegidos para la presentación de la prueba deben garantizar la integridad, usabilidad, costos limitados y dentro de lo posible cumplir los estándares de la industria para los mismos. La finalidad de los principios es beneficiar a todas las partes haciendo un E- Discovery más eficiente, más seguro y con menos costos.

Dentro del objeto, se toman los juicios donde el volumen y la naturaleza de la información electrónicamente almacenada aumentan la complejidad del caso.

Asimismo se hace hincapié en la necesidad de proteger la información de accesos no autorizados, dada la calidad de "sensible" de la información que obra en los juicios penales. Las partes deben limitar el acceso a esta información dentro de su propio equipo de abogados.

En la instancia de discusión sobre volúmenes, también hay que determinar cual información deberá ser considerada confidencial y las medidas de seguridad tendientes a evitar accesos no autorizados. Si no existe acuerdo entre las partes se podrá solicitar al juzgado una orden de protección de la información.
Una vez acordadas las medidas de seguridad, se discute la producción de la información en las siguientes categorías:

3 Documento disponible en: http://www.cafc.uscourts.gov/images/stories/announcements/Ediscovery_Model_Order.pdf. (Página visitada el 11 de julio de 2012).

4 El documento se encuentra disponible en la página web http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf. (Página visitada el 12 de julio de 2012).

- Materiales de investigación (p.ej. historiales policiales)
- Declaraciones de testigos
- Documentación referida a objetos físicos (p.ej. archivos de muestras forenses)
- Dispositivos digitales de terceros (p.ej. computadoras, teléfonos)
- Fotografías y grabaciones de audio/video
- Archivos y documentos de terceros
- Información de escuchas
- Pruebas y exámenes
- Informes de peritos
- Acuerdos
- Materiales que requieran consideraciones especiales (p.ej. secretos comerciales, pornografía infantil, información tributaria)
- Otras informaciones relevantes

Si una de las partes se encuentra en prisión, se deberán tomar los recaudos a fin que el acceso a la información no sea limitado por el uso de un software y/o hardware.

Respecto a la transmisión por correo electrónico del E- Discovery, las partes deben acordar tres niveles de seguridad:

- Información que no puede ser transmitida por correo electrónico (p.ej. datos referidos a la protección de testigos, información de seguridad nacional, secretos comerciales).
- Información que puede ser transmitida por correo electrónico previamente encriptada (p. ej. información de negocios, datos personales).
- Información que puede ser transmitida por correo electrónico.

Este protocolo también define términos a fin que todas las partes implicadas en un litigio, los utilicen de manera unívoca.

Finalmente cuenta con una lista de elementos a tener presentes en el caso de utilizar E- Discovery:

- ¿El volumen o la naturaleza de ESI aumentan perceptiblemente la complejidad del caso?
- ¿Este caso implica la información clasificada?
- ¿Implica secretos comerciales, seguridad nacional?
- ¿Las partes tienen asesores técnicos apropiados?
- ¿Las partes se han reunido y han definido sobre posibles problemas?
- ¿Las partes han acordado el formato?
- Las categorías que se pueden incluir (ya descriptas ut supra)
- Tabla de contenidos
- Si los expedientes papel se procesarán como ESI
- ¿Quién es el propietario de los datos?
- Si hay información clasificada, sensible, tributaria, de secretos comerciales o similares
- Si la transmisión por correo electrónico es adecuada
- Si el demandado está preso y puede acceder a la información
- Si alguna parte tiene limitaciones de hardware o software
- Si hay producción a partir de un dispositivo digital de terceros
- Si hay imágenes "espejo" forenses o dispositivos digitales
- Tratamiento de metadatos de terceros
- Medidas de seguridad para la transmisión por correo electrónico
- Medidas de seguridad para evitar accesos no autorizados
- Si se necesitan órdenes de protección por parte del juzgado
- Si los costos y/o tareas son compartidos
- Como preservar los documentos
- ¿Se documentaron acuerdos y desacuerdos de las partes?
- ¿Hay algún acuerdo informal entre partes para la resolución de controversias?
- ¿Hay necesidad de designar un coordinador de E- Discovery en el caso de múltiples demandados?

5. Conclusiones

El E- Discovery debe utilizarse en el supuesto que exista un juicio donde relevar la prueba manualmente sea excesivamente costoso y dilatado temporalmente. De todas maneras la utilización de herramientas forenses deben ser usadas de manera que no vulneren la privacidad de las personas.

La utilización de E- Discovery, se acepta jurisprudencialmente en Estados Unidos, país del common law, pero hay que tener en cuenta cómo se debería habilitar su utilización en países codificados como el nuestro.

CAPITULO X

GEOLOCALIZACIÓN PÚBLICA Y PRIVADA

Dra. Esc. Beatriz Rodríguez

GEOLOCALIZACIÓN PÚBLICA Y PRIVADA

Dra. Esc. Beatriz Rodríguez Acosta

1. Introducción

Nos encaminamos a un mundo más abierto, mucho más interconectado donde la tecnología lo que ha hecho es facilitar esa tendencia, fruto de una necesidad básica en el ser humano: relacionarse con otros, buscar grupos de pertenencia e iguales con los que identificarse.

Por lo tanto, ahí es donde nace la creciente necesidad de la llamada geolocalización o el geoposicionamiento, porque la mejor manera de encontrar algo es saber dónde está localizado, coordenadas exactas de espacio y tiempo real para facilitar la tarea[1].

Este valor de la ubicación geográfica se ha vuelto muy importante principalmente para las compañías o empresas, beneficiándose más aún con la utilización de la tecnología celular.

En los últimos 20 años se ha producido un aumento en el uso de los datos de localización debido a dos factores principales:

- Aumento en el uso de los datos de localización vía satélite, mayormente en lo que se refiere a la asistencia de personas en peligro,
- La difusión de la telefonía celular, mediante la cual cada usuario lleva siempre un dispositivo por el que se le puede localizar.

La tecnología de geolocalización se basa en el Sistema de Información Geográfica (GIS) para la gestión, análisis y visualización del conocimiento geográfico.

El conocimiento geográfico se estructura en diferentes conjuntos de información, ya sean mapas interactivos que ofrecen una visión interactiva de la información geográfica como respuesta a cuestiones concretas, datos geográficos que incluyen información vectorial, modelos digitales del terreno, así como modelos de geoprocesamiento de datos, y de metadatos[2].

¿Para qué se utiliza esta tecnología? Para diferentes situaciones: como llegar al trabajo evitando las zonas con más tráfico, buscar un restaurante, publicar el lugar exacto en el que nos encontramos para compartirlo con nuestros contactos, saber dónde quedamos para cenar, entre otras.

Sin embargo, esta nueva forma de encontrar "algo o alguien" puede estar vulnerando derechos fundamentales, como por ejemplo la privacidad, la intimidad, ese algo que los individuos no quieren que los terceros ajenos a su entorno tengan acceso sin su consentimiento.

1 http://www.marketingnews.es/varios/opinion/1051829028705/geolocalizacion-meeting-points.1.html (Página visitada el 21 de abril de 2012).

2 http://www.idg.es/computerworld/articulo.asp?id=167772 (Página visitada el 21 de abril de 2012).

2. Concepto

Antes de comenzar con el concepto podemos decir que los términos localización, georreferenciación, geolocalización, geoposicionamiento son sinónimos por lo que se puede utilizar cualesquiera de ellos. Este término es bastante reciente, se puede calificar como un neologismo, que aparece en nuestro idioma desde mediados de 2009.

En el Diccionario de la Real Academia Española[3] no se encuentra la palabra "geolocalización" definida, pero sí hayamos la palabra "localización" la que significa: acción y efecto de localizar. Localizar es: averiguar el lugar en que se halla algo o alguien. Esta palabra al tener el sufijo "geo" incorporado se refiere a la identificación de una situación geográfica en forma automática.

Este concepto lo tenemos que vincular con el concepto de la tecnología utilizada para su realización, el sistema de información geográfica o SIG.

El SIG de acuerdo con la definición de F. Bouillé de 1978, es un modelo informatizado del mundo real, descrito en un sistema de referencia ligado a la Tierra, establecido para satisfacer unas necesidades de información específicas respondiendo, del mejor modo posible, a un conjunto de preguntas concreto[4].

3. Clasificación

La geolocalización puede ser de diferentes tipos por lo que podemos clasificarla en:

- **Directa:** la ubicación se realiza mediante coordenadas, está establecido para un determinado sistema de proyección,
- **Indirecta**: se asocia al elemento que se representa, que puede ser una clave o índice, casi siempre éstas son datos administrativos como puede ser una dirección, el código postal, que son usados para la determinación de una posición,
- **Referencial:** se efectúa mediante un punto de interés determinado.

Otra forma es clasificarla es de acuerdo con el medio por el cual se realiza la geolocalización:

- **Por medio de GPS (Global Positioning System: sistema de posicionamiento mundial):** éstos obtienen su localización vía satélite. Es la más usada y confiable de todas, por la cobertura, movilidad y sobre todo la precisión que ofrece. Ejemplo: GPS Dedicados, Sistemas de Navegación, algunos SmartPhones,
- **Triangulación de antenas de redes celulares:** es la más distribuida y la menos usada, esto debido a que no es muy difundido por las compañías, el coste no es muy accesible, en muchos casos las mismas compañías bloquean el acceso. Aunque la precisión no es tan buena, se aproxima bastante a lo real. Ejemplo: Celulares de las últimas generaciones, smartphones, conexiones 3G,
- **Por dirección IP:** ya muchos scripts (guiones, archivos de órdenes simples que en Windows se dan cuando usamos lenguajes como Java) y nuevos estándares son capaces de ofrecernos información sobre nuestra localización por medio de IP. Es el sistema más inexacto en la mayoría de las ciudades, debido a que localiza el último nodo que nos distribuye señal a nuestro hogar u oficina, a veces puede ser muy cercano, aunque otras puede no serlo, dependerá de nuestro proveedor de Internet, que tan bien mapeados y distribuidos estén sus

3 http://buscon.rae.es/draeI/SrvltConsulta (Página visitada el 21 de abril de 2012).

4 http://www.minhap.gob.es/ (Página visitada el 30 de abril de 2012).

nodos de conexión[5].

- **Wi Fi:** la tecnología es similar al uso de estaciones de base. Se valen de un número de identificación único que puede ser detectado por un dispositivo móvil y ser enviado a un servicio que conoce la ubicación de cada uno de estos puntos de identificación únicos. La identificación única de cada punto de acceso WiFi es su dirección de control de acceso al medio conocidas como las direcciones MAC por las siglas inglesas de Medium Access Control. Esta localización es cada vez más precisa debido a la medición continua que se realiza. La dirección MAC de un punto de acceso WiFi, en combinación con su ubicación calculada, está íntimamente ligada a la ubicación del propietario del punto.

4. Consecuencias de la geolocalización

Al momento de surgir los sistemas de localización se pensó que eran datos técnicos, no se les dio otra naturaleza, solo que eran necesarios para hacer y recibir llamadas por los teléfonos celulares, y quienes tenían esos datos técnicos, solamente eran los operadores de comunicaciones electrónicas.

Con el correr del tiempo y el avance de las tecnologías comenzaron las empresas a darse cuenta que estos datos suministraban información de los individuos y así pasaron a verse como una potencial forma de ingreso para ellas.

Estos datos van dejando la estela de actividades que realiza la persona al cabo del día, por ejemplo cuando sube al ómnibus y compra el boleto con la tarjeta, cuando va al cajero automático del banco y retira dinero, cuando utiliza su celular, como vemos no solo usando el teléfono celular podemos ser localizados.

Con la localización aparecen situaciones nuevas que resultan ventajosas y desventajosas dependiendo en qué situación nos encontremos.

Entre las nuevas situaciones que surgen podemos mencionar: el marketing de proximidad, la realidad aumentada, la geolocalización social.

4.1. Marketing de proximidad[6]

El marketing de proximidad es la distribución de contenido o información de relevancia a través de mensajes multimedia, texto, imagen, utilizando dispositivos móviles dotados de Bluetooth una transmisión que será recibida por los usuarios que estén ubicados a una distancia próxima del punto emisor.

La estrategia del marketing de proximidad tiene como principal fortaleza el hecho de contar con la autorización previa del cliente para poder ver y recibir la publicidad, lo que hace de ella una estrategia totalmente eficiente que cuenta con el consentimiento y por lo tanto el interés de los usuarios.

Este marketing tiene una eficiencia del 90% de acuerdo con un estudio realizado por Telefónica, pero uno de los principales obstáculos a los que se enfrenta esta modalidad radica en la delgada línea que separa la información del abuso, por lo que se aconseja a las empresas que lo vayan a utilizar no llegar al abuso con los envíos de mensajes.

Hay que tener presente también que lo único que se conoce del usuario es su localización por lo que es necesario para poder acceder a él, su permiso y consentimiento con lo que la privacidad está garantizada.

5 http://jafrancov.com/2010/07/que-es-la-geolocalizacion/ (Página visitada el 21 de abril de 2012).

6 Su especialista en Mercadeo. Dial.net. (Página visitada el 30 de julio de 2012).

Esta publicidad que es de interés para el usuario ya que dio su consentimiento, no sólo se va a transmitir por las redes sociales como Facebook y Twitter sino que también lo hará por aquéllas que usan los sistemas de geolocalización como Foursquare.

La geolocalización se nutre con la publicidad del marketing de proximidad por lo que le es de gran valor y ha encontrado en las redes sociales su plataforma de propagación e identificación de nuevas áreas de negocios pensadas para la satisfacción de nuevos intereses y necesidades derivadas de la interacción.

Los mensajes tienen posibilidades amplias porque pueden ir desde informar sobre algún servicio cercano, ya que juegan con el valor añadido de la posición geográfica, así como invitar a alguien a descargarse contenidos o cambiar cupones de descuentos.

4.2. Realidad aumentada[7]

La realidad aumentada es el término que se usa para definir una visión directa o indirecta de un entorno físico del mundo real. Además combina elementos reales con otros virtuales creando una realidad mixta en tiempo real. Es decir, podemos apuntar la cámara de nuestro móvil a un punto determinado de la calle y en nuestra pantalla aparecerán esos elementos más una sobreimpresión virtual, como por ejemplo ofertas en un restaurante o el precio del apartamento en venta al que se está apuntando.

Ayuda a dar respuesta a necesidades con soluciones justo a tiempo. Es el usuario el que la busca, al revés del marketing de proximidad.

Esta sobreimpresión virtual se puede enviar a otros amigos y utilizando la geolocalización podemos encontrar el punto que queremos o a quien queremos.

Sistemas como Google Latitude o Foursquare utilizan estos servicios aplicándolo a las redes sociales; al conectarse ya se puede ver dónde están los amigos, o visitar un sitio nuevo y compartir la localización.

Foursquare puede convertirse en un juego ya que permite hacer check-ins en lugares nuevos y va dando puntos por ello. De este modo el conseguir medallas (badges) por descubrir sitios nuevos, o ser el "mayorship" de un sitio por ir muy a menudo al restaurante favorito, se puede convertir en una competición con los amigos. Por no hablar de las recomendaciones de primera mano que tendrá de los lugares más sugerentes.

La publicidad ya está probando la realidad aumentada, ya que es un medio interactivo y sorprendente.

4.3. Geolocalización social

Actualmente no basta con decir qué, con quién, cuándo y cómo, sino que queremos que todos se enteren dónde hacemos las cosas que hacemos.

La geolocalización social cuenta de tres elementos: el sistema de geolocalización, el teléfono móvil y la red social.

7 ainara%20ladrero%20social%20media%20Geolocalización%20y%20realidad%20aumentada_.html (Página visitada el 24 de julio de 2012).

Los principios que debemos tener en cuenta en la geolocalización social son los siguientes:

- Se necesita solucionar una necesidad en un solo click el famoso "just in time"
- Todos somos usuarios pero cada uno hace un uso diferente
- Los usuarios interactúan de forma diferente con el producto, quieren más información que les sorprendan, quieren sentir que son ellos los que controlan la situación
- los celulares se han convertido en una extensión de nuestro cuerpo y mente, por lo que entrar en ellos es formar parte de la intimidad del individuo
- es necesario facilitar al usuario el control de la seguridad
- con Internet en el celular y la geolocalización social no existen las fronteras y se debe buscar la simplicidad

La geolocalización unida a las redes sociales es un canal para los centros de contacto que tienen la intención de optimizar sus servicios, se dice que con esta modalidad Internet dejaría de ser Internet porque se podría localizar a la persona en el lugar en que está.

5. Privacidad

El punto relevante de la geolocalización es saber qué se va a hacer con el tratamiento de los datos personales.

¿Qué sucede con la privacidad y estas nuevas modalidades de utilización de la tecnología? ¿Realmente, la geolocalización afecta o no la privacidad?

No siempre queremos ser localizados, y mucho menos que esa localización la sepa todo "el mundo".

Al principio se almacenaban los datos personales obtenidos por los operadores de telecomunicaciones, ahora se va más allá y se utilizan, cómo vamos a tratarlos para no vulnerar los principios consagrados en el tratamiento de datos personales al agregarle un valor añadido dado por empresas, que muchas veces ni siquiera están en el territorio en el que se encuentra el involucrado.

Esto trae consigo dos consecuencias, la reticencia de un uso masivo de este tipo de tecnologías y los problemas legales con los que se pueden encontrar.

En la práctica, estos sistemas de geolocalización presentan diversas cuestiones que los proveedores de servicios de geolocalización deben conocer para respetar y garantizar el derecho a la intimidad y a la protección de datos personales de los usuarios de servicios de geolocalización.

De acuerdo con las nuevas modalidades que van surgiendo, con respecto al marketing de proximidad utilizando la tecnología de Bluetooth no se verían afectados los usuarios, ya que el individuo presta su consentimiento para que llegue a su celular la información que solicita entrar.

Actualmente la regulación, a nivel de derecho comparado, de la geolocalización en el sector de los celulares se limita, principalmente, a la Directiva Europea de Protección de Datos 95/46/CE.

A efectos de la aplicabilidad de esta directiva se considera que los datos de localización de los Smartphones y la combinación de la dirección única MAC y de la localización calculada de un punto de acceso WiFi son datos personales.

Respecto a las estaciones de bases o antenas y los datos obtenidos por los operadores de telecomunicaciones se aplica la Directiva Europea de Privacidad 2002/58/CE.

Sin embargo, estas directivas establecen el régimen general de la protección de datos sin llegar a resolver cuestiones específicas de la geolocalización a través de los dispositivos móviles, es decir,

son meras directrices. No obstante, este instrumento conlleva una serie de riesgos propios, sobre todo de privacidad, que requieren un tratamiento individualizado y que deberán ser objeto de una regulación en un futuro cercano.

El hecho de que los usuarios conserven el móvil prácticamente las 24 horas del día con ellos, unido al hecho de que los celulares suelen contener un alto contenido de información personal, provoca que los proveedores de servicios basados en la geolocalización cuenten con una base de datos muy amplia sobre los consumidores.

Dichos proveedores pueden conocer desde el domicilio de un usuario a través de la inactividad nocturna, hasta el lugar de empleo del mismo a través de la pauta de desplazamiento por la mañana o incluso un patrón de comportamiento puede mostrar datos específicos como visitas a lugares religiosos, presencia en manifestaciones u otros datos que afectan a la esfera privada de los particulares.

Además esta constante vigilancia de la localización que permite la tecnología de los Smartphones puede ser secreta o semi secreta, por ejemplo cuando no se informa debidamente de que los servicios de localización están en la posición "on".

El mayor riesgo que plantea la evolución de la geolocalización y, por tanto, de los datos disponibles, es el de los nuevos usos que pueden darse a dichos datos, usos que no se han tenido en cuenta cuando fueron obtenidos.

Las Autoridades de Protección de Datos destacan el impacto que pueden tener en la privacidad de los usuarios los Servicios de Geolocalización debido a que la tecnología de dispositivos móviles inteligentes- Smartphones- permite la monitorización constante de los datos de localización, a que los dispositivos están íntimamente ligados a una persona concreta, y a que normalmente existe una identificabilidad directa e indirecta del usuario.

El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE ha analizado la problemática de los datos de localización obtenidos a través de Smartphones[8].

El Grupo dispone que la principal base legítima que hay que aplicar en una regulación de la geolocalización en el sector de los móviles sea la del previo consentimiento informado. Pero dicho consentimiento plantea problemas, ya que no siempre está claro si realmente ha sido concedido libremente, si el que lo concede conoce lo que éste abarca o bajo qué condiciones lo concede.

En primer lugar, en el consentimiento han de especificarse la finalidad para la que se procesan los datos (si estos cambian, el consentimiento deberá renovarse), el plazo concreto por el que se presta el consentimiento y la especificación de los datos de localización que se conservarán.

El Grupo establece que por defecto, los servicios de geolocalización deben estar en "off", ya que, un mecanismo de opt-out no es adecuado para obtener el consentimiento informado del usuario.

Además, el consentimiento puede ser problemático respecto a ciertas personas como empleados o menores. En el primer caso, la decisión del empleado a oponerse a prestar su consentimiento puede conllevar la pérdida de su trabajo. Por eso en el ámbito laboral, ha de demostrarse que el consentimiento es necesario para alcanzar un objetivo legítimo y que éste no puede conseguirse por medios menos intrusivos.
En cuanto a los menores, los padres pueden estar interesados en la aplicación de la geolocalización como medio de control de la actividad de sus hijos. Pero al mismo tiempo la intimidad y la privacidad de los menores han de ser protegidas. El Grupo considera que son los padres los que deben hacer balance y juzgar si la utilización de la geolocalización está justificada, pero han de informar a sus

8 Opinión 13/11 del G29 http://ec.europa.eu/justice/data-protection/index_en.htm (Página visitada el 30 de julio de 2012).

hijos y dejarles participar en la decisión de la aplicación de la geolocalización.

Al elaborar el mapa de los puntos de acceso WiFi, las compañías pueden almacenar legítimamente direcciones MAC y calcular las localizaciones de dichos puntos de acceso necesarios para ofrecer sus servicios de geolocalización. Para que este almacenamiento sea legítimo, el responsable de los datos mencionados ha de ofrecer la posibilidad de darse de baja de la base de datos sin trabas.

El Grupo también se pronuncia en cuanto a la información ofrecida a los usuarios. Ésta ha de ser clara y comprensible para el ciudadano medio, además de fácilmente accesible. La calidad de la información sobre el servicio es requisito indispensable para la validez del consentimiento. Respecto a esto los sitios web de redes sociales y navegadores tienen un papel muy importante.

Para proteger los derechos de los sujetos de los datos, los responsables de los datos de geolocalización tienen que dar la posibilidad a los usuarios de acceder a sus datos de localización en un formato legible y permitirles su rectificación y eliminación sin necesidad de aportar excesivas trabas.

Finalmente se pronuncia sobre los períodos de retención de los datos, recomendando que los datos de geolocalización o perfiles derivados de los mismos deberían ser eliminados tras un período razonable que está aún por determinar.

En Estados Unidos se ha tratado el fenómeno de la geolocalización en varios proyectos de legislación que han estado a punto de ser aprobados pero han quedado por el camino, pero actualmente los legisladores están presionando por una legislación destinada a hacer frente a los problemas de la recolección, uso y divulgación de información de localización.

En el 2012, la Comisión Federal de Comercio (FTC) ha establecido que determinados datos recolectados por la geolocalización tienen la característica de ser datos sensibles que merecen un mayor nivel de seguridad y protección.

Así en lo que va de este año ya se han presentado tres proyectos de ley en el Congreso:

- El proyecto denominado Geolocalización, Privacidad y Vigilancia (GPS) regula la penalización del seguimiento de las personas y exige al gobierno obtener una orden antes de la recolección de la información.

  Este proyecto define la información de geolocalización como la información derivada de un dispositivo que no es el contenido de una comunicación que puede ser utilizado para determinar o inferir sobre la ubicación de una persona.

  Además, prohibía a las empresas que revelen los datos de seguimiento geográfico de sus clientes a terceros sin su consentimiento.

- Otro de los proyectos presentados en marzo de este año fue la Ley de Protección de Geolocalización de Comunicaciones en Línea, que define nuevamente qué es la información de geolocalización, pero a diferencia del proyecto mencionado anteriormente, no se ocupa de la recolección de datos en el ámbito comercial, ni del uso e intercambio de esta información, sino que se centra en garantizar que tanto la información de localización como las comunicaciones electrónicas cuentan con la protección de la Cuarta Enmienda contra el acceso no gubernamental

- El tercer proyecto ya había sido presentado con anterioridad en 2011 y aprobado por el Comité Judicial del Senado en diciembre de 2012. Este prohíbe a las empresas recolectar, recibir, registrar, obtener o divulgar la información de geolocalización de un dispositivo de comunicaciones electrónicas, como por ejemplo los smartphones, sin el consentimiento expreso.

Dado que la información de localización puede ser recogida y utilizada en muchos contextos diferentes y tipos de datos, empresas y organizaciones serían afectadas por la legislación de geolocalización.

6. Casos prácticos

El servicio por excelencia basado en la geolocalización es Foursquare, es aplicado a las redes sociales y fue creado en el 2009.

Se basa en marcar (check-ins) lugares específicos donde uno se encuentra e ir ganando puntos por "descubrir" nuevos lugares, los que son recompensados con "badges", una especie de medallas, y los "mayorships", que son ganadas por las personas que más hacen "check-ins" en un cierto lugar. A partir de la información que los usuarios han ido introduciendo el servicio ha evolucionado hacia un motor de recomendaciones, el cual sugiere lugares interesantes de manera inteligente.

Tenemos otros servicios que usan la geolocalización como el Google Street View que ha sido desarrollado desde Google Map y Google Earth. Este proporciona panorámicas desde el nivel de la calle permitiendo a quien lo use ver la ciudad seleccionada.

Esto llevó a que numerosas personas opinaran sobre este servicio estableciendo que violaba la privacidad de las personas cosa que Google desmintió porque solo se tomaban imágenes de la calle y se bloqueaban todas aquéllas que vulneraran la intimidad.

Esto llevó a un enfrentamiento entre el Comisionado Federal de la Autoridad de Protección de Datos de Alemania Peter Schaar y Peter Flescher del Consejo de Privacidad de Google, debido a que el primero sostenía que eran detectadas las direcciones MAC con las cámaras de Google y esto estaba violando la privacidad de acuerdo con el trabajo realizado por el Grupo del artículo 29.

Gowalla era una red con servicio de localización que fue comprada por Facebook, pero que la cerraron en marzo de este año porque no resistió a Foursquare.

Google Place no existe más es reemplazado por Google Plus para incorporar su red social a sus otros productos, con el objetivo de crear una experiencia web unificada.

En nuestro país tenemos sistemas que usan la geolocalización como Encuentra de Antel e iBus de Movistar y Cutcsa por ejemplo.

Encuentra[9] es un servicio que ayuda a encontrar la ubicación geográfica aproximada de los amigos, los hijos o la persona con servicio de ANTEL móvil que se desee hallar en cualquier momento, así como obtener el listado de lugares de interés que se encuentran próximos a la ubicación del usuario.

Este servicio cuenta con el consentimiento de las personas a ser contactadas, ya que al momento de querer hacerlo se los invita a ser parte de la agenda perteneciente a quien tiene Encuentra. Los invitados deben autorizarlo a que los localice, si no lo hacen no podrá encontrarlos. Tienen que ser de ANTEL móvil todos para poder utilizar el servicio.

Para aceptar el invitado que se quiere localizar envía la palabra ACEPTAR + Celular. Es importante notar que la autorización se pide y se otorga a un celular específico, no a una localización en particular. Si autoriza a que otro usuario te localice, no recibirá más SMS pidiendo la autorización cada vez que intente localizarlo ese usuario autorizado, lo ubicará directamente sin notificarle nuevamente.

9 http://www.antel.com.uy (Página visitada el 30 de julio de 2012).

Se puede realizar seguimiento de los contactos especificando cuánto tiempo se quiere hacer éste y con qué frecuencia se realizarán las localizaciones. Existen algunas excepciones como, cuando el celular esté apagado, fuera del área de cobertura, en roaming o cuando el usuario esté fuera del horario habilitado o suspendido, donde no será posible obtener una localización del celular.

Si bien se solicita el consentimiento del invitado para ser localizado, así como se puede bloquear los datos o darse de baja del servicio, en ningún momento se específica que pasará con la protección de los datos personales en caso de comunicaciones, trasferencia, etc..

Otro de los servicios de geolocalización que se brinda en nuestro país es el iBus[10], por el que al enviar un mensaje de texto se recibe como respuesta un sms con la identificación de las paradas y/o el tiempo estimado de arribo al lugar del próximo ómnibus del recorrido consultado, brindando el acceso universal de la información, incentivando y motivando la mejora del transporte público de pasajeros.
No se menciona nada acerca de la normativa de protección de datos pero podría quedar implícita dentro de la cláusula de legislación aplicable.

7. Conclusiones

La geolocalización es un sistema que ayuda a ubicar a las personas y a las cosas en el lugar geográfico en que se encuentran.

Esta ubicación puede dejar resultados positivos o no, dependiendo del uso que se le de a la información que surja de ella y si se le han aplicado los principios de la protección de datos personales como el consentimiento previo e informado.

Si bien existe normativa que puede ser aplicada a ella por extensión, no siempre se la considera.

En nuestro país podemos aplicar la Ley Nº 18.331, de 11 de agosto de 2009, de Protección de Datos Personales y Acción de Habeas Data, debido a que tanto los datos utilizados por el teléfono inteligente para realizar la geolocalización combinados con la dirección MAC (que es única al igual que las IP) como los datos de la localización calculada de un punto de acceso WiFi, son datos personales, que al final identifican a la persona (Art.4º literal D)).

10 http://www.ibus.com.uy/terminos_y_condiciones.html (Página visitada el 30 de julio de 2012).

CAPITULO XI

MARKETING COMPORTAMENTAL EN LINEA

Prof. Dra. Esc. María José Viega

MARKETING COMPORTAMENTAL EN LINEA

Prof. Dra. Esc. María José Viega

1. Introducción

El marketing directo, la publicidad en Internet, la captura de datos con fines de publicidad han sido temas que hemos abordado con anterioridad en diversos trabajos. Pero, tratándose de un aspecto tan crítico de la vida comercial, del contacto comercial inicial, de la forma en que podemos llegar a los consumidores, como obtener nuevos clientes y acceder a un nuevo nicho de mercado, cuando toda la información se encuentra disponible en Internet y existe la tecnología para procesarla y utilizarla de la forma más provechosa, nos sigue planteando permanentes desafíos1.

En el diccionario de la Real Academia Española la palabra "comportamental" no se encuentra. Marketing comportamental es la traducción que se ha realizado de la expresión **"on line behavioral advertising"** (OBA).

En una ponencia realizada en el año 2002 sobre "Privacidad en Internet" decíamos: "Hoy por hoy se entiende que la vida privada no se limita a la intimidad, sino que este concepto ha sido sustituido por uno más general como es el de privacidad. Internet es una amenaza en la difusión de elementos relativos al individuo y un desafío para el derecho no solo en este tema puntual sino a las repercusiones que tiene en general la globalidad"2. Estos temas son tan actuales como en aquel momento, incluso aumentando la problemática basado en el mayor desarrollado tecnológico.

Y agregábamos que "La Red es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www. Para enfrentar este desafío debemos tener en cuenta los siguientes elementos: a) en primer lugar que la infraestructura de Internet está basada en datos personales (IP); b) un segundo elemento se refiere a los instrumentos técnicos utilizados, los software de navegación, por ejemplo, que envían más información de la requerida para realizar una conexión y c) en tercer lugar la cantidad de datos que nos solicitan para realizar actividades comerciales en línea".

Destacábamos tres elementos de fundamental importancia en Internet para el manejo de datos, que recopilan y envían información sin que los usuarios estemos informados. Y mencionábamos: las cookies, los navegadores y los contenidos activos.
La Comisión Federal de Comercio (FTC) en los EE.UU. define el Online Behavioral Advertising (OBA) como "el seguimiento de las actividades de los consumidores en línea a través del tiempo -incluyendo las búsquedas que ha llevado a cabo el consumidor, las páginas web visitadas y el contenido que ha visto- con el fin de ofrecer publicidad dirigida a los intereses de los consumidores individuales".

Según Phil Lee3 el objetivo de la OBA es servir a la publicidad que es más relevante para los intereses de los consumidores y, al hacerlo, aumenta el digamos el **click-through** en esos anuncios. Algunos estudios han sugerido que los anuncios dirigidos actualmente tienen un **click-through rate**

1 Viega, María José. "El marketing comportamental en línea desde la óptica de los datos personales". Ponencia presentada como miembro del Comité Organizador en el Congreso de Derecho Informático. Mar del Plata, 2011.

2 Viega María José. "Privacidad en Internet". Anuario de Derecho Informático Nº 2. Fundación de Cultura Universitaria. Páginas 235 y siguientes.

3 Lee, Phil. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

de aproximadamente 6.700% más alto que el que ordinariamente tiene una red.

Como se observa, este es un problema que no solo preocupa a la Unión, sino que interesa a nivel internacional. EE.UU. también ha buscado vías para dar soluciones a las empresas y proteger a los consumidores. En esta línea, el FTC tiene como cometido vigilar que las compañías cumplan lo prometido. Un caso reciente fue una queja recibida en agosto de 2012, respecto a que Google pasó a terceros cookies de sus usuarios. El FTC entendió que esto era una violación a los acuerdos y sancionó a Google con una multa de U$S 22.5 millones, que es la multa más alta que han aplicado en materia de privacidad4.

2. Modalidades de publicidad comportamental

Existen diferentes modalidades a través de las cuales es posible realizar un seguimiento de un usuario a los efectos de determinar su comportamiento con fines de envío de publicidad. Analizaremos las siguientes, no sin antes mencionar que la tecnología avanza día a día y por tanto es necesario pensar en soluciones tecnológicamente neutras a los efectos de que continúen siendo de utilidad a pesar de las nuevas modalidades que puedan ir apareciendo.

2.1. Las cookies

La tecnología más utilizada son las cookies de rastreo que se instalan en el terminal del usuario, consiste en un código alfanumérico que se almacena y recupera posteriormente y permite que el proveedor reconozca a un antiguo visitante que va construyendo un perfil. Normalmente las cookies las coloca el editor y no el propietario del sitio, por lo que se suelen llamar "cookies de terceros".

Podemos caracterizar a las cookies de la siguiente forma:

- Están ligadas a un dominio: solo puede leerlo o modificarlo el sitio de internet procedente de un dominio similar.
- Tienen vidas útiles distintas. Encontramos las "Cookies persistentes" duran mucho tiempo o hasta que se las borre manualmente.
- Si la persona utiliza diferentes buscadores, las cookies serán diferentes para cada buscador.

Las "Flash cookies" poseen técnicas reforzadas de rastreo y no pueden borrarse con la configuración tradicional de privacidad de un buscador. Se utilizan para restaurar las cookies tradicionales. Esta práctica se conoce como **respawning** (reproducción).

2.2. Control del contenido de los usuarios

En esta modalidad la red de publicidad se asocia con un ISP para controlar el contenido de las búsquedas del usuario e insertar cookies de rastreo en todo el tráfico no encriptado de webs.

Un ejemplo de ello es la empresa Phorm, que utiliza tecnología Webwise y ofrece un servicio de publicidad comportamental que usa la inspección por paquetes en profundidad para examinar las páginas que visitan los usuarios. Phorm realizó acuerdos con los ISP para poder realizar el servicio. El G29 aclara que no tiene conocimiento que esta tecnología se esté aplicando en la Unión Europea, pero que los problemas jurídicos van más allá de la protección de datos y exceden el ámbito del dictamen.

4 Ramírez, Edith. Marketing Comportamental en línea. http://privacyconference2012.org/wps/wcm/connect/c376b5004e43e1c88f43ffc08ba-c212e/Panel_G_Marketing_comportamental_en_linea.pdf?MOD=AJPERES (Página visitada el 28 de agosto de 2013).

2.3. Localización física

Otra forma de determinar un perfil del usuario es a través de la localización física, que puede deducirse de la dirección IP y de los puntos de acceso wifi.

Phil Lee[5] manifiesta que vale la pena recordar que, aunque la opinión del Grupo de Trabajo se centra en redes de anuncios de terceras partes y cookies en realidad hay diferentes tipos de OBA. Y establece los tres tipos principales que se ven típicamente, cuyo análisis desarrollamos a continuación.

En primer lugar, es cuando un editor del sitio web, pone sus "cookies" en sus propios sitios web y recoge información sobre los visitantes y utiliza esa información para orientar los anuncios a los visitantes en su propio sitio. Eso es bastante común, se puede pensar en ello por ejemplo, cuando se visita Amazon y Amazon le da recomendaciones de libros basados en la navegación anterior y el historial de compras. Y curiosamente, en realidad, es algo que la gente probablemente ni siquiera pensaba en llamar OBA, hasta hace más o menos un año.

En el otro extremo del espectro, está la vigilancia del tráfico de los ISP o la inspección profunda de paquetes y esta es tecnología de punta desplegada por organizaciones como PHORM. Lo que ocurre allí es que el proveedor de tecnología OBA intercepta todo el tráfico que pasa a través de un proveedor de servicios de Internet y recoge los detalles sobre las páginas web que se utiliza y los hábitos de navegación de los clientes, y el ISP usa esa información para orientar los anuncios en sitios web de la asociación y es lo que está en el lado más intrusivo del espectro de la publicidad de comportamiento. Si lo desea, puede pensar en él como que tu cartero inspeccione tu correo.

Redes de anuncios de terceras partes, una especie de modelo de anuncio de Google, se encuentra en algún lugar entre los dos extremos del espectro. Y lo que pasa es que un proveedor de la OBA coloca cookies en sitios web de un asociado para recopilar información sobre los visitantes de esos sitios y el objetivo es generar anuncios a los usuarios. Ahora, históricamente, una gran parte del debate en torno a OBA inició el interés sobre formas de la tecnología en el Reino Unido en 2008. Lo que ocurrió allí fue que PHORM desarrolló un ensayo de su tecnología con un proveedor servicios de Internet aquí con British Telecom y lo hizo sin hacer ningún tipo de declaraciones a los usuarios. La prensa lo llamó un tipo de "ensayos secretos". Cuando salió a la luz, los usuarios estaban naturalmente disgustados de que su tráfico ISP estuviese siendo monitoreado sin su conocimiento y sin su consentimiento. Y recibió mucha atención adversa de la prensa y de todo lo que siguió después, todo el debate y la regulación europea que siguió es la forma en que realmente comenzó esta historia.

2.4. Redes sociales

El usuario de las redes sociales puede intentar controlar, con la configuración de su perfil, qué datos quiere que sean públicos y para quién, pero la cuestión se plantea con la información que tiene de él el prestador de servicios de redes sociales y los usos que de ella se hagan así como la información publicada por terceros sobre este usuario[6].

En las condiciones de uso de Facebook encontramos lo siguiente: "Es posible que Facebook utilice información de tu perfil sin identificarte individualmente ante terceros. Esto se hace con propósitos como establecer a cuanta gente en una red le gusta una película, y para personalizar anuncios y promociones".

5 Lee, Phil. Ob. Cit.

6 Paniza Fullana, Antonia. "Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores". Revista española de protección de datos de la Agencia de Protección de Datos de la Comunidad de Madrid, Nº 6 Enero – Junio 2009. Página 47.

En primer lugar, no debemos olvidar que es necesario el consentimiento del usuario para que se puedan utilizar los datos personales. Las redes sociales tratan de obtenerlo con la aceptación de las condiciones generales, lo cual es un tema dudoso. Pero, además, Facebook declara que: "... almacenamos cierta información de tu navegador usando cookies... Podemos utilizar información sobre ti que recopilemos en otras fuentes incluyendo, entre otras, periódicos y fuentes de Internet como blogs, servicios de mensajería instantánea, la plataforma de desarrolladores de Facebook y otros usuarios de Facebook, para complementar tu perfil". La principal cuestión que nos atañe es la utilización de cookies, sin olvidarnos de la vía de obtención del consentimiento y la recopilación de datos obtenidas de otras fuentes[7].

El Grupo de Trabajo del Artículo 29 en el Dictamen 1/2009 entiende que la configuración predeterminada del navegador, con carácter general, no puede entenderse como autorización previa para la obtención de datos personales. Por otra parte, la AEPD ha manifestado que Internet no es una fuente accesible al público, por lo tanto será necesario obtener el consentimiento e informar previamente sobre la finalidad del tratamiento.

3. Aspectos normativos de la Unión Europea

Entiendo importante destacar el esfuerzo realizado por la Unión Europea frente al desafío que presentan las cookies, a través de la regulación realizada por la Directiva 2009/136/CE de 25 de noviembre de 2009, así como los interesantes análisis realizados por el Grupo de Trabajo del artículo 29, que vierten luz sobre la temática.

3.1. Directiva 2009/136/CE de 25 de noviembre de 2009

Por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) N° 2006/2004 sobre la cooperación en materia de protección de los consumidores

La Directiva 95/46/CE relativa a la protección de las personas físicas relativo al tratamiento de los datos personales y a la libre circulación de éstos, se aplica en los asuntos no cubiertos específicamente por la Directiva modificada.

El artículo 5 apartado 3 exige el consentimiento autorizado del abonado o usuario para almacenar información legalmente u obtener acceso a información almacenada en su equipo terminal.

Se establece en el Considerando 66 de la Directiva que: "Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a la información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espías o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y compleja cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más sencillo posible para el usuario. Las excepciones a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario. Cuando sea técnicamente posible y eficaz, de conformidad

7 Viega, María José. "Marketing comportamental en línea. El desafío de las cookies". Libro electrónico publicado en http://mjv.viegasociados.com/?page_id=205

con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación. La aplicación de estos requisitos debe ganar en eficacia gracias a las competencias reforzadas concedidas a las autoridades nacionales".

Por lo tanto, todo almacenamiento de cookies o cualquier otro sistema similar y la utilización posterior de cookies que hayan sido previamente almacenados para tener acceso a información de los usuarios debe cumplir con el artículo 5 apartado 3. Este artículo es neutro tecnológicamente por lo que aplica a cualquier tecnología utilizada para almacenar o acceder a información almacenada en el equipo de los usuarios.

Por otra parte, no tipifica la información, por lo que no requiere que sean datos personales, sino que posee mayor amplitud, ya que refiere a la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

El Grupo de Trabajo del Artículo 29 en su Dictamen 1/2008 de 4 de abril de 2008 sobre cuestiones relacionadas con motores de búsqueda determina que, en la mayoría de los casos, las cookies y las direcciones IP deben ser considerados datos personales.

3.2. Dictamen 2/2010 del Grupo de Trabajo del Artículo 29 de 22 de junio de 2010 sobre Publicidad Comportamental

El Dictamen analiza cuales son las funciones y las responsabilidades de los distintos actores involucrados en la publicidad comportamental y determina:

- En relación a los Proveedores de redes de publicidad: en publicidad comportamental la obligación de obtener el consentimiento informado corresponde a los proveedores de redes de publicidad. Por otra parte, estos proveedores desempeñan el papel de responsables de tratamiento de datos, ya que tienen un control completo de los objetivos y medios del tratamiento de datos.
- En relación a los Editores: ceden espacio en alquiler en sus sitios a las redes de publicidad para colocar anuncios y configuran sus sitios de modo que los buscadores de los visitantes sean redireccionados automáticamente a la página del proveedor de redes de publicidad, que le enviará la cookie y publicidad a medida.

El Grupo de Trabajo del Artículo 29 entiende que los editores tienen cierta responsabilidad en el tratamiento de datos porque con la configuración del sitio desencadenan la transferencia de la dirección IP. Pero como éstos no retienen información personal, no tiene sentido aplicarles disposiciones como por ejemplo el derecho de acceso. Pero no cabe dudas que tienen la obligación de informar a las personas sobre el tratamiento de datos.

Junto con los proveedores de redes de publicidad, los editores "deben garantizar que la complejidad y las características técnicas del sistema de publicidad orientada por el comportamiento no les impidan encontrar las vías adecuadas para cumplir con las obligaciones que incumben a los responsables del tratamiento y salvaguardar los derechos de los interesados"[8].

Los acuerdos de servicios entre editores y proveedores de redes de publicidad deben establecer las funciones y responsabilidades de ambas partes de acuerdo con el tipo de colaboración que se describa en los mismos.

8 Grupo de trabajo del Artículo 29. Dictamen 1/2010 de 16 de febrero de 2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento".

Tenemos básicamente dos tipos de cookies. Son las cookies que se necesitan para proporcionar el servicio solicitado específicamente por el usuario. Podemos ver ejemplos de esto: su carro de la compra puede estar en una "cookie" cuando usted está comprando cosas en un sitio web en Internet, puede ser una cookie de sesión, cuando se conecta a su banco, una cookie a veces de preferencia. Para este tipo de cookies que no tienen una pregunta de opt in o opt out o consentimiento en la mayoría de los casos.

Los otros tipos de cookies como OBA, pero no sólo, como los otros tipos de cookies tienen un régimen específico. Básicamente dice que el almacenamiento o acceso a las cookies en el equipo terminal sólo está permitido a condición de que el abonado o usuario haya dado su consentimiento por haber recibido información clara y comprensible. Así que, cuando usted rompe esto, el primer paso es la información, el segundo paso es el consentimiento y el almacenamiento o no almacenamiento de la información en el terminal del usuario requiere consentimiento previo.

3.2.1 Obligación de obtener el consentimiento previo de los usuarios

El artículo 5 apartado 3 establece que un proveedor de redes de publicidad que desee almacenar información o tener acceso a información almacenada en el equipo terminal del usuario, puede hacerlo si:

- Ha proporcionado al usuario información clara y completa con arreglo a la Directiva 95/46/CE, especialmente sobre el objetivo del tratamiento de los datos;
- Ha obtenido el consentimiento del usuario para el almacenamiento o el acceso a la información en su equipo terminal, tras haberle proporcionado la información mencionada en el punto anterior.

Por tanto, el consentimiento debe ser previo e informado y por supuesto debe ser revocable. Con relación al punto de si la configuración del buscador implica consentimiento, ya que se proporciona información en los términos y condiciones generales o usos de privacidad en relación a cookies de terceros utilizados para publicidad comportamental. Pero el Grupo de Trabajo del Artículo 29 entiende que esta práctica no cumple con el artículo 5 apartado 3, especialmente en la versión modificada, que hace hincapié en proporcionar información previa y obtener el previo consentimiento.

Se fundamenta en que el Considerando 66 de la Directiva 2002/58/CE señala que el consentimiento del usuario puede expresarse utilizando la configuración adecuada de un buscador u otras aplicaciones **"cuando sea técnicamente posible y eficaz, con arreglo a las disposiciones correspondientes de la Directiva 95/46/CE".**

De acuerdo al Dictamen 2/2010 para que los buscadores u otras aplicaciones puedan ser indicativos de consentimiento válido deben:

- Por defecto, rechazar cookies de terceros y requerir que el usuario realice una acción expresa para aceptar la configuración de una transmisión continuada de información contenida en los cookies por sitios web específicos.
- Los buscadores, juntos o en combinación con otras herramientas de información, deben transmitir información clara, completa y perfectamente visible para garantizar que el consentimiento esté plenamente fundamentado. Las advertencias genéricas, sin referencia explícita a la red de publicidad que está instalando el cookie, no son suficientes.

Los proveedores de redes de publicidad ofrecen sistemas de exclusión voluntaria que permitan a los usuarios optar por no recibir publicidad a medida. Tales sistemas no son adecuados para obtener el consentimiento de un usuario corriente, si bien son positivos en la medida que facilitan la exclusión voluntaria.

Ya la Recomendación 1/1999 sobre tratamiento invisible y automático de datos personales en Internet establecía: "En el caso de cookies, debería informarse al usuario cuándo está previsto que el software de internet reciba, almacene o envíe un cookie. El mensaje debería especificar, en un lenguaje normalmente comprensible, qué información se pretende almacenar en el cookie y con qué objetivo así como el período de validez del cookie".

Cuando el considerando 25 de la Directiva 2002/58/CE dice que: **"el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión... en conexiones posteriores"**, puede entenderse que si la persona acepta una cookie no solo acepta el envío sino también la ulterior recogida de datos.

En este sentido el Grupo de Trabajo del Artículo 29 entiende que la aceptación no puede ser de una vez y para siempre y propone tres líneas de acción: 1. limitar el alcance del consentimiento en el tiempo, 2. se debe dar información complementaria y 3. el consentimiento dado siempre puede revocarse.

Respecto al consentimiento de los niños, el Grupo de Trabajo del Artículo 29 estima que los proveedores de redes de publicidad no deben ofrecer grupos de interés dirigidos a enviar publicidad comportamental a los niños o influir en ellos.

Es relevante tener en cuenta en este punto la Opinión 15/2011 del Grupo de Trabajo del Artículo 29 de 13 de julio de 2011 sobre la definición de consentimiento.

El dictamen hace un análisis exhaustivo del concepto de consentimiento como se utilizan actualmente en la Directiva de Protección de Datos y en la Directiva sobre la privacidad. Basándose en la experiencia de los miembros del Grupo de Trabajo del artículo 29, el dictamen ofrece numerosas ejemplos de un consentimiento válido y no válido, centrándose en sus elementos clave, tales como el significado de "indicación", "libremente", "específico", "sin ambigüedades", "explícito", "informada", etc. El dictamen, además, aclara algunos aspectos relacionados con la noción de consentimiento. Por ejemplo, el momento de cuándo debe obtener el consentimiento, como el derecho a oponerse difiere de consentimiento, etc.

El dictamen se emitió en parte en respuesta a una petición de la Comisión en el contexto de la actual revisión de la Directiva de Protección de Datos. Por lo tanto, contiene recomendaciones para su consideración en la revisión. Esas recomendaciones incluyen:

- Aclarar el significado de "sin ambigüedades" el consentimiento y explicar que el consentimiento sólo que se basa en las declaraciones o acciones para expresar acuerdo constituye un consentimiento válido;
- Tratamiento de los datos que requieren para poner en marcha mecanismos para demostrar el consentimiento;
- La adición de un requisito explícito en relación con la calidad y accesibilidad de la información que constituye la base para el consentimiento, y
- Una serie de sugerencias con respecto a los menores y demás incapaces.

Un enfoque similar al adoptado en virtud del artículo 9 sobre el tratamiento de datos de localización aparte de los datos de tráfico. El proveedor del servicio deberá informar a los usuarios o abonados - antes de la obtener su consentimiento el tipo de datos de localización aparte de los datos de tráfico que serán procesados. El artículo 13 establece el requisito de obtener el consentimiento previo de los usuarios pudiendo utilizar los sistemas automáticos de llamada sin intervención humana, fax o email con fines de venta directa.
Respecto al artículo 13 (2-3), derecho de oposición y su distinción de consentimiento se establece que: "**...los clientes de manera clara y muy clara se les da la oportunidad de oponerse...".**

En cuanto a la utilización de aparatos de llamada automática, máquinas de fax y correo electrónico,

se requiere el consentimiento previo del interesado.

Si el destinatario de la comunicación comercial es un cliente existente y la comunicación tiene como objetivo la promoción de productos similares o propios del proveedor o servicios, el requisito no es el consentimiento, sino asegurar que a las personas "se les da la oportunidad de objetar" ex artículo 13 (2).

La necesidad del consentimiento debe ser distinguido de este derecho de oposición. El consentimiento basado en la falta de acción de los individuos, por ejemplo, a través de los casilleros ya marcados, no cumple con los requisitos de consentimiento válido en virtud de la Directiva 95/46/CE.

La misma conclusión se aplica a la configuración del navegador que acepta por defecto, la orientación de los usuarios (a través del uso de cookies). Esto es claro en la nueva redacción del artículo 5 (3).

Estos dos ejemplos no cumplen, en particular, los requisitos para una indicación inequívoca de deseos. Es indispensable que al interesado se le dé la oportunidad de tomar una decisión y para expresarlo, por ejemplo, marcando la casilla de sí mismo, teniendo en cuenta el propósito del procesamiento de datos.

En su dictamen sobre la publicidad comportamental el Grupo de Trabajo ha concluido que "parece de suma importancia que a los navegadores se los provea de configuración de protección de privacidad. En otras palabras, de ser provistos de la configuración de "la no aceptación y no la transmisión de cookies de terceros". Como complemento de esto y para que sea más eficaz, los navegadores deberían exigir a los usuarios que atraviesen un asistente de privacidad cuando ellos instalan o actualizan el navegador por primera vez y proporcionar una manera fácil de ejercitar la elección durante el uso".

3.2.2 Obligación de información

En la publicidad comportamental los usuarios deben recibir información de la identidad del proveedor de la red de publicidad, del objetivo del tratamiento de sus datos, debe conocer que el cookie permitirá al proveedor conocer sus visitas a los diferentes sitios web, los anuncios en que en ha cliqueado, el tiempo que ha permanecido, etc.

El Considerando 25 de la Directiva 2002/58/CE establece que la información debe ser clara y precisa y estar tan asequible para el usuario como sea posible.

Quien tiene la obligación de proporcionar la información es quien envía y lee la cookie. Pero ya habíamos mencionado que los editores tienen la obligación de informar a los usuarios sobre el tratamiento de sus datos al redireccionar su buscador. El Grupo de Trabajo del Artículo 29 no sugiere que se envíe información dos veces, sino que considera que en este campo hay una necesidad clara de cooperación entre los proveedores de publicidad y editores para decidir quién proporciona la información y como debe hacerlo.

3.2.3 Otras obligaciones y principios derivados de la Directiva 95/46/CE

Cualquier categorización posible de los usuarios basada en datos sensibles implica que puedan cometerse abusos, por tanto los proveedores de redes de publicidad que ofrecen y utilicen categorías de interés que revelen información sensible, deben cumplir con el artículo 8 de la Directiva 95/46/CE.

Este artículo prohíbe el tratamiento de datos sensibles excepto en determinadas circunstancias específicas, que en este caso la única base jurídica para legitimar el tratamiento sería un consentimiento explícito y específico. Por tanto dicho consentimiento no puede obtenerse configurando el buscador.

El Grupo de Trabajo del Artículo 29 es consciente de que los perfiles reunidos y utilizados en publicidad comportamental podrían utilizarse para objetivos distintos de la publicidad, como por ejemplo para desarrollar nuevos servicios de índole aún no definida. Pero esto está condicionado al cumplimiento del artículo 6 apartado 1 letra b) que establece el principio de limitación de objetivos, que prohíbe el tratamiento de datos personales que no sean compatibles con los fines que hicieron legítima la recogida de datos inicial. Por tanto, la segunda utilización de información recogida y almacenada con fines de publicidad comportamental iría en contra del artículo 6 letra b) de la Directiva 95/46/CE.

Dice el Dictamen 2/2010 que: "Si los proveedores de redes de publicidad desean utilizar la información reunida con fines de publicidad comportamental para fines segundos e incompatibles, por ejemplo en otros servicios, necesitan una nueva base de datos jurídica para ello con arreglo al artículo 7 de la Directiva 95/46/CE. Por ello, deberán informar a los usuarios y, en la mayoría de los casos, obtener su consentimiento con arreglo al artículo 7 letra a)".

Pero además, el artículo 6 apartado 1 letra e) dispone la eliminación de los datos cuando dejen de ser necesarios para los fines recogidos, es el principio de conservación de los datos. Por lo cual, la información sobre el comportamiento de los usuarios debe eliminarse si ya no es precisa para desarrollar un perfil. Y establece el dictamen que: "Todo responsable de tratamiento de datos debe poder justificar la necesidad de un período de conservación determinado".

También deben cumplirse los derechos de acceso, rectificación, eliminación y oposición. El Grupo de Trabajo del Artículo 29 conoce iniciativas de proveedores de redes de publicidad por las que se ofrece acceso a categorías de interés con las que se etiqueta a las personas en base al número ID del cookie, para que las personas puedan modificarlas o eliminarlas.

Los proveedores de redes de publicidad también deben garantizar el cumplimiento de las disposiciones de transferencias de datos personales a países terceros, por ejemplo cuando los servidores están situados fuera de la Unión Europea.

Mullock[9] considera que existen otras áreas a considerar, vemos varias capas de protección de datos, antes de entrar en las "cookies" propiamente dichas, como es la problemática de las direcciones IP, el conocimiento y consentimiento y toda la cuestión referente al opt in y opt out. Los casos que han pasado por los tribunales aquí en este momento tienden a su vez en sus hechos que ha habido un caso reciente en Suiza que se encuentra que las direcciones IP son datos personales. Pero, si las direcciones IP son datos personales, entonces usted realmente necesidad ver el estilo de la OBA que está teniendo lugar y los detalles de la operación especial de entender si se podría aplicar la ley de privacidad para su funcionamiento en virtud de los datos personales tratados.

El segundo punto es la piedra angular de la Directiva sobre protección de datos, es el concepto de conocimiento y consentimiento, y, en particular, el concepto de consentimiento libre e informado plenamente. Así que la idea de que opt in opt out en relación a las cookies es el final de la historia, sería muy miope.

El tercer punto refiere a toda la cuestión de opt in opt out que no es aplicable sólo a las cookies. Como parte de la directiva PEC es muy aplicable en relación con otras formas de comercialización o el canal de comercialización. Es muy importante para, por ejemplo, el uso de los datos de tráfico y de localización.

9 Pannetrat, Allan. IAPP Web Conference - October 7, 2010. The Article 29 Working Party Opinion on Behavioral Advertising: Interpretations and Consequences.

3.3. Dictamen 4/2012 del Grupo de Trabajo del Artículo 29 de 7 de junio de 2012 sobre la exención del requisito de consentimiento en la cookies

El dictamen explica cómo el artículo 5, apartado 3, repercute en el uso de los **cookies**, entendiendo que este término no excluye otras tecnologías similares. El artículo 5, apartado 3, permite que los **cookies** queden exentos del requisito de consentimiento informado si cumplen alguno de los siguientes criterios:

Criterio A: la **cookie** se utiliza «al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas».

Criterio B: la **cookie** es «estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario».

El Dictamen 4/2012 analiza las exenciones a este principio, en el contexto de las **cookies** y las tecnologías conexas.

Como hemos analizado en el punto 4.1 el Artículo 5.3 de la Directiva 2002/58/CE, modificado por la Directiva 2009/136/CE, establecía el requisito del Consentimiento Informado, antes de que los datos fueran tratados en el equipo del usuario. En virtud de ese artículo, se establecía la exención del consentimiento informado al cumplirse alguno de estos dos criterios:

- Cuando la cookie sea utilizada con el único propósito de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas.
- Cuando la cookie resulte estrictamente necesaria para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

El reciente Dictamen 04/2012 de 7 de junio del presente analiza estos dos requisitos a los efectos de determinar si una cookie está exenta o no del consentimiento informado, aclarando que el análisis se lleva a cabo sin perjuicio del derecho a ser informado y el derecho a oponerse establecido por la Directiva 95/46/CE, que se aplican a tratamiento de datos personales con carácter general.

En el Criterio A deben considerarse al menos tres elementos como estrictamente necesarios para que exista una red de comunicaciones entre dos
partes:

- La capacidad para dirigir la información a través de la red, en particular mediante la identificación de los extremos de la comunicación.
- La capacidad de intercambiar los elementos de los datos en el orden previsto, en particular mediante la numeración de los paquetes de datos.
- La capacidad de detectar errores de transmisión o pérdida de datos.

Con relación al Criterio B tiene que pasar las dos siguientes pruebas:

- El servicio de la sociedad de la información ha sido expresamente solicitado
- por el usuario: el usuario (o suscriptor) hizo una acción positiva para solicitar un servicio con un perímetro claramente definido.
- La cookie es estrictamente necesaria para habilitar el servicio de sociedad de la información: si las cookies están deshabilitadas el servicio no funcionará.

El dictamen retoma la clasificación de las cookies en: cookies de sesión o cookies persistentes, de primeras o terceras partes. Luego del análisis de las características de una cookie y de los diferentes escenarios posibles, concluye que las siguientes cookies pueden estar exentas de la obligación del consentimiento informado, bajo determinadas condiciones y siempre que no sean utilizadas para otros fines.

1. "User input cookies" (*cookies* de sesión utilizadas típicamente cuando el usuario ingresa a un sitio), son temporales y se eliminan al finalizar la sesión. Estas cookies son necesarias para prestar un servicio en Internet y además el usuario solicita el servicio y realiza una acción, como hacer clic en un botón o completar un formulario.

2. Cookies de autenticación: se utilizan para la autenticación del usuario en un sitio web, para ver información de su cuenta, saldo o transacciones. Funcionan únicamente mientras dura la sesión y puede aplicárseles el criterio B, el cual no se aplica cuando se trate de cookies persistentes.

3. Cookies de seguridad, utilizadas para prevenir abusos en la autenticación, como por ejemplo, detectar repetidos intentos fallidos de validación, siempre que tengan una duración limitada y no se refiera a servicios no solicitados por el usuario.

4. Cookies de sesión de contenido multimedia, contienen datos técnicos de la sesión para reproducir video o audio, son conocidas como "flash cookies", usadas por ejemplo Adobe Flash y expiran cuando finaliza la sesión.

5. Cookies de sesión de balanceo de carga, mientras dure la sesión. El balanceo de carga es una técnica que permite la distribución de la tramitación de las solicitudes del servidor web sobre un conjunto de máquinas a los efectos de optimizar el rendimiento. Esto puede realizarse con una cookie de sesión, que está exceptuada por el criterio A.

6. *Cookies* para la personalización de la interface - *"UI customization cookies".* Se utilizan por ejemplo para seleccionar el idioma del usuario, para recordar sus búsquedas, son de duración determinada y no pueden estar enlazadas con cookies persistentes como el nombre de usuario. Están exoneradas en base al criterio B.

7. Cookies de plug-in para compartir contenidos en redes sociales - "*Social plug-in content shared cookies*" identifican a los miembros de una determinada red social, siempre y cuando el usuario no haya realizado un "*log-out*" de la red social. Muchas de las redes sociales proponen "plug-in de módulos sociales" que los operadores de sitios web pueden integrar en su plataforma, en particular para permitir a los usuarios de redes sociales compartir contenidos que les gustan con su "Amigos" y proponer otras funcionalidades relacionadas como la publicación de comentarios. Entiende el Grupo de Trabajo del Artículo 29 que las redes sociales que desean utilizar cookies con fines adicionales (o una vida útil más larga), más allá del criterio B tienen que informar y obtener el consentimiento.

El primer aspecto importante a tener en cuenta es la finalidad de la instalación de la cookie para determinar si está exenta o no del consentimiento y siempre se necesitará éste cuando se trate de cookies de terceros. El segundo aspecto consiste en analizar que es estrictamente necesario desde el punto de vista del usuario, nunca del proveedor de servicios.

También se analizan en el Dictamen los casos de cookies que no están exceptuadas de obtener el consentimiento y son los siguientes:

1. "Social plug-in tracking cookies". Como se describió anteriormente muchas de las redes sociales proponen "plug-in de módulos sociales" que en el sitio web los propietarios pueden integrar en su plataforma, para ofrecer algunos servicios que pueden ser considerados como "Solicitado

expresamente" por sus miembros. Sin embargo, estos módulos también se puede utilizar para rastrear personas, tanto miembros como no miembros, como las cookies de terceros utilizadas para otros fines como por ejemplo la publicidad de comportamiento, análisis o estudios de mercado. Con esos fines, estas cookies no pueden ser consideradas "estrictamente necesarias" para proporcionar una
funcionalidad expresamente solicitado por el usuario, por tanto no es posible aplicar el criterio B.

2. "Third party advertising". Las cookies de terceros utilizadas para la publicidad de comportamiento no están exentas de consentimiento como ya fue señalado en detalle por el Grupo de Trabajo en el Dictamen 2/2010 y en el Dictamen 16/2011. El requisito del consentimiento se extiende a todas las cookies de terceros relacionadas con el funcionamiento utilizado en la publicidad, incluyendo cookies utilizadas con el propósito de limitación de frecuencia, detección de fraudes, investigación y análisis de mercado, mejora y depuración del producto, ya que ninguno de estos fines se puede considerar que estar relacionado con un servicio o funcionalidad de un servicio de la sociedad de la información expresamente solicitado por el usuario, como requerido por el criterio B.

El Grupo de Trabajo ha participado activamente desde el 22 diciembre de 2011 en la labor de la World Wide Web Consortium (W3C) para estandarizar la tecnología y el significado del no rastreo. En vista del hecho de que las cookies a menudo contienen identificadores únicos, que permiten el seguimiento del comportamiento del usuario a través del tiempo y a través de sitios web y la posible combinación de estos identificadores con otros datos de identificación, el Grupo de Trabajo está preocupado por la posible exclusión del no rastreo de determinadas cookies que se dice que son necesarios para fines operativos.

3. "First party analytics". Google Analytics es una herramienta de medición de estadística de audiencia de sitios web, que a menudo se basa en cookies. Estas herramientas son especialmente utilizadas por los propietarios de sitios web para estimar el número de visitantes únicos, para detectar las palabras clave de búsqueda más utilizadas del buscador que llevan a una página web o para localizar los temas de navegación web.

El Dictamen finaliza estableciendo las pautas principales y concluye: "En última
instancia, para decidir si una cookie está exenta del principio del consentimiento informado es importante verificar cuidadosamente si se cumple uno de los dos criterios de exención definidos en el artículo 5.3 de la Directiva 2009/136/CE. Después de un cuidadoso examen, si las dudas siguen existiendo respecto a si se aplica o no un criterio de excepción, los operadores de sitios web deberían examinar detenidamente si no existe en la práctica, la oportunidad de obtener el consentimiento de los usuarios de una manera discreta, sencilla, evitando así la inseguridad jurídica".

4. Estados Unidos

El FTC reconoce los beneficios del marketing comportamental, ya que varios consumidores prefieren información relevante sobre sus intereses particulares. En virtud de ello es importante recabar el libre consentimiento. Asimismo, se toman precauciones sobre cómo recabar ese consentimiento en tanto parte de un marco más amplio que el FTC está desarrollando. En diciembre de 2010, se lanzó un reporte inicial sobre privacidad y buenas prácticas. El marco tiene tres principios: Privacidad desde el diseño (privacy by design), proporcionar opciones claras y transparentes para que el consumidor elija y aumentar la transparencia[10].

10 Ramírez, Edith. Marketing Comportamental en línea. http://privacyconference2012.org/wps/wcm/connect/c376b5004e43e1c88f43ffc08ba-c212e/Panel_G_Marketing_comportamental_en_linea.pdf?MOD=AJPERES (Página visitada el 28 de agosto de 2013).

Los siete principios que establece el FTC son[11]:

- **1.** Transparencia respecto a la recolección y uso de datos, proveyendo a los consumidores avisos claros mediante múltiples mecanismos.
- **2.** Elección del usuario, el consumidor tiene el control sobre el marketing comportamental.
- **3.** Seguridad de los datos apropiada
- **4.** Limitación en la creación de segmentos de interés especialmente en niños y en la recolección de datos sensibles.
- **5.** Educación a los consumidores sobre el marketing comportamental en línea y sobre el marco regulatorio.
- **6.** Conformidad y aplicación, lograr mecanismos que aseguren el efectivo cumplimiento.
- **7.** Revisión regular del marco para asegurarse que comprenda tecnologías y técnicas de negocios.

La noticia del día de hoy es que Facebook debe pagar 20 millones de dólares por el uso de datos para publicidad: "El juez de distrito de San Francisco Richard Seeborg consideró que la suma, una pequeña parte de los miles de millones que se reclamaban por este caso, era justa dados los desafíos de probar que los miembros de Facebook resultaron perjudicados económicamente o que la señalización 'Me gusta' para los productos no implicaba ningún tipo de consentimiento. (...) El acuerdo también establece que Facebook modifique sus reglas y dé más control a los usuarios sobre el uso potencial de sus datos en el contexto de la publicidad. La demanda fue presentada a principios de 2011 después de que Facebook lanzara su programa de publicidad 'Historias patrocinadas'[12].

5. Conclusiones

Como hemos mencionado en otras oportunidades este es un tema que tiene importantes connotaciones económicas para las empresas que realizan publicidad en la web, pero que un uso incorrecto de la tecnología afecta a las personas en su derecho humano a la privacidad. La normativa jurídica al respecto es muy importante a la hora de proteger nuestros derechos, pero también es muy importante utilizar herramientas tecnológicas adecuadas para evitar la captura de nuestros datos cuando no hemos dado el consentimiento para ello.

Una de las herramientas tecnológicas para prevenir el seguimiento on line es el "do no track", que es un mecanismo que permite al usuario deshabilitar las tecnologías de rastreo. Este mecanismo debe cumplir con los siguientes requisitos críticos: debe ser universal; que se encuentre centralizado; fácil de encontrar y usar; durable, si se elige una vez no hay que estar eligiéndolo constantemente; efectivo, comprehensivo y debe permitir optar por el no rastreo y la no recolección de datos.

11 Winton, Ashley. Marketing Comportamental en línea. http://privacyconference2012.org/wps/wcm/connect/c376b5004e43e1c88f43ffc08ba-c212e/Panel_G_Marketing_comportamental_en_linea.pdf?MOD=AJPERES (Página visitada el 28 de agosto de 2013).

12 http://informe21.com/ciencia-y-tecnologia/facebook-debe-pagar-20-millones-de-dolares-por-el-uso-de-datos-para-publicidad. Noticia del día 28 de agosto de 2013, visitada la página el mismo día.

CAPITULO XII
PIRATERÍA Y PRIVACIDAD

Dra. Jimena Hernández

PIRATERÍA Y PRIVACIDAD

Dra. Jimena Hernández

1. Introducción

La Stop Online Piracy Act, conocida como Ley SOPA, es un proyecto de ley nacido en Estados Unidos, pensado para detener la piratería en línea. Frente a la sospecha de utilización sin autorización de material sujeto a derechos de autor, esta norma habilita a la justicia a revisar, perseguir y desconectar a cualquier sospechoso.

Su principal objetivo es la protección de los contenidos que circulan en la web y se encuentran protegidos por derechos de autor, buscando ser un instrumento de fortalecimiento de las normas ya existentes en la materia.

El problema que presenta es que su esquema de funcionamiento, puede implicar una amenaza a derechos fundamentales tales como la protección de datos personales y la libertad de expresión.

Varias voces se han levantado a favor y en contra de este proyecto, y de ahí el interés que presenta su estudio y el análisis de los diversos efectos que generaría su aplicación dentro y fuera de fronteras.

2. Derechos de autor y piratería

2.1. Introducción a los Derechos de autor

Los derechos de autor y derechos conexos son ampliamente reconocidos como tales en varios instrumentos internacionales y nacionales.

Su protección se fundamenta en que se trata de derechos esenciales para la creatividad humana ya que ofrecen a los creadores determinados incentivos bajo formas de reconocimiento y recompensas económicas equitativas. Este sistema de derechos busca que los creadores cuenten con la garantía de que sus obras serán divulgadas sin tener que preocuparse de las copias no autorizadas o la piratería.

En lo que respecta a los derechos conexos, la OMPI destaca que en los últimos 50 años, se ha expandido rápidamente el ámbito de los derechos conexos al derecho de autor. Estos derechos conexos han ido desarrollándose en torno a las obras protegidas por el derecho de autor y conceden derechos similares, aunque a menudo más limitados y de más corta duración, a: los artistas intérpretes o ejecutantes (tales como los actores y los músicos) respecto de sus interpretaciones o ejecuciones; los productores de grabaciones sonoras (por ejemplo, las grabaciones en casetes y discos compactos) respecto de sus grabaciones; los organismos de radiodifusión respecto de sus programas de radio y de televisión.

Como punto de partida en cuanto a su reconocimiento y regulación, cabe mencionar la Declaración Universal de Derechos Humanos, en la cual los derechos de autor se encuentran contenidos en el numeral 2° del artículo 27 de 18 de Diciembre de 1948, indicándose que: “Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora”.

Debemos mencionar además, el papel que ha jugado en cuanto al reconocimiento y difusión de los Derechos de Autor y Derechos conexos, la OMPI (Organización Mundial de la Propiedad Intelectual) creada en 1967, contando actualmente con 185 Estados miembros dentro de los cuales se encuentra nuestro país.1 La OMPI es el organismo especializado del sistema de organizaciones de las Naciones Unidas dedicado al uso de la propiedad intelectual, patentes, derecho de autor, marcas, diseños, entre otros. Los Estados miembros de la OMPI determinan la orientación estratégica y las actividades de la Organización para lo cual, se reúnen en asambleas, comités y otros órganos decisorios.

De especial relevancia resultan en cuanto a la protección de programas de ordenador, el Convenio de Berna para la Protección de las Obras Literarias y Artísticas (Acta de París de 1971), el Acuerdo sobre los Aspectos de Propiedad Intelectual vinculados al Comercio (ADPIC), y los nuevos Tratados de la OMPI sobre Derecho de Autor del año 1996 (ámbito digital e internet). El Convenio de Berna y el acuerdo ADPIC fueron aprobados en nuestro país por las Leyes N° 14.910 y N° 16.671 respectivamente.

En nuestro ordenamiento jurídico debemos mencionar lo consagrado por el artículo 33 de la Constitución de la República Oriental del Uruguay que especifica la protección de "el trabajo intelectual, el derecho del autor, del inventor o del artista, serán reconocidos y protegidos por la ley".

El derecho de autor se encuentra regulado por las Leyes Nº 9.739, de 17 de diciembre de 1937 y Nº 17.616, de 10 de enero de 2003 y por el Decreto Nº 154/004, del 3 de mayo de 2004, entre otras disposiciones.

De acuerdo a lo regulado por las leyes mencionadas, podemos decir que la protección de los derechos de autor implica la protección del derecho moral de éstos sobre sus creaciones literarias, científicas o artísticas, y el reconocimiento del derecho de dominio sobre las producciones de su pensamiento, ciencia o arte. Es importante destacar que cuando nos referimos a creaciones del autor se incluyen por ejemplo las obras literarias, obras de teatro, bases de datos, películas, composiciones musicales, obras artísticas, obras arquitectónicas, pinturas, esculturas, publicidad, folletos, fotografías, programas de ordenador, entre otros.

Los derechos concedidos a los autores implican la posibilidad de prohibir o autorizar la reproducción bajo distintas formas, la ejecución o interpretación, por ejemplo en el caso de una obra teatral, las grabaciones de la misma, como por ejemplo discos, la radiodifusión por cualquier medio, la traducción a otros idiomas. También son quienes pueden vender los derechos de sus obras.

Es importante señalar que la Ley prevé que los derechos de autor puedan inscribirse en el registro que lleva a sus efectos la Biblioteca Nacional, teniendo en cuenta que se trata de una inscripción de carácter facultativa y que su no realización no afecta el goce y el ejercicio de los derechos de autor.

La vigilancia y contralor de la aplicación de la Ley está a cargo de un Consejo de Derechos de Autor, integrado por cinco miembros, que duran cinco años en sus funciones y que son designados por el Ministerio de Educación y Cultura. El Consejo de Derechos de Autor ejerce la supervisión y el contralor del registro y le compete resolver las controversias que se susciten con motivo de las inscripciones.

En importante mencionar dentro del conjunto normativo que regula a los derechos de autor, el Decreto N° 154/989, de 11 de abril de 1989 por el cual se regula la inscripción del software en el Registro de Derechos de Autor. Se definen a los programas de ordenador como inscribibles ante el registro mencionado por entenderse como una producción intelectual protegida por la Ley N° 9.739. Se prevé que puedan depositarse en forma completa o por trechos suficientes para caracterizar la creación del programa. Se dispone además que las informaciones que fundamenten el registro de programas de ordenador tendrán carácter secreto, pudiendo, mediando examen del Consejo de

1 Datos obtenidos de http://www.wipo.int/about-wipo/es/. (Página visitada el 3 de agosto de 2012).

Derechos de Autor, levantarse a requerimiento del propio autor o por orden judicial.

2.2. Infracciones al Derecho de autor

Las infracciones a los derechos de autor ocurren cuando una obra protegida es utilizada (reproducida, traducida, adoptada, exhibida o interpretada en público, distribuida, emitida, o comunicada en público) sin el permiso de los titulares de los derechos y dicho uso no está cubierto por ninguno de los límites del derecho de autor.

El plagio implica copiar una obra entera o parcialmente, pretendiendo ser el autor, en cambio el término piratería se refiere a la venta ilegal e intencionada de obras protegidas por el derecho de autor.

En palabras del Dr. Delpiazzo[2], y de acuerdo al Glosario de Derechos de Autor y Derechos Conexos de la OMPI, se define a la piratería de modo genérico como la reproducción de obras por cualquier medio adecuado, con miras de transmisión. Indica que dicha definición no está pensada expresamente para los productos informáticos. Debemos manejar un concepto amplio de piratería para comprender también la copia no autorizada para uso propio. La expresión piratería, y su identificación con una reproducción no autorizada, se encuentran ligadas a la presencia de un comportamiento ilícito.

2.3. Regulación nacional

La rapidez de los avances tecnológicos y la necesidad de ampliar la protección de los derechos de autor para adaptarse a éstos, hizo inminente la necesidad de reformar la normativa existente en nuestro país. De acuerdo a ello, se sanciona la Ley N° 17.616, de 10 de enero de 2003.

Esta nueva regulación introduce expresamente[3] la protección de los programas de ordenador, sean programas fuente o programas objeto. De acuerdo a lo mencionado por el Dr. Carlos E. Delpiazzo[4] además de los programas de ordenador, contempla expresamente a las compilaciones de datos y a las informaciones y algoritmos formulados en secuencias originales ordenadas en forma apropiada para ser usada por un dispositivo de procesamiento de información o de control automático. Destaca además que la normativa contempla la figura del productor de creaciones informáticas sobre quien se consideran cedidos los derechos patrimoniales sobre éstas y quienes tienen la autorización para decidir sobre su divulgación y ejercer los derechos morales sobre ellas. De acuerdo a ello, tiene el derecho de autorizar la reproducción, distribución, transformación y comunicación.

En lo que refiere a la protección de los derechos, la ley señala que los titulares podrán solicitar inspecciones judiciales con el objeto de constatar los hechos que comprueben infracciones a ésta. Además de ello, el Juez podrá ordenar las medidas cautelares necesarias para evitar que se cometa la infracción o que se continúe o repita una violación ya realizada.

La ley prevé la posibilidad de que el lesionado (sea el autor o causahabiente) inicie las acciones civiles necesarias para que le sean reparados los daños y perjuicios generados, y además, pueda solicitar acumulativamente una multa de hasta diez veces el valor del producto en infracción. El infractor deberá abonar los daños y perjuicios generados y la multa de hasta diez veces el valor del programa.
También se han introducido algunas modificaciones respecto a los delitos vinculados a las violaciones al derecho de autor disponiéndose que "el que edite, venda, reproduzca o hiciere reproducir por cualquier medio o instrumento -total o parcialmente-; distribuya; almacene con miras a la

2 Delpiazzo, Carlos y Otros.- "Protección jurídica del Software. Ciclo de Conferencias organizado por el Instituto de Investigación jurídica". Publicada en Fundación de Cultura Universitaria. Montevideo, mayo 1992. Página 10.

3 Artículo 5° de la Ley N° 9.739 de 17 de diciembre de 1937 en la redacción dada por el artículo 3° de la Ley N° 17.616 de 10 de enero de 2003.

4 Delpiazzo, Carlos y Otra. "Lecciones de Derecho Telemático" Tomo I. Publicada en Fundación de Cultura Universitaria. Montevideo, abril 2004. Página 49.

distribución al público, o ponga a disposición del mismo en cualquier forma o medio, con ánimo de lucro o de causar un perjuicio injustificado, una obra inédita o publicada, una interpretación, un fonograma o emisión, sin la autorización escrita de sus respectivos titulares o causahabientes a cualquier título, o se la atribuyere para sí o a persona distinta del respectivo titular, contraviniendo en cualquier forma lo dispuesto en la presente ley, será castigado con pena de tres meses de prisión a tres años de penitenciaría". Se prevé la misma pena para quien "fabrique, importe, venda, de en arrendamiento o ponga de cualquier otra manera en circulación, dispositivos o productos, los componentes o herramientas de los mismos o preste cualquier servicio cuyo propósito sea impedir, burlar, eliminar, desactivar o eludir de cualquier forma, los dispositivos técnicos que los titulares hayan dispuesto para proteger sus respectivos derechos".

La ley prevé que el Juez podrá, además de aplicar las sanciones que correspondan, ordenar en la sentencia la confiscación y destrucción de las copias de obras o producciones y de sus embalajes, así como de todos los equipos utilizados para su fabricación.

Además se indica que "el que reprodujere o hiciere reproducir, por cualquier medio o procedimiento, sin ánimo de lucro o de causar un perjuicio injustificado, una obra, interpretación, fonograma o emisión, sin la autorización escrita de su respectivo titular, será castigado con multa de 10 UR (diez unidades reajustables) a 1.500 UR (mil quinientas unidades reajustables)".[5]

A propósito de la regulación nacional y su aplicación práctica podemos encontrar numerosos fallos en la jurisprudencia nacional[6].

3. Piratería en Internet

La esfera de los derechos de autor se ha expandido enormemente gracias a los progresos tecnológicos. La divulgación de las obras a través de Internet plantea nuevos desafíos, teniendo en cuenta que varios elementos que se encuentran en la web, son susceptibles de ser protegidos por los derechos de autor tales como las obras literarias, los programas de computación, las bases de datos, las obras audiovisuales, las creaciones multimedia, las fotografías, entre otros.

El Observatorio Mundial de Lucha Contra la Piratería de la UNESCO se refiere a la **Piratería cibernética** (o en línea) como "la descarga o distribución ilícitas en Internet de copias no autorizadas de obras, tales como películas, composiciones musicales, videojuegos y programas informáticos". Se agrega que las descargas ilícitas se llevan a cabo mediante redes de intercambio de archivos, servidores ilícitos, sitios Web y ordenadores pirateados.

La OMPI entiende la piratería como una infracción a los Derechos de Autor, una violación a lo que se conoce como copyright. Implica el uso no autorizado o prohibido de las obras cubiertas por leyes de derecho de autor, conociéndose como la distribución electrónica no autorizada o la descarga desde Internet de programas de software con copyright.

En palabras de Delia Lipszyc[7] los problemas de derecho de autor y derechos conexos que presenta Internet se relacionan con la licitud de las difusiones, las condiciones en que se efectúan, el pago de las remuneraciones originadas por las sucesivas explotaciones y las responsabilidades en el flujo de la información protegida.
Con el desarrollo de Internet se han apreciado tres etapas importantes en el debate sobre su impacto en los Derechos de autor[8]:

5 Artículo 46 de la Ley N° 9.739 en la redacción dada por el artículo 15 de la Ley N° 17.616.

6 Página de consulta: www.jurisprudenciainformatica.gub.uy.

7 Lipszyc, Delia. "Nuevos temas de derechos de autor". Publicada por UNESCO, CERLALC y Zavalía. Página 279.Buenos Aires, 2004.

8 Lipszyc, Delia citando a Fiscor, M. Conferencia sobre "La protección del derecho de autor y derechos conexos. Papel que desempeñan los Tratados de la OMPI sobre Internet". Durante la Consulta Regional de la OMPI sobre Comercio Electrónico y Propiedad Intelectual. Buenos

- En la primera se indicó que el derecho de autor y los derechos conexos no serían aplicables en el entorno de las redes digitales.
- Luego se planteó un enfoque contrapuesto, indicando que era posible que todo siguiera igual en el derecho de autor porque era perfectamente apto para el entorno de las redes sociales.
- En una tercera etapa se llegó a la conclusión de que sólo eran necesarias algunas adaptaciones a la normativa, que se realizaron a través de los Tratados de la OMPI sobre Derecho de Autor y sobre Interpretación o Ejecución y Fonogramas. Se analiza cómo estas adaptaciones eran motivadas por ciertas particularidades que presentaban para las obras las redes digitales. Entre otras razones porque en éstas la información se encuentra desmaterializada, no se transmite en copias tangibles, las redes permiten que la información sea accesible simultáneamente por una cantidad ilimitada de personas en el mundo y la información es recibida por el usuario en el momento y lugar en los que se encuentre.

3.1. Problemática que plantea

La piratería en Internet presenta importantes dificultades que pueden analizarse desde diversos puntos de vista.

El Observatorio Mundial de Lucha Contra la Piratería de la UNESCO ha determinado que las principales consecuencias de la piratería afectan a los creadores, porque las ventas ilícitas afectan sus ingresos. También a los trabajadores de las industrias culturales porque la piratería reemplaza a las producciones originales y por ende a sus empleos. Por último, se señala la afectación de este fenómeno a los Estados en virtud de la marginalidad en la cual se desarrollan estas actividades.

Se señalan también las repercusiones para la creatividad de los autores y la diversidad de expresiones culturales, como también para las industrias culturales legales que se ven imposibilitadas de competir contra las copias ilegales.

Todo ello, sin olvidar, como lo hemos analizado, que la piratería es un delito y como tal genera víctimas, y a su vez constituye una importante fuente de divisas para organizaciones delictivas.

3.2. Iniciativas mundiales para combatir la piratería en Internet

En los últimos tiempos hemos sido partícipes del surgimiento a nivel mundial de nuevos proyectos normativos dirigidos a regular y proteger los derechos de autor en Internet.

Es interesante realizar un análisis de los diversos proyectos planteados para intentar arribar a conclusiones sobre su posible aplicación, sus implicancias y las afectaciones que puedan generarse a otros derechos en juego.

En el plano internacional debemos tener presente la iniciativa denominada ACTA (Counterfefeiting Trade Agreement) o Acuerdo Comercial Anti-Falsificación. Se trata de un acuerdo voluntario y de carácter multilateral que busca proteger la propiedad intelectual. Fue negociado entre 2007 y el 2010 por Estados Unidos, la Unión Europea, Suiza, Canadá, Australia, Nueva Zelanda, México, Singapur, Marruecos, Japón y Corea del Sur. Ocho de los once países negociadores firmaron el acuerdo en octubre de 2011, pero hasta el mes de octubre de 2012, sólo ha sido ratificado por Japón.

El objetivo de esta iniciativa era combatir la falsificación y piratería, así como promover la cooperación internacional y crear normas internacionales eficientes para la observancia de los derechos de propiedad intelectual. Pretende establecer estándares para la observancia de los derechos de

Aires, 1999.

propiedad intelectual frente a los retos actuales, a través de la cooperación internacional. Las disposiciones del acuerdo permiten que las compañías que ofrecen conexión a internet revelen ante las sociedades de derechos de autor la identidad de usuarios sospechosos de copiar o distribuir material protegido.

Este acuerdo no permaneció ajeno a las críticas y varias organizaciones como la Electronic Frontier Fundation, y numerosos países europeos se manifestaron en contra de la firma de este acuerdo, fundamentalmente por entender que la iniciativa resulta violatoria de libertades y derechos fundamentales, además de no contener tutela judicial en los procesos que prevé.

Según lo informado por el Parlamento Europeo el proyecto no contó finalmente con los votos necesarios para ser aprobado por la Unión Europea[9].

3.3. Normativa en los países europeos

En varios países europeos se han promovido normas que han intentado regular el fenómeno de la piratería en Internet.

En España, adquiere relevancia la llamada Ley Sinde (por el nombre de su impulsora, Ángeles González-Sinde, Ministra de Cultura durante el gobierno de Rodríguez Zapatero) que integra la Ley de Economía sostenible de éste país[10]. Esta ley implica la creación de la Comisión de Propiedad Intelectual, como un órgano colegiado para el ejercicio de las funciones de mediación y arbitraje, y de salvaguarda de los derechos de propiedad intelectual.

Se dispone que la Comisión cuente con dos secciones. La primera, formada por tres miembros nombrados por el ministro de Educación, Cultura y Deporte, asumirá las funciones de mediación y arbitraje. La segunda, estará compuesta por el secretario de Estado de Cultura como presidente y cuatro vocales de los Ministerios de Cultura, Industria, Presidencia y Economía con titulación superior y conocimientos de propiedad intelectual, a ella le corresponde la salvaguarda de los derechos de propiedad intelectual frente a la vulneración por los responsables de servicios de la sociedad de la información.

La Sección podrá adoptar las medidas para que se interrumpa la prestación de un servicio que vulnere derechos de propiedad intelectual o para retirar los contenidos que vulneren los citados derechos siempre que el prestador, directa o indirectamente, actúe con ánimo de lucro o haya causado o sea susceptible de causar un daño patrimonial. Antes de proceder a la adopción de estas medidas, el prestador de servicios de la sociedad de la información deberá ser requerido a fin de que en un plazo no superior a las 48 horas pueda proceder a la retirada voluntaria de los contenidos declarados infractores o, en su caso, realice las alegaciones y proponga las pruebas que estime oportunas sobre la autorización de uso o la aplicabilidad de un límite al derecho de Propiedad Intelectual. Transcurrido el plazo anterior, en su caso, se practicará prueba en dos días y se dará traslado a los interesados para conclusiones en plazo máximo de cinco días. La Comisión en el plazo máximo de tres días dictará resolución. La retirada voluntaria de los contenidos pondrá fin al procedimiento. En todo caso, la ejecución de la medida ante el incumplimiento del requerimiento exigirá de la previa autorización judicial. Lo dispuesto en este apartado se entiende sin perjuicio de las acciones civiles, penales y contencioso-administrativas que, en su caso, sean procedentes.
De acuerdo a lo expresado, la Comisión adquiere potestades para determinar si una página web vulnera los derechos de propiedad intelectual, y tramitar su cierre. Es importante tener presente que actuará mediando denuncia de la parte que considere que sus derechos de autor se han infringido.

La Ley Sinde no estuvo exenta de críticas por parte de los usuarios así como de diversas organizaciones,

9 Noticia disponible en: http://www.europarl.europa.eu/news/es/pressroom/content/20120703IPR48247/html/El-Parlamento-Europeo-rechaza-ACTA (Página visitada el 27 de abril de 2013).

10 Texto disponible en: http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf (Página visitada el 27 de abril de 2013).

fundadas principalmente en la escaza participación judicial en el proceso y la posible censura y control sobre Internet.

El Congreso español aprobó definitivamente la Ley de Economía Sostenible el 15 de febrero de 2011, aprobando más tarde el Real Decreto 1889/2011 por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual.

Otra disposición interesante resulta la Ley Antipiratería del Reino Unido denominada como Digital Economy Act,[11] en la cual se incluyen disposiciones como la desconexión de los usuarios que descarguen de forma continuada material protegido por derechos de autor, caso en el cual se prevé la realización de una serie de avisos, pudiendo llegarse incluso a la imposición de multas de hasta 50.000 libras. Al igual que la normativa española, se prevé el cierre de páginas web que ofrezcan enlaces a contenidos con copyright.

Más controvertida es la norma que obliga a los proveedores de servicios de Internet a vigilar a sus usuarios para detectar si descargan archivos protegidos y, en caso de que lo hagan, avisar a los titulares de los mismos. Si un proveedor se niega a cumplir estas normas se arriesga a ser sancionado con una multa de hasta 250.000 libras. El Parlamento de Reino Unido aprobó el proyecto en abril del año 2010.

4. Ley SOPA

4.1. Conceptualización

Una de la iniciativas más resonantes en Estados Unidos ha sido el proyecto conocido como Ley SOPA, que refiere a la denominada Stop On Line Piracy Act (Ley H.R. 3261) que fue presentado en la Cámara de Representantes de Estados Unidos el 26 de Octubre del año 2011 por el Representante Lamar S. Smith, fundándose en los principios de su antecesora, la Ley conocida como PIPA o Protect IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act). Ésta última, tiene por objetivo brindar al gobierno de los Estados Unidos y a los titulares de **derechos de autor** herramientas adicionales para restringir el acceso a aquellos sitios web que infrinjan o falsifiquen bienes, en especial aquellos sitios registrados fuera del territorio de los Estados Unidos. La intención del proyecto es ayudar a frenar a sitios web extranjeros que publican ilegalmente, y algunas veces venden, propiedad intelectual del país.

El proyecto normativo parte de la finalidad de promover la prosperidad, la creatividad, el espíritu empresarial y la innovación mediante la lucha contra el robo de la propiedad en Estados Unidos.

La norma se integra con dos títulos: la lucha contra la piratería en línea y las mejoras adicionales para combatir el robo de propiedad intelectual. Prevé que un individuo, empresa u organismo que piense que sus derechos de autor están siendo vulnerados puede solicitar una orden judicial contra la web. Además, el Departamento de Justicia también puede solicitar bloqueos por iniciativa propia contra aquellos sitios web que permitan o faciliten la infracción a los derechos de autor.

Dentro de las medidas previstas se incluye el bloqueo por parte de los proveedores de Internet a la web o servicio en cuestión, ordena a los proveedores de acceso a Internet (ISP) que bloqueen los servidores DNS para que no acepten solicitudes de sitios web (locales y extranjeros) que alojen copias ilegales de videos, canciones, fotografías, software u otros, y a los proveedores de hosting que suspendan los servicios de hospedaje a los sitios sospechosos de violar la ley y/o enlazados con quienes sean sospechosos de hacerlo. También prevé el congelamiento de fondos por las

11 Texto disponible en: http://www.legislation.gov.uk/ukpga/2010/24/contents (Página visitada el 27 de abril de 2013).

empresas facilitadoras del cobro en Internet como por ejemplo PayPal. Además, los servicios de publicidad como AdSense de Google deben bloquear la web o servicios y no aceptar fondos para publicidad de sitios que alojen material ilegal en el extranjero. Por último, se obliga a los motores de búsqueda como Google a modificar los resultados que arrojan las búsquedas para excluir aquellos sitios web (locales y extranjeros) que alojen material ilegal. Las empresas contarán con un plazo de cinco días para acatar la orden legal.

El proyecto de ley penaliza el streaming[12] no autorizado de contenidos protegidos por copyright y prevé una pena máxima de cinco años de prisión por cada diez piezas musicales o películas descargadas dentro de los seis meses desde su estreno. Además brinda inmunidad a todos aquellos proveedores de Internet que voluntariamente lleven a cabo acciones contra tales sitios haciendo además responsable al sitio web infractor de cualquier daño producido al titular de los derechos, incluso sin tener que demostrarlo.

Como puede inferirse de las disposiciones analizadas, este proyecto ha despertado la polémica en varios sectores. Hay quienes se han manifestado a favor de la iniciativa basándose en la protección que otorga a la propiedad intelectual, el mercado asociada a ésta y sus puestos de trabajo, además de servir como elemento fortalecedor de las leyes que ya se encuentran vigentes en la materia.

Entre sus defensores se encuentran algunas organizaciones de gran importancia como la Motion Picture Association of America (MPSS), y la Recording Industry Association of America, así como otras compañías asociadas a la televisión, el cine y la música y otras que dependen de marcas registradas. A ellas se suman algunas empresas de la industria tecnológica como es el caso de Apple, Adobe y Microsoft, entre otras.

Varias voces de han levantado en contra de la ley SOPA alineándose un importante grupo de asociaciones y grandes empresas de la industria tecnológica estadounidense. Un caso de relevancia es el de la Electronic Frontier Fundation. Se trata de una **organización sin ánimo de lucro** con sede en **Estados Unidos** que tiene por objetivo proteger los derechos asociados a la libertad de expresión. Su objetivo principal declarado es educar a la prensa, los legisladores y el público sobre las cuestiones relacionadas a las **libertades civiles** relacionadas con la tecnología; y actuar para defender esas libertades[13].

También la plataforma NetCoalition.com que agrupa e empresas como Google, Yahoo, Amazon, eBay, PayPal, Expedia, Wikipedia, entre otros, se han manifestado claramente en contra de esta iniciativa.

Dentro de las medidas de oposición más trascendentes, debemos recordar que el día 18 de enero de 2012, se llevó a cabo el denominado "apagón" de Internet, liderado por Wikipedia y secundado de un modo u otro por más de 10.000 sitios de Internet entre los cuales se encontraron Mozilla y Google. En el transcurso del apagón en la página de Wikipedia en inglés podía leerse la inscripción "Imagina el mundo sin conocimiento libre".

4.1. Principales problemas que plantea

Varias son las problemáticas que esta iniciativa plantea, y que han servido para fundar las numerosas críticas y oposiciones que ha generado.

Dentro de las principales preocupaciones encontramos la innovación en la web. Es posible cuestionar

12 Streaming es un término que hace referencia al hecho de escuchar música o ver vídeos sin necesidad de descargarlos de Internet, por ejemplo, cuando se transmite radio en vivo por Internet.

13 Más información sobre esta organización se encuentra disponible en www.eff.org.

que la Ley SOPA se convierta en un inconveniente para ésta, afectando los negocios vinculados a la red así como la inversión y el empleo asociados a ésta. Ello, partiendo de la idea general de que la regulación de Internet, en el caso de que se entienda pertinente, debe ser efectiva, proporcionada y preservar los beneficios de una Internet abierta.

Prosiguiendo con el análisis, podremos pensar en las implicancias que esta normativa generaría para los sitios web. Frente a la sospecha de infracción se produciría la baja del sitio lo cual puede significar un importante golpe económico, sobre todo para los sitios de bajo presupuesto.

Por otra parte, preocupa la situación de los blogs o sitios que alojan contenido proporcionados por los usuarios, como por ejemplo Youtube o incluso las redes sociales. Los portales basados en la interacción con los usuarios pueden verse bloqueados por la acción de alguno de ellos. Esta situación podría generar censura en portales y sitios de todo el mundo porque la mayoría de las conexiones pasan por Estados Unidos. Para evitarlo, cada sitio debería evaluar y filtrar continuamente los contenidos que se publican, para librarse de asumir la responsabilidad por los contenidos subidos por los usuarios y por lo tanto, las sanciones que la ley prevé.

Merece especial atención las posibles vulneraciones que esta normativa podría significar para la libertad de expresión en Internet, sobre todo si pensamos en que cualquier sitio en la red puede ser investigado y monitoreado, e incluso sancionado.

Las posibles implicancias o limitaciones a la libertad de expresión han sido el principal detonante para que actualmente el proyecto de encuentre en suspenso. La administración del Presidente Barack Obama, a través del blog de la Casa Blanca, anunció que se opondría a toda iniciativa de ley que limite la libertad de expresión en Internet, aumente los riesgos cibernéticos y erosione la capacidad de innovación en red[14].

5. Repercusiones de las leyes planteadas para el derecho a la protección de datos personales

Uno de los temas que ha generado importantes críticas por parte de las empresas, los usuarios y la doctrina, ha sido el de la repercusión que pueden tener leyes como la SOPA, en el derecho a la protección de datos personales.

Los temores acerca de los posibles atentados contra la privacidad de los usuarios se fundamentan en la posibilidad de que, a través de una orden judicial, se exija a los proveedores de Internet que bloqueen el acceso para sus clientes localizados en Estados Unidos hacia el sitio infractor. Estas normas impulsan a los proveedores a vigilar la información que los usuarios suben a la red. Implicaría inspeccionar las direcciones IP de sus clientes, y así analizar la información que se transmite desde y hacia el usuario.

Para analizar esta cuestión, es interesante partir de algunas precisiones conceptuales sobre las direcciones IP. El Dr. Carlos Delpiazzo[15] explica de manera simple algunos de éstos conceptos. Indica que una red es la manera de conectar varias computadoras entre sí, compartiendo recursos e información. El protocolo es el lenguaje que permite la interconexión entre todos ellos, como idioma único. De los protocolos existentes el más difundido es el TCP/IP que funciona como el idioma

14 Información disponible en: http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-on-line-piracy. (Página visitada el 27 de abril de 2013).

15 Delpiazzo, Carlos y Otra. Ob. Cit. "Lecciones de Derecho Telemático" Tomo II. Publicada en Fundación de Cultura Universitaria. Montevideo, marzo 2009. Página 89.

común conocido por todos. La sigla IP representa a cualquier máquina conectada a la red, de modo de que las otras máquinas puedan enviarle datos. Se habla de direcciones IP como un identificador. En virtud de que para los usuarios no es fácil retener las secuencias numéricas que integran su IP, se ha creado el denominado Sistema de Nombres de Dominio o DNS, por el cual, cada nombre de dominio es un identificador técnico que traduce una dirección IP.

Lo que debemos estudiar en este punto es el carácter de dato personal de la dirección IP de los usuarios y determinar si se trata de un dato que identifique a la persona o lo haga identificable.

En opinión de la Agencia Española de Protección de Datos Personales emitida en Informe N° 327/2003, la cuestión debe resolverse a través del análisis de la definición misma de dato personal como cualquier información concerniente a persona física identificada o identificable. Se afirma que los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Ello implica que si se puede identificar al usuario, es posible acceder a otros datos como el nombre, dirección, teléfono u otros.

Se concluye el Informe indicando que "aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos".

También el Grupo de Trabajo del Artículo 29, en el Dictamen N° 4 del año 2007, sobre el concepto de datos personales, ha determinado que "los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva"[16].

La consideración de la Dirección IP como un dato de carácter personal implica la aplicación de las leyes en la materia y por lo tanto la imposición de determinadas obligaciones para los responsables de las bases de datos. Una de las más trascendentes será la asociada a la adopción de medidas de seguridad que garanticen la protección integral de los datos.

De acuerdo a estas opiniones que hemos analizado, las leyes como la SOPA deberán tener presente la calidad de dato personal de las direcciones IP. Ello lleva a reflexionar sobre la naturaleza de la protección de datos personales como un derecho fundamental, que en caso de afectarse, debería ser en forma restrictiva y en casos expresamente determinados.

6. Conclusiones finales

En el transcurso del presente trabajo hemos analizado la regulación de los derechos de autor y la transformación que han sufrido como consecuencia de la incidencia de la tecnología y de Internet.

Es claro que el tema de la piratería en Internet es un fenómeno que genera opiniones controversiales y ha provocado un intenso debate. Las iniciativas legales que se han presentado para combatir este

16 Texto disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf (Página visitada el 3 de setiembre de 2013)

fenómeno presentan importantes discrepancias en virtud de su inevitable colisión con derechos fundamentales tales como la libertad de expresión y la protección de datos personales.

Lo cierto es, que más allá de las leyes que hemos analizado, el problema de la piratería en línea persiste y los problemas que genera aún se encuentran sin solución. Buscar la forma de regular Internet de manera tal que la propiedad intelectual quede protegida, sin violar las libertades fundamentales, sin generar poderes excesivos a favor de los gobiernos, y sin reprimir la innovación y la inversión en la web, no es una tarea fácil de afrontar.

Sin duda debe fomentarse un debate más profundo acerca de estas cuestiones y de la necesidad de que exista una regulación, con la participación de todos los actores interesados y de la opinión pública, en búsqueda de soluciones con el mayor grado de consenso posible.

CAPITULO XIII

COOPERACIÓN INTERNACIONAL

Esc. Cecilia Montaña

COOPERACIÓN INTERNACIONAL

Esc. Cecilia Montaña

1. Introducción

La cooperación internacional entre las autoridades de protección de datos, es cada vez más necesaria ante el avance de la tecnología. El cumplimiento de las distintas normativas nacionales en la materia, muchas veces implica flujo transfronterizo de datos. A esto se debe adicionar las brechas de seguridad que involucran a más de un estado y la existencia de las grandes bases de datos (big data).

La actual tendencia hacia una legislación global de protección de datos personales y los diversos sistemas de cooperación serán los temas a analizar.

2. Implicancias de la Cooperación internacional en el ámbito de las autoridades de Protección de Datos

En el ámbito internacional existen diferentes formas o maneras en las que pueden funcionar los mecanismos de Cooperación.

Puede decirse entonces que existen mecanismos de Cooperación que funcionan en forma horizontal, donde las Autoridades se encuentran en un plano de igualdad. Es el caso de las Autoridades de Protección de Datos que por razones geográficas, realizan acuerdos de intercambio de tecnología y conocimiento entre ellas, por ejemplo APPA, (por sus siglas en inglés Asia Pacific Privacy Authorities).

Otra forma de Cooperación se desarrolla en aquellos lugares donde existe una Autoridad de Protección de Datos más antigua, la cual apoya y fomenta la creación y funcionamiento de Autoridades en países donde la Protección de Datos es más reciente.

3. Funcionamiento de la Cooperación Internacional

La cooperación Internacional se hace posible gracias a diversas formas que se reflejan en varios instrumentos normativos: acuerdos, declaraciones, planes de acción, reuniones ministeriales y de expertos, y programas de supervisión, evaluación y asistencia.

4. Sistemas de Cooperación Internacional

4.1. Asia Pacífico

APPA

Uno de los sistemas de cooperación es la APPA (Asia Pacific Privacy Authorities), que reúne a las autoridades de México, Australia, Canadá, Hong Kong, Nueva Zelanda, Korea y la FTC de EEUU.

Esta Asociación funciona como foro para intercambiar ideas sobre normativa, tecnologías y el manejo de las consultas y las denuncias. El foro comenzó con las autoridades de Australia, Nueva Zelanda Hong Kong y Korea. Los demás miembros se unieron en el 2005, y desde ese año tiene una convención anual donde se discuten temas tales como: reforzar el cumplimiento de las leyes entre las jurisdicciones, enmiendas normativas, la existencia de un código a nivel mundial sobre cómo realizar los test anti doping.

Dentro de los objetivos adoptados en Auckland en diciembre de 2010, se resuelve que:

- La privacidad es un tema relevante a nivel mundial.
- Las redes conectan personas y negocios sin tomar en cuenta fronteras físicas.
- Tanto los gobiernos como la sociedad esperan regulaciones efectivas
- Los problemas relacionados con la privacidad pueden surgir en una jurisdicción y otras autoridades de protección de datos se pueden beneficiar estando alertadas.
- Las autoridades de protección de datos cada vez son más llamadas a resolver problemas transfronterizos.
- Las autoridades de protección de datos pueden beneficiarse buscando información, inspiración y asistencia fuera de fronteras.
- Los participantes del foro intercambian conocimientos y recursos técnicos.

El foro estableció a nivel regional la importancia de la privacidad y el mantenimiento de flujos de información.
Como resoluciones se toman:

- Facilitar el intercambio de conocimiento en la región
- Fomentar la cooperación en protección de datos
- Promover conjuntamente actividades de concientización
- Promover las mejores prácticas entre autoridades de protección de datos
- Trabajar para mejorar la regulación
- Mejorar la cooperación transfronteriza

Asimismo el foro estableció pautas para estandarizar las prácticas administrativas tales como citar informes de denuncias, publicación de reportes, consolidar la World Legal Information Institute's Privacy Law Library como punto de acceso a los informes.

La lista de los miembros de la APPA, así como de los comunicados de los distintos Foros: http://www.privacy.gov.au/aboutus/international/appa

4.2. Asistencia de CNIL a otras autoridades

CNIL

La autoridad francesa de Protección de Datos es el miembro creador de la Asociación Francófona de Autoridades de Protección de Datos Personales (AFAPDP). Esta asociación funciona desde 2007 con el cometido de promover la cultura de las "libertades informáticas" en el seno de los países francoparlantes. Asimismo uno de los objetivos era lograr que Burkina Faso, Túnez y Marruecos tuvieran una ley de protección de datos.
Se trata de otro tipo de cooperación internacional, donde una autoridad de protección de datos personales con mucha historia (la CNIL fue creada en enero de 1978) apoya a otros países a desarrollar normativa en materia de protección de datos personales.

Dentro de los compromisos de la AFAPDP se encuentran:

- En 2004 en la Conferencia de Ouagadougou se comprometieron al desarrollo de normas de PDP y a la cooperación entre las autoridades de PDP independientes.
- En 2006 en la Conferencia de Bucarest se comprometieron a pronunciarse favorablemente a la existencia de un instrumento internacional que garantice el derecho a la protección de los datos personales.
- En 2010 en la Conferencia de Montreal se comprometieron a adoptar una legislación que garantice la PDP y sostener esfuerzos en vías de lograr una herramienta internacional.

La CNIL tiene como objetivo concretar estos compromisos, así como los demás estados miembros de la AFAPDP, quienes entienden que las tecnologías de la información son una oportunidad para consolidar un estado de derecho.

Asimismo y a pedido de las autoridades de Protección de Datos Personales francoparlantes, la CNIL desarrolló un proyecto de ley de PDP para poner a disposición de los demás estados. En la redacción se tuvieron en cuenta 3 objetivos:

- participar en el acercamiento de las legislaciones.
- hacer visible el derecho a la Protección de Datos Personales.
- que la ley se adapte a las problemáticas locales.

El proyecto cuenta con 34 artículos, un anexo con sanciones administrativas y uno con sanciones penales. Como archivo separado se incluye una exposición de motivos.

Los documentos se encuentran disponibles en el link:
http://www.cnil.fr/la-cnil/nos-defis/a-linternational/francophonie/

4.3. Sistema de información europea, (Cooperación Schengen).

SISTEMA DE INFORMACIÓN SCHENGEN (SIS)

El Acuerdo de Schengen fue firmado en 1985 (en la ciudad de Schengen, Luxemburgo) y entró en vigor en 1995. Se trata de un acuerdo para eliminar controles fronterizos dentro del espacio del acuerdo y unificar controles externos al mismo. El espacio incluye a los estados del espacio europeo con la excepción de Bulgaria, Chipre y Rumanía que aún no son miembros de pleno derecho y por eso se mantienen los controles aduaneros con los citados países.

La libre circulación implica dentro del espacio de Schengen medidas de cooperación y coordinación entre los servicios de policía y las autoridades judiciales. Los Estados miembros participantes facilitan datos, denominados "descripciones", sobre personas buscadas o desaparecidas, bienes robados u ocultados.

Dentro del tratado, el Título VI refiere a la protección de datos personales de las personas incluidas en la base de datos del SIS.

El 8 de febrero de 2012 Peter Hustnix en su conferencia en el Parlamento Europeo "Data Protection and Schengen Governance" concluye que en el desarrollo del SIS se debe considerar la protección de datos personales como una obligación desde el diseño del software (privacy by design).

Un punto importante sería que los datos se borren automáticamente luego de un plazo establecido.

Además los ciudadanos deben ser protegidos eficazmente contra las inexactitudes de los datos o negligencia en el intercambio, así como estar informados de sus derechos.[1]

La protección de datos personales es esencial para la legitimidad y éxito del SIS y la supervisión del desarrollo del SIS II. El SIS II permite acceso a Europol, Eurojust y autoridades locales de licencias de vehículos y además adiciona datos biométricos.

4.4. El Grupo de trabajo del artículo 29

ARTICLE 29 WORKING PARTY

El Grupo de trabajo del artículo 29 fue creado por la Directiva de protección de datos (Directiva 95/46/CE) y comenzó su funcionamiento en 1996.

Este Grupo se compone por un representante de la autoridad de protección de datos de cada Estado miembro de la Unión Europea, asimismo se incluye al Supervisor Europeo de Protección de Datos y también un representante de la Comisión Europea, lo cual hace de este grupo una importante plataforma de cooperación.

El Grupo busca lograr una armonización de las normas de protección de datos a nivel europeo. En base a esas normas es que surgen los estándares de adecuación, clasificándose a los países como adecuados o no adecuados.

El Grupo de Trabajo del artículo 29 tiene dentro de sus principales misiones la de dar consejos de expertos a los Estados en relación con la protección de datos y promover la aplicación uniforme de la Directiva de protección de datos en todos los estados miembros de la UE a través de la cooperación. Asimismo el Grupo de trabajo facilita a la Comisión dictámenes sobre las leyes comunitarias que afectan el derecho a la Protección de Datos Personales.

4.5. Red Iberoamericana de Protección de Datos

RIPD

La Red Iberoamericana de Protección de Datos fue creada en 2003, con el acuerdo de representantes de 14 países de Iberoamérica.

Esta Red se constituye como un foro de entidades públicas y privadas que desarrollan iniciativas relacionadas a la protección de datos personales, así como el intercambio de experiencias, conocimiento y buenas prácticas en la materia.

Actualmente los integrantes de la RIPD, se encuentran avocados a obtener el estatus de país adecuado por parte de la Comisión Europea mediante desarrollos normativos que garanticen el

1 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-02-08_SD_Schengen_EDPS_EN.pdf (Página visitada el 12 de julio de 2012).

derecho a la protección de datos como un derecho fundamental.

Uruguay obtuvo esta adecuación en el año 2012, siendo el segundo en obtenerla junto a Argentina dentro de Latinoamérica.

La RIPD se compone de los siguientes miembros: Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, España, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, República Dominicana, Uruguay y Venezuela.

Dentro de sus cometidos se encuentra la suscripción de acuerdos y convenios para la colaboración entre los diversos organismos garantes de protección de datos.[2]

5. Buenas prácticas

Una de las buenas prácticas que mejores resultados plantea es el mantener reuniones de trabajo en forma asidua con el objetivo de acompasar la normativa de protección de datos a las nuevas tecnologías. Así lo realiza por ejemplo el Grupo de Trabajo del Artículo 29, quien mantiene reuniones temáticas a través de múltiples canales abordando la problemática que se pueda suscitar en temas referentes a la protección de datos y privacidad. (subgrupos de trabajo presenciales y a través de internet).

En Marzo de 2012 la CNIL envió una nota a Google a fin de que adecuaran el funcionamiento del buscador a la normativa de Protección de Datos de la UE. Con dicha nota se adjuntaba un cuestionario con la finalidad de determinar si la nuevas políticas de Google se adaptan a la buenas prácticas respecto a la protección de datos. Dentro de las mismas se consulta sobre la finalidad de los datos, si existe la opción opt-in para el intercambio de datos sensibles y también contempla la protección de datos en las plataformas móviles.[3]

Dentro del marco de las buenas prácticas, desde enero de 2013 Europa cuenta con una nueva forma de combatir los ciberataques. Fue creada la unidad especializada de lucha contra el cibercrimen "European Cybercrime Centre" o EC3 (por las siglas en ingles).

El Centro EC3 es una respuesta colectiva de la Unión Europea, que a través de la Comisión Europea creó el Centro utilizando la infraestructura de Europol. Cada vez es mayor el flujo de datos personales a través de redes sociales e internet generándose así un aumento directamente proporcional en la ciberdelincuencia que genera un alto costo a la sociedad y un reto a los encargados de hacer cumplir la ley.

El EC3 tiene como principales cometidos abordar varias áreas de la delincuencia informática como por ejemplo: el fraude en línea, explotación sexual infantil en línea, y aquéllas que afectan la infraestructura crítica y sistemas de información en la Unión Europea.[4]

2 http://www.redipd.org/documentacion/acuerdos_convenios/index-ides-idphp.php (Página visitada el 1 de mayo de 2013).

3 http://www.cnil.fr/la-cnil/actualite/article/article/nouvelles-regles-de-confidentialite-de-google-la-cnil-adresse-un-questionnaire-detaille/ (Página visitada el 19 de julio de 2012).

4 https://www.europol.europa.eu/ec3 (Página visitada el 1 de mayo de 2013).

6. Conclusiones

Se debe concluir que el único camino posible en este mundo globalizado es proteger la privacidad y la confidencialidad de los individuos como derechos fundamentales que son, conforme a los instrumentos existentes.

No debemos olvidar que la seguridad y los derechos humanos como conceptos inmutables nos llevan a compartir responsabilidades y consensuar reglas y principios a través de las herramientas de cooperación.

Asimismo es primordial a nivel latinoamericano fortalecer los mecanismos de cooperación existentes tales como la RIPD, para lograr mayor acercamiento y coordinación entre las Autoridades de Protección de Datos, estrechando los lazos entre estas entidades reguladoras.

CAPITULO XIV

HERRAMIENTAS DE CONCIENTIZACIÓN Y DIFUSIÓN

¿PREPARADO PARA UNA VIDA 3.Ø?

Dra. Bárbara Muracciole

HERRAMIENTAS DE CONCIENTIZACIÓN Y DIFUSIÓN ¿PREPARADO PARA UNA VIDA 3.Ø?

Dra. Bárbara Muracciole

1. Introducción

Tan importante como abordar los problemas de la privacidad desde lo que hoy sucede, es hacerlo pensando en el futuro. Por esa razón, es que aún en plena vigencia de la web 2.0, les proponemos conocer las características y desafíos de la vida 3.0.

2. ¿Evolución o revolución?

Para poder ver con mayor claridad hacia donde nos dirigimos, es necesario recordar de dónde venimos y dónde estamos. En este sentido, tenemos que tener presente que para llegar a la web 3.0, necesariamente pasamos por las versiones 1.0 y 2.0.

2.1. Web 1.Ø

Todo comenzó con una web unidireccional y no colaborativa. Muchos leían información que pocos producían en virtud de ser quienes conocían los lenguajes de programación. La web era un repositorio estático de información. Los sitios eran carentes de toda interacción y actualización periódica. Incluso la conexión era diferente, se hacía a través de la línea telefónica mediante un módem, produciendo aquel sonido característico y peculiar. En ese entonces, utilizar el correo electrónico requería de mucho tiempo, dedicación y paciencia.

2.2. Web 2.Ø

Con el advenimiento de la versión 2.0, el escenario cambió. Entramos en una era bidireccional y colaborativa. Los propios usuarios nos transformamos en proveedores de contenidos, debido a la posibilidad de publicar información por nosotros mismos y cambiar contenidos sin necesidad de especiales conocimientos técnicos. Las fuentes de producción de contenidos pasaron a ser múltiples, facilitando y promoviendo la interacción.

Las conexiones se aceleraron al igual que las velocidades de navegación. Consultar el correo pasó a formar parte de nuestras vidas, al igual que las redes sociales. La web 2.0 cambió definitivamente nuestra forma de relacionarnos, comunicarnos y trabajar. Se incorporó de forma tal a nuestras vidas, que resulta dificil pensar en vivir "desconectados".

En relación a la web 1.0, esta versión ahorró tiempo al usuario, estandarizó lenguajes y facilitó la convergencia tecnológica y de contenidos, convirtiéndose en el mayor repositorio de información disponible en la actualidad.

Sin embargo, la información que conforma este repositorio no tiene la capacidad de relacionarse entre sí, no está clasificada, no está ordenada y no posee formato estándar. Resultado de ello: la sobrecarga de información y heterogeneidad de las fuentes, con los consecuentes problemas de interoperabilidad. Cuando el internauta busca un determinado dato, recibe una masa caótica de información que no es capaz de procesar y que le genera más dudas que certezas.

2.3. Web 3.0

Se utiliza usualmente como sinónimo o en forma indistinta a web semántica, lo que no es correcto. Estamos ante un término más amplio que engloba la inteligencia artificial, la semántica, la tridimensionalidad y la geoespacialidad, y que promete solucionar los problemas de su antecesora mediante agentes inteligentes que leerán información y devolverán conocimiento. Este avance por demás significativo, ha dado lugar a varios autores a sostener que el paso de la versión 2.0 a la 3.0 más que una evolución, es una revolución.

2.3.1. Web semántica

Siguiendo la estructura planteada por W3C en su Guía Breve de Web Semántica[1], proponemos tres grandes preguntas:

2.3.1.1. ¿Qué es la Web Semántica?

La Web Semántica es una web dotada de mayor significado, que permitirá a cualquier usuario encontrar la información que busca en forma rápida y sencilla. Se basa en la idea de agregar significado a la web, sumarle semántica mediante metadatos asociados a la información. Esto hará que la web deje de ser solamente comprensible por los seres humanos y que pueda ser comprendida por máquinas a través de software capaz de relacionar, clasificar y comprender el contenido.

"Esta Web extendida y basada en el significado, se apoya en lenguajes universales que resuelven los problemas ocasionados por una Web carente de semántica en la que, en ocasiones, el acceso a la información se convierte en una tarea difícil y frustrante".[2]

2.3.1.2. ¿Para qué sirve?

Al realizar una búsqueda, el usuario recibirá exactamente lo que busca, evitando el "buceo" manual entre cientos y en algunos casos miles de resultados. Esto, debido a que "El software es capaz de procesar el contenido, razonarlo, combinarlo y realizar deducciones lógicas para resolver problemas cotidianos automáticamente"[3].

2.3.1.3. ¿Cómo funciona?

La Web tendrá la capacidad de construir una base de conocimiento sobre las preferencias de los usuarios, información que, combinada con la contenida en la web, será capaz de responder con exactitud las solicitudes realizadas por los usuarios.

"La forma en la que se procesará esta información no sólo será en términos de entrada y salida de parámetros sino en términos de su **SEMÁNTICA**. La Web Semántica como infraestructura basada en metadatos aporta un camino para **razonar** en la Web, extendiendo así sus capacidades"[4]

1 W3C. "Guía Breve de Web Semántica". Publicada en http://www.w3c.es/Divulgacion/GuiasBreves/WebSemantica (Página visitada el 12 de Agosto de 2012).

2 W3C. Ob. Cit. Pág. 1.

3 W3C. Ob. Cit. Pág. 1.

4 W3C.Ob. Cit. Pág. 2.

2.3.2. Web 3D

Web 3.0 también significa convergencia del mundo real con el mundo virtual.

Se denomina de esta forma, por un lado, a la posibilidad de desplazarnos a través del navegador por un espacio tridimensional. Por ejemplo MapsGL de Google Maps. Se apoya en la WebGL para ofrecernos vistas tridimensionales. Podemos acercarnos a nuestros objetivos y desplazarnos por las tres dimensiones virtuales. Es una extensión de vida hacia los mundos virtuales.

Por otro lado, refiere a la posibilidad de interconectar mundos virtuales con instalaciones y sensores físicos en una realidad convergente. Nos referimos a los mundos de realidad virtual conectados a nuestra realidad física a través de la web.

2.3.3. Web geoespacial

La Web 3.0 implica asimismo la identificación de la información en un tiempo y en un lugar determinados. El componente geoespacial sumado a la semántica, logran simplificar las búsquedas y resolver asuntos cotidianos de los usuarios de la web.

Pensemos en una búsqueda orientada a conocer los vuelos a la ciudad de Buenos Aires el día de mañana por la mañana. Como bien señala W3C en su Guía Breve de Web Semántica, la ubicación geográfica desde la que el usuario envía su pregunta será detectada en forma automática sin necesidad de especificar el punto de partida, elementos de la oración como "mañana" adquirirán significado convirtiéndose en un día concreto calculado en función de un "hoy". Algo semejante ocurriría con el segundo "mañana", que será interpretado como un momento del día. Resultado: búsquedas más precisas y personalizadas.

2.3.4. Web de las cosas

La web 3.0 también se identifica con la llamada "web de las cosas", debido a que nos permitirá controlar plenamente objetos a distancia. A través de un mensaje de texto en nuestros celulares, podremos recibir reportes sobre cómo funciona el sistema de riego o calefacción de nuestras casas, para poder regularlos y encontrar el jardín regado y la casa calefaccionada cuando retornemos de nuestros trabajos.

Según Vint Cerf "La web 3.0 nos llevará a la internet de las cosas, en donde todas las aplicaciones y los objetos van a tener la potencialidad de interactuar unos con otros. La clave será la interconexión total"[5]

5 Infobae.com. "Cómo será la Web 3.0". Publicado en http://www.infobae.com (Página visitada el 12 de Agostos de 2012).

3. Privacidad y protección de datos

La Web 3.0 será "una Web hecha de partes de cada uno de nosotros, una Web que estará presente en forma natural y permanente en nuestras vidas, y que por esta razón deberá "conocernos mejor", demandará una mayor "transparencia" en la relación con el usuario, y es ahí donde será interesante observar el rol que jugará la privacidad, y el rol que jugaremos "nosotros"."[6]

Atento a la capacidad de relacionar información de esta nueva versión, la primera impresión que se tiene al estudiar estos temas, es que los individuos seremos transparentes ante los agentes inteligentes y que será muy difícil preservar un espacio privado en la web 3.0. Lo que no significa que pueda prescindirse de la privacidad y la protección de datos, sino que habrá que repensar los principios en pos de su aplicación al nuevo escenario de juego.

Comparto plenamente las menciones realizadas por algunos autores respecto de "que el rol que ocupa hoy la privacidad en Internet dará un giro interesante" y "que la privacidad en la Web 3.0 es un punto que debería tenerse en cuenta desde el diseño de sus componentes funcionales y técnicos, dado que si no se cuenta con la confianza y la colaboración del usuario, la esencia del fenómeno social conocido como Web 3.0 estará perdida"[7].

4. Propuestas

En este sentido, resultan alentadores algunos proyectos que desde el campo técnico piensan en proteger la privacidad desde su diseño. Es el caso del proyecto Smart Data, llevado adelante por el científico George Tomko, para desarrollar aplicaciones Web basadas en agentes inteligentes que llevarán a cabo dos tareas: almacenar de forma segura los datos personales y proteger la privacidad y seguridad de los datos[8].

Pero no solo desde el campo técnico es necesario abordar la protección de la privacidad en la web versión 3.0. La educación sigue siendo un factor clave. Nos referimos a una educación útil que empodere a los usuarios y les permita navegar con plena conciencia. El eslabón más débil de la cadena es el usuario que utiliza tecnología que desconoce.

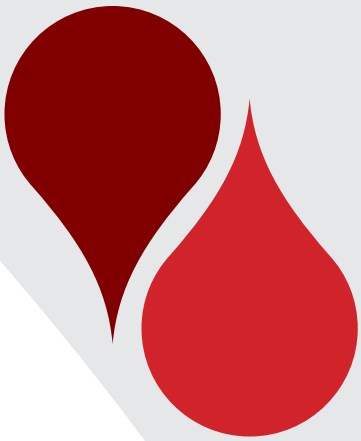
5. Conclusiones

La Web 2.0 se encuentra próxima a cambiar. En el nuevo escenario, será necesario defender que los derechos a la privacidad y a la protección de datos personales no deben renunciarse para utilizar o acceder a mejores aplicaciones en los entornos virtuales, y eso únicamente podrá hacerlo un usuario educado al respecto.

6 Sallis, Ezequiel. "El Rol de la Privacidad en la Web 3.0 y Más Allá". Publicado en http://www.root-secure.com/arch/Rol_de_la_Privacidad-Web_3_y_Mas_Alla.pdf (Página visitada el 12 de Agosto de 2012).

7 W3C. Ob. Cit. Pág. 2.

8 Información disponible en http://www.ipsi.utoronto.ca/docs/TomkoLectureNov29-10.pdf (Página visitada el 15 de Febrero de 2013).



CAPITULO XV

NUEVA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES

Dra. Graciela Romero

NUEVA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS PERSONALES

Dra. Graciela Romero

1. Introducción

Los cambios producidos por las nuevas tecnologías de la información (NTI) han impactado directamente en la forma en que la información y los datos personales circulan alrededor de todo el mundo. Esto ha obligado a diseñar o re-diseñar las soluciones jurídicas ya existentes, para poder dar respuesta acorde a los problemas que se generan, sobre todo con relación a la protección de la privacidad de las personas.

Es el caso concreto de la Directiva Europea 46/95/CE, que data del año 1995 y que ya no se encuentra en consonancia con los nuevos tiempos. Además la misma ha sido aplicada por los países que integran la Unión Europea de una forma tan dispar, que ello ha provocado desconfianza e inseguridad, en cuanto a las garantías y derechos que poseen tanto las personas como las empresas.

Al respecto, Peter Hustinx, Supervisor Europeo de Protección de Datos, ha señalado otra razón que avala el cambio y refiere al "impacto del Tratado de Lisboa que entró en vigor en diciembre del 2009", por el cual "la Carta de Derechos Fundamentales pasó a ser vinculante para las instituciones y organismos de la Unión Europea", reconociendo en forma explícita, "(...)el derecho a la protección de datos personales (artículo 8), que se añade al respeto por la vida privada (artículo 7)".

En cuanto al uso masivo de la red, Viviane Reding, Comisaria de Justicia de la Unión Europea y Vicepresidenta de la Comisión ha señalado que "hace 17 años, menos de un 1 % de los europeos usaba Internet. Hoy en día se transfieren e intercambian enormes cantidades de datos personales entre continentes y de una punta a otra del mundo en fracciones de segundos. La reforma facilitará el funcionamiento de las empresas y les permitirá ahorrar costes. La existencia de un marco legal sólido, claro y uniforme a escala de la UE permitirá liberar el potencial del Mercado Único Digital y fomentar el crecimiento económico, la innovación y la creación de empleo"[1].

Es en definitiva, a causa de esta nueva realidad cultural, social, económica y política, que la Comisión Europea ha apostado a una reforma que unifique toda la legislación de la materia, impulse la economía digital de la región, suprima algunos costos y otorgue nuevos derechos y garantías a las personas, sobre todo a los consumidores de servicios en línea y usuarios de redes sociales. La protección de datos personales se posiciona nuevamente, como un aspecto central del desarrollo e impulso que se pretende otorgar a la economía del continente, tal cual se reconoce en la Agenda Digital Europea y en la Estrategia Europa 2020.

1 Comunicado de Prensa de la Comisión Europea. Visto http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=ES&guiLanguage=en. (Página visitada el 29 de mayo de 2012).

2. Ámbito de aplicación de la nueva normativa

2.1. Alcance

La reforma propone la creación de dos nuevas herramientas jurídicas: un Reglamento[2] que se aplicará en todos los países que integran la Unión Europea, buscando así suprimir la actual fragmentación legislativa, "estableciendo un marco sólido, coherente y moderno en materia de protección de datos a escala de la UE, tecnológicamente neutro y válido para las próximas décadas"[3], y una Directiva[4] que se aplicará a los datos personales que son tratados con fines de prevención, detección, investigación o persecución de los delitos por parte de las autoridades correspondientes.

A su vez, se aplicará al tratamiento total o parcialmente automatizado, así como al no automatizado de aquellos datos personales, contenidos en una base o fichero que reúna determinadas características. En cambio, no será de aplicación al tratamiento de datos personales que se realice en el ejercicio de actividades que no están comprendidas en el ámbito de aplicación del derecho de la UE, en particular la seguridad nacional. Tampoco al que realice una persona física, sin interés lucrativo en el ejercicio de actividades exclusivamente personales o domésticas, ni al que realizan las autoridades competentes con fines de prevención, detección, investigación, etc., de los delitos para lo cual se aprobará la nueva directiva, según ya se ha expresado.

Por su parte, alcanzará al tratamiento de datos personales en el contexto de actividades llevadas a cabo por el responsable o encargado de un establecimiento ubicado en la UE, pero también al tratamiento de datos cuyos titulares residan en la UE aunque sea realizado por un responsable de establecimiento que no tenga sede en la UE, siempre que ese tratamiento se refiera a actividades relacionadas con la oferta de bienes o servicios o al control de su conducta.

También se aplicará al tratamiento de datos, realizado por un responsable que no esté en el territorio de la UE, pero corresponda la aplicación de la legislación nacional de un Estado miembro en virtud del Derecho Internacional Público (por ejemplo embajadas, consulados, buques o aeronaves).

El criterio finalmente adoptado en este nuevo reglamento, se enfoca más hacia las personas y sus derechos, presuponiendo la aplicación de una normativa que protege y garantiza el control de los datos personales más allá de las fronteras, lo cual aplica aunque la empresa no esté ubicada en la UE (art. 3.2), en consonancia con lo establecido en el Dictamen 8/2010 del Grupo de Trabajo del Artículo 29[5].

2 Ver Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de Protección de Datos). Bruselas, 25.1.2012. Accesible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

3 Ver Ficha Financiera Legislativa. Compatibilidad y posible sinergia con otros instrumentos financieros. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF Pág. 95.

4 Ver Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de delitos o la ejecución de sanciones penales, y a la libre circulación de estos datos. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=-COM:2012:0011:FIN:ES:PDF Pág. 1.

5 Ver http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf (Página visitada el 7 de junio de 2012).

2.2. Objetivos

Con la esta nueva reglamentación se buscan los siguientes objetivos[6]:

a) Adaptar los principios, derechos y garantías de las personas a una nueva realidad política, social y económica. Al decir de la propia Comisión: "aumentar la eficacia del derecho fundamental a la protección de datos y otorgar a los interesados el control de sus propios datos, en particular en el contexto de la evolución tecnológica y la creciente globalización"[7].

b) Uniformizar la legislación de protección de datos personales de los países que conforman la Unión Europea, mejorando "la dimensión del mercado interior de la protección de datos reduciendo la fragmentación, reforzando la coherencia y simplificando el entorno reglamentario"[8]. Por otra parte, en lo que refiere a los responsables, entidades públicas y empresas, la Comisión afirma que "se beneficiarán de una mayor seguridad jurídica gracias a la armonización y clarificación de las normas y procedimientos", que garantizarán "las mismas condiciones y aplicación coherente" de las normas.

c) Por último, **reducir los costos administrativos y simplificar los trámites que deben realizar las empresas** eliminando, por ejemplo, las notificaciones de bases de datos o ficheros, a la vez que se impulsa la economía digital de la región reforzando la confianza de los consumidores, creando empleo y fomentando la innovación. En este sentido, se afirma que las personas tendrán un mejor control de sus datos personales lo cual aumentará la confianza en el entorno digital.

2.3. Impacto

Se prevé que la reforma beneficie directamente a "las personas físicas, mediante el refuerzo de sus derechos en materia de protección de datos, en particular en un entorno digital"[9], pero a su vez que "simplifique el entorno legal para las empresas y el sector público, lo que permitirá estimular el desarrollo de la economía digital en el marcado interior de la UE y más a allá de sus fronteras, en consonancia con los objetivos de la Estrategia Europa 2020"[10].

Esta proyección se realiza a partir de la información obtenida a través de la realización de una amplia consulta a los ciudadanos europeos, a los consumidores, autoridades, entidades que trabajan a favor de la protección de datos personales, así como a diversos operadores del sector privado. Asimismo, se consideraron también como aportes, los estudios y dictámenes emitidos por el Grupo de Trabajo del Artículo 29 y del Supervisor Europeo de Protección de Datos.

Respecto a la consulta, la gran mayoría de los entrevistados opinó que "los principios generales siguen siendo válidos, si bien es necesario adaptar el marco vigente para responder mejor a los retos que plantea el rápido desarrollo de las tecnologías (especialmente en línea) y la globalización creciente, al tiempo que se mantiene la neutralidad tecnológica del marco jurídico"[11].

6 Ver resultados de la Consulta a las Partes Interesadas y Evaluación de Impacto: http://eurlex.europa.eu/LexUriServ/LexUriServ.douri=COM:2012:0011:FIN:ES:PDF. Pág. 5.

7 Ver Ficha Financiera Legislativa. Objetivos Estratégicos. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do uri=COM:2012:0011:FIN:ES:PDF. Pág. 92.

8 Ver Ficha Financiera Legislativa. Objetivos Estratégicos. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do uri=COM:2012:0011:FIN:ES:PDF. Pág. 92.

9 Ver Resultados de la Consulta a las Partes Interesadas y Evaluación de Impacto. lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF. Pág. 3.

10 Ver Ficha Financiera Legislativa. Objetivos Estratégicos. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do uri=COM:2012:0011:FIN:ES:PDF. Pág. 95.

11 Ver Resultados de la Consulta a las Partes Interesadas y Evaluación de Impacto. En: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF. Págs. 3 y 4.

En cambio, "la actual fragmentación de la protección de datos personales en la Unión, ha sido el blanco de duras críticas, especialmente por parte de los operadores económicos, que solicitaron una mayor seguridad jurídica", así como la complejidad de las normas en materia de transferencias internacionales lo que constituye un impedimento para el funcionamiento más fluido del mercado[12].

3. La protección de datos en un mundo globalizado

3.1. Definiciones

En la reforma se han introducido nuevos conceptos, así como también se han re-definido otros,- que si bien ya estaban incluidos en la actual Directiva 46/95/CE-, ahora se precisan con el objetivo de adaptar su significado a los cambios ya mencionados.
Es así que en el art. 4° se define a:

a) Interesado: Toda persona física identificada o que pueda ser identificada, directa o indirectamente. La novedad en este sentido, es que se incluyen también como datos personales a los datos de localización o el identificador en línea o dirección IP (Art. 4.1).

b) Violación de datos personales: Toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma (Art. 4.9). Recordemos además que estas brechas de seguridad deben ser comunicadas en un plazo establecido en el reglamento (24 horas).

c) Normas Corporativas Vinculantes (BCR´s): Políticas de protección de datos personales asumidas por un responsable o encargado de tratamiento establecido en el territorio de un Estado de la UE para las transferencias o conjunto de transferencias de datos a un responsable o encargado del tratamiento en uno o más países terceros dentro de un grupo de empresas (Art. 4.17).

d) Establecimiento principal: Respecto al responsable, éste será el lugar de la UE donde se adopten las decisiones principales en cuanto a los fines, condiciones y medios de tratamiento. Si este tipo de decisiones no se adopta en la UE, será el lugar en el que se tienen las principales actividades de tratamiento. En lo que respecta al encargado de tratamiento, se entiende que es el lugar de su administración central en la UE (Art. 4.13).

e) Datos genéticos: Todos los datos relativos a las características de una persona, que sean hereditarias o adquiridas, durante el desarrollo prenatal temprano (Art. 4.10).

f) Datos biométricos: Cualquier dato relativo a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos (Art. 4.11).

g) Datos de salud: Cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona. Se amplía el alcance del concepto, incluyéndose como datos de salud por ejemplo la información contenida en los recibos de pago realizados al médico, también el número que identifique a determinado socio con su mutualista o con su seguridad social (Art. 4.12).

h) Consentimiento: Cualquier manifestación de voluntad otorgada de forma específica, libre, informada y explicita, a través de la cual el interesado expresa su acuerdo con el tratamiento de datos (Art. 4.8).

12 Ver Resultados de la Consulta a las Partes Interesadas y Evaluación de Impacto. En: http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF. Págs. 3 y 4. (Página visitada el 3 de setiembre de 2013)

i) Niños: Todas las personas menores de 18 años (Art. 4.18). Esta definición tiene su fundamento en lo establecido en la Convención de Derechos del Niño de 1989.

3.2. Consentimiento: modificaciones y alcance

A partir de la nueva reglamentación sólo se admite el consentimiento expreso, y ello significa un cambio importante respecto a lo que sucede actualmente donde también se admite el consentimiento tácito (art.7).

Por otra parte, se considera lícito el tratamiento de datos sin el consentimiento del interesado, cuando el tratamiento es necesario para cumplir con una misión de interés público o es inherente al ejercicio del poder público, o cuando éste tenga por finalidad la realización de un interés legítimo perseguido por el responsable del tratamiento, y siempre y cuando no se vulneren los intereses o derechos fundamentales de los interesados, en particular si se trata de un niño (art 6.1.f).

En los casos en que sea necesario que el interesado otorgue su consentimiento en el contexto de una declaración escrita, el mismo debe ser otorgado de forma diferenciada respecto a las demás cuestiones relativas a la relación que se mantiene (art 7.2). Además, el consentimiento no habilita el tratamiento de los datos personales cuando exista un claro desequilibrio entre la posición del interesado, y la del responsable del tratamiento (7.4).

Por otra parte, el consentimiento de los menores de 13 años solo será válido si es otorgado por sus padres o representantes legales (art 8.1). Se agrega a su vez, que el responsable del tratamiento deberá realizar todos los esfuerzos razonables para obtener el consentimiento en forma verificable, considerando especialmente el uso de las tecnologías disponibles. Este cambio impactará directamente en el uso de las redes sociales.

Con respecto a las actividades de marketing, se establece que para recoger y tratar datos destinados a ese fin, será necesario obtener el consentimiento del interesado. En este sentido se adopta el criterio del Dictamen 5/2004 del Grupo de Trabajo del Artículo 29[13].

3.4. Tratamiento de datos especiales

El nuevo reglamento dedica buena parte de su articulado a regular el tratamiento de ciertos datos que deben ser especialmente protegidos. En este sentido se establece que cuando el tratamiento refiera a datos de salud, datos biométricos o datos genéticos, deberá realizarse un "Informe de Impacto de Privacidad" por parte del responsable y del encargado del tratamiento (art. 33).

A su vez, como existe en la propuesta una clara intención de reforzar la protección de los datos de los menores de edad, también establece la obligación de realizar este informe cuando se traten datos personales de personas menores de edad.

Por otra parte, cuando el tratamiento refiera a la oferta directa de servicios de la sociedad de la información dirigidos a niños menores de 13 años, éste sólo será lícito si el consentimiento ha sido dado o autorizado por el padre o tutor (8.1).

Por último, entre las excepciones que habilitan a tratar datos especialmente protegidos, se encuentra la que indica que esos datos hayan sido hecho públicos por parte del propio interesado. Se agrega a su vez, que para recolectar los datos deberá informarse al titular acerca del período de tiempo en que se tendrán almacenados, así como del derecho que posee el titular a entablar una acción ante la Autoridad de Control correspondiente, aportándole a tales efectos la dirección de la misma.

13 Ver http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_es.pdf (Página visitada el 7 de junio de 2012).

4. Reconocimiento de nuevos derechos

La propuesta refuerza el control que se ejerce sobre los datos, tanto a través de las características que se otorgan al consentimiento, como al derecho a recibir información, -en particular cuando esas actividades afecten a niños-; mejora los medios que permiten ejercer tales derechos; el aumento de la independencia y las competencias otorgadas a las autoridades de control y las medidas de seguridad que se exigen, entre otros aspectos.

A su vez, a los derechos ya reconocidos en la legislación europea, se agregan otros que mencionaremos especialmente como el Derecho al Olvido, a la Portabilidad de los Datos y a presentar una reclamación ante una autoridad de control de cualquier estado miembros de la UE.

4.1. Derecho al Olvido

Este derecho, -que es en realidad una aplicación del actual derecho a la cancelación u oposición-, enfatiza en que los responsables del tratamiento están obligados a suprimir los datos de los interesados que así lo soliciten, sobre todo cuando los mismos han sido proporcionados cuando éste era menor de edad (Art. 17.1).

Ello significa, que si los datos se han hecho públicos, por ejemplo a través de internet, el responsable deberá eliminar los links o documentos donde figuren los mismos. En este sentido, algunos especialistas advierten que esta redacción es confusa, pero que sería razonable interpretar que dicha obligación recae sobre el responsable que primero publicó esos datos personales, aunque los mismos luego hayan sido recogidos o publicados en otros sitios de internet, por lo cual será quien debe dirigirse a éstos para pedir la cancelación[14].

Por otra parte, si los datos se han hecho públicos hay que ver si ello "afecta a las actuales fuentes de acceso público, ya que uno de los medios que se considera para esa publicidad es que se hayan publicado en internet. En consecuencia, podría valorarse la posibilidad de que internet pase a ser una fuente de acceso público. En cierta forma, se bloquea el derecho al olvido sobre los medios de comunicación digitales, ya que el art. 15 recoge como una de las excepciones para no proceder a la cancelación que los datos personales se hayan publicado en base al ejercicio de la libertad de expresión"[15].
En definitiva, se regula el derecho en virtud del cual los usuarios pueden exigir a los proveedores de servicios de Internet que borren sus datos, cuando éstos dejan de ser necesarios para los fines para los que se recabaron o cuando el cliente se dé de baja.

En reciente entrevista, el nuevo director de la Agencia Española de Protección de Datos (AEPD), José Luis Rodríguez, explica el alcance de este derecho al olvido, y cómo se puede ejercer de una forma efectiva. En este sentido señala que "No tiene nada que ver con un derecho a reescribir la historia, un derecho a refutar la memoria o un derecho de alterar las bases documentales, ya sean textos de boletines oficiales, ya sean hemerotecas. Básicamente, ningún derecho tiene un carácter absoluto, ha de buscarse un equilibrio con otros derechos, principios o intereses con los que puede colisionar. (...) Por ello tiene un alcance diferente en función de sobre qué se aplica. Es mayor sobre los datos que nosotros hemos entregado a un tercero; es el caso, por ejemplo, de la información personal que

14 Ver comentarios al borrador de Reglamento de Protección de Datos de la Unión Europea. Dr. Javier Sempere. Asesor de la Agencia de Protección de Datos de la Comunidad de Madrid.
http://www.madrid.org/cs/Satellitec=CM_Revista_FP&cid=1142670244190&esArticulo=true&idRevistaElegi=1142664149793&language=es&pagename=RevistaDatosPersonales%2FP%2Fhome_RDP&siteName=RevistaDatosPersonales (Página visitada el 1 de junio de 2012).

15 Ver Comentarios al borrador de Reglamento de Protección de Datos de la Unión Europea. Dr. Javier Sempere. Asesor de la Agencia de Protección de Datos de la Comunidad de Madrid.
http://www.madrid.org/cs/Satellitec=CM_Revista_FP&cid=1142670244190&esArticulo=true&idRevistaElegi1142664149793&language=es&pagename=RevistaDatosPersonales%2FP %2Fhome_RDP&siteName=RevistaDatosPersonales (Página visitada el 1 de junio de 2012).

hemos proporcionado en un blog o, el caso más significativo, esa información que ponemos en una red social"[16].

4.2. Derecho a la Portabilidad de los Datos

También se conferirá a las personas el derecho explícito a retirar sus datos (por ejemplo fotos o una lista de amigos) de una aplicación o un servicio y transferirlos a otra aplicación o servicio sin que los responsables del tratamiento puedan bloquearlo[17].

Es en definitiva, el derecho que posee el titular a obtener del responsable del tratamiento una copia de los datos conservados, y la libertad de transferirlos de un proveedor de servicio a otros sin trabas porque son sus datos y por ende le pertenecen.

En definitiva, cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tendrá derecho a obtener del responsable del tratamiento, una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos[18].

Además, cuando se le hayan facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos o cualquier otra información que haya facilitado y se conserve en un sistema de tratamiento automatizado, a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento[19].

4.3. Derecho a reclamar ante las autoridades de control

Sin perjuicio de los recursos administrativos o judiciales disponibles, todo interesado que considere que el tratamiento de sus datos ha vulnerado el reglamento, tiene derecho a presentar su reclamo ante una autoridad de control de cualquier Estado que forme parte de la UE.

También pueden hacerlo los organismos, organizaciones o asociaciones, debidamente constituidas, que protejan los derechos o intereses de las personas afectadas en la protección de sus datos personales ya sea en representación de éstas o independientemente de las mismas.

16 Ver www.datospersonales.org. Entrevista a José Luis Rodríguez, Director de la AEPD. "El 'olvido digital' en España es una búsqueda de equilibrio". 25/02/2012 Fuente: El Mundo (Página visitada el 1 de junio de 2012).

17 Ver www.datospersonales.org. Bruselas regulará el derecho al olvido en las redes sociales. 04/05/2011 Fuente: nuevastecnologias.com (Página visitada el 1 de junio de 2012).

18 Ver http://www.datospersonales.org/ Actualidad Normativa: INTERNACIONAL (Página visitada el 1 de junio de 2012).

19 Ver http://www.datospersonales.org/ Actualidad Normativa: INTERNACIONAL (Página visitada el 1 de junio de 2012).

5. Obligaciones atribuidas

5.1. A los responsables

En cuanto a la rendición de cuentas de quienes son responsables o encargados de tratamiento, en la actual reforma propuesta para la UE se establecen una serie de obligaciones específicas:

- Formar al personal que trata los datos personales.
- Notificar las brechas de seguridad o violaciones graves a las Autoridades de Control (dentro de las 24 horas), avisarle a los damnificados y/o hacerlas públicas.
- Realización de informes de impacto de privacidad cuando se maneje un gran volumen de datos o datos especialmente protegidos (descripción del tratamiento, valoración del riesgo, medidas de seguridad y mecanismos adoptados para la adecuada protección de los datos).
- Documentar las diversas actuaciones que tengan relación con el tratamiento de datos personales. Conservar esta documentación que puede ser requerida por la Autoridad de Control.
- Poseer una adecuada política de seguridad de la información (en base a los riesgos, la naturaleza de los datos, y los costos de implementación).
- Designar a un responsable de protección de datos cuando ello corresponda (organismo públicos y empresas de más de 250 empleados).
- Informar debidamente a los titulares de los datos (sobre el período en que se almacenarán, la forma en que puede ejercer sus derechos o se puede denunciar, si se van a realizar transferencias a países adecuados, entre otros elementos).
- Obtener el consentimiento en forma expresa, aún para las actividades de marketing.

5.2. A los encargados del tratamiento

El encargado de tratamiento también tiene obligaciones, a saber:

- El personal que emplea debe estar sometido al deber de secreto en forma estatutaria.
- La relación con el responsable debe estar documentada, no sólo mediante un contrato sino con instrucciones y obligaciones específicas.
- Documentar las actuaciones relacionadas con el tratamiento de datos personales.
- Realizar informes de impacto de privacidad cuando corresponda.

Todas estas obligaciones que deben adoptar tanto el responsable como el encargado de tratamiento, podrán ser objeto de una auditoría independiente, tanto interna como externa. No sólo se podrán auditar los aspectos de seguridad de la información, sino los aspectos jurídicos del tratamiento (calidad, cesiones, etc.).

También se introduce la idea de otorgar un certificado de calidad a los servicios, productos y procesos que cumplan con la normativa de protección de datos personales. Debido a ello, la Comisión Europea deberá crear estándares técnicos de certificación y promoverá la entrega de estos sellos.

6. Funcionamiento y control en el nuevo sistema

6.1. Las Autoridades Nacionales de Protección de Datos

Se establece que cada Estado debe disponer de una o más autoridades públicas de control, en caso de que sean más de una, éste deberá designar a aquélla que actuará como punto de contacto único, estableciendo también un mecanismo para garantizar el cumplimiento por parte de las demás autoridades de las normas sobre coherencia en la aplicación del reglamento.
Funciones a cargo de las mismas:

- Supervisar la aplicación de la nueva normativa y su aplicación coherente en toda la UE. Para ello, entre otras cosas, deberá asesorar, conocer sobre las consultas y reclamaciones presentadas, investigar y resolver en un plazo razonable; cooperar y compartir información con otras autoridades de control; hacer seguimiento de las novedades de interés y que incidan en la protección de datos; autorizar operaciones de tratamiento, emitir dictámenes sobre códigos de conducta y aprobar normas corporativas vinculantes.
- Cooperar entre sí y con la Comisión. Para ello podrán llevar a cabo actividades de investigación conjuntas, tareas de investigación conjuntas y medidas represivas conjuntas. También deberán facilitarse información útil entre sí y se prestarán asistencia mutua, sin demoras y a más tardar en un plazo de un mes tras haber recibido la solicitud. Si no se responde dentro de este plazo, la autoridad solicitante será competente para adoptar una medida provisional en el Estado de la autoridad omisa y someter el caso al Consejo Europeo de Protección de Datos. Por otra parte se establece que, no se podrá negar la información a menos que no fuera competente para dar curso a la solicitud recibida, o el hecho de atender la misma fuera incompatible con las disposiciones del reglamento.
- Actuar con total independencia en el ejercicio de sus funciones, por lo cual sus miembros no solicitarán ni aceptarán instrucciones de nadie, se abstendrán de cualquier acción o participación en actividad profesional que sea incompatible con sus funciones, ya sea remunerada o no, así como deberán ser elegidos por sus cualificaciones, experiencia y aptitudes y cesados cuando las mismas ya no se reúnan.
- Elaborar un informe anual sobre sus actividades que será presentado en el parlamento nacional y se pondrá a disposición del público, de la Comisión y del Consejo Europeo de Protección de Datos.

6.2. Mecanismo de coherencia para la actuación conjunta

El artículo 57 introduce un mecanismo de coherencia para garantizar la uniforme aplicación en las operaciones de tratamiento de datos que pueden afectar a interesados de varios Estados miembros. El artículo 58 establece los procedimientos y condiciones para un dictamen del Consejo Europeo de Protección de Datos. El artículo 60 se refiere a las decisiones de la Comisión que obligan a la autoridad competente a suspender su proyecto de medida cuando sea necesario para garantizar la correcta aplicación del Reglamento[20].

El mecanismo podrá ser solicitado por éstas, la Comisión o el Consejo Europeo de Protección de Datos, sobre todo en aquellos casos en que una autoridad de control no presente un proyecto con la medida que aplicará, o no coopere como se establece en el reglamento.

De todas formas, antes de adoptar cualquiera de las medidas dispuestas en la nueva normativa (art. 58.2), las autoridades de control deben comunicar tal proyecto al Consejo Europeo de Protección de Datos.

20 Fuente: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF (Página visitada el 3 de setiembre de 2013)

Las autoridades de control y la Comisión deberán comunicar por vía electrónica y en formato normalizado, toda información útil, en particular, el resumen de los hechos y el proyecto de medida y su fundamento. El Consejo Europeo por su parte, emitirá un dictamen sobre el asunto si así se decide por mayoría, o si una autoridad de control o la Comisión lo solicitaren. La autoridad o las autoridades de control involucradas lo tendrán y en el plazo de dos semanas luego de recibido, deberán comunicar al Presidente del Consejo Europeo y a la Comisión si mantienen o modifican su proyecto de medida.

En casos excepcionales, cuando una autoridad de control estime que es pertinente intervenir en forma urgente para proteger los derechos de los interesados, podrá adoptar medidas provisionales por determinado plazo, comunicando sin demora a la Comisión y al Consejo Europeo.

6.3. Consejo Europeo de Protección de Datos

Se crea el Consejo Europeo de Protección de Datos que estará compuesto por el Director de una autoridad de control de cada Estado de la UE y por el Supervisor Europeo de Protección de Datos. Si en un Estado hay varias autoridades de control, se designará al director de una de ellas como representante común.
La Comisión por su parte, tendrá derecho a participar en todas las actividades y reuniones de este nuevo órgano, que tendrá total independencia en su actuación y cuenta con una serie de tareas asignadas (art. 66), tales como:

a) Asesorar a la Comisión sobre cuestiones relacionadas a la protección de datos personales de la UE, en particular sobre las propuestas de modificación al reglamento.
b) Examinar, a iniciativa propia o a instancia de uno de sus miembros o de la Comisión, las cuestiones relativas a la aplicación del reglamento, emitir directrices, recomendaciones y mejores prácticas. Posteriormente debe analizar cómo se aplican las mismas en la realidad.
c) Emitir dictámenes sobre los proyectos de decisión de las autoridades de control con arreglo a lo establecido en el mecanismo de coherencia ya analizado.
d) Promover la cooperación y los intercambios bilaterales y multilaterales de información y prácticas entre las autoridades de control.
e) Promover programas de formación, así como el intercambio entre los funcionarios de las diferentes autoridades de control.
f) Promover el intercambio de conocimientos y documentación sobre la legislación y las prácticas en materia de protección de datos personales.

Por otra parte, cuando la Comisión solicita el asesoramiento del Consejo podrá fijar un plazo para la prestación de ese asesoramiento, teniendo presente la urgencia del asunto.

A su vez, este órgano deberá informar periódicamente a la Comisión sobre el resultado de sus actividades, así como elaborará un informe anual sobre la situación en materia de protección de datos personales. El informe debe incluir el examen realizado a la aplicación práctica de las directrices, recomendaciones y mejores prácticas emitidas que además será público.

El Consejo elegirá de entre sus miembros, a un Presidente y dos Vicepresidentes que durarán 5 años en su cargo, pudiendo ser renovables. Uno de los Vicepresidentes será el Supervisor Europeo de Protección de Datos, a menos que éste haya sido elegido Presidente.

7. A modo de conclusión

Esta reforma muestra que la tendencia es ir hacia el aumento de las obligaciones y hacia una rendición de cuentas de los responsables y encargados de tratamiento (accountability), poniendo énfasis en la formación, capacitación, prevención, así como en el control posterior y eventual de las autoridades de cada país. En este sentido, la Comisión Europea también tendrá la facultad de establecer protocolos y procedimientos pudiendo existir especificaciones para ciertos sectores o atendiendo a la situación de cada responsable.

Con los objetivos ya señalados, se establecen una serie de obligaciones que apuntan a reforzar la responsabilidad y la rendición de cuentas de cada responsable ante una eventual auditoría por parte de las autoridades de control de cada país.

Se propone además que el responsable y el encargado de tratamiento, así como el representante del responsable si lo hubiera, deberán poner a disposición de la autoridad de control, a solicitud de ésta, toda la información relacionada con el tratamiento de datos personales que realizan.

Es por ello, que los responsables y encargados de tratamiento (menos las personas físicas que traten datos personales sin un interés comercial y empresas y organizaciones que empleen menos de 250 personas y traten datos personales solo como actividad accesoria a sus actividades principales), deberán conservar dicha información pues ésta puede ser solicitada y auditada por la Autoridad de Control en cualquier momento.

CAPITULO XVI

PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA. AMPLIANDO HORIZONTES

Prof. Dra. Esc. María José Viega
Dra. Flavia Baladán

PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA. AMPLIANDO HORIZONTES

Prof. Dra. Esc. María José Viega
Dra. Flavia Baladán

1. Introducción

El nacimiento y desarrollo del derecho a la protección de datos personales se formaliza en el seno europeo a partir del último tercio del siglo pasado, mediante normas supranacionales y de derecho interno de cada país.

Estas normas permitieron que la Unión Europea avanzara rápida y considerablemente en la construcción de un sistema garante de los datos personales coherente y armonizado, que poco a poco ha sido internalizado por otros continentes como un derecho autónomo.

América Latina no ha estado ajena a la tuición de este derecho. Con base constitucional o sin ella, numerosos países fueron progresivamente regulando el derecho a la protección de datos a través de normas locales o nacionales, en conjunción con las tradiciones jurídicas propias (habeas data, amparo).

América Latina ha tenido importantes avances en protección de datos, los cuales cobran relevancia en los últimos años y que surgen con claridad del análisis normativo que se realizará en los próximos puntos. Nos encontraremos así con países adecuados a la normativa europea, países que tienen ley y órgano de control y aquéllos que solo tienen una normativa constitucional o legal.

Durante la década del 70 se realizó el desarrollo europeo en la materia, siendo inexistente en América Latina, donde comenzó a plantearse el tema en la década del 80.

El primer país en incorporar disposiciones específicas fue Guatemala en 1985, seguida por Nicaragua en 1987 y es simbólica la inclusión en la Constitución Brasileña 1988 ya que consagra el Habeas Data.

La Acción Judicial de Habeas Data, como máxima garantía para las personas, ha sido consagrada a nivel constitucional en muchos países de la región. Tuvo su origen en la salida de las dictaduras militares y fue concebida como una herramienta para permitir al ciudadano conocer directamente y, en caso necesario, rectificar las informaciones que sobre él se almacenaban en bases de datos.

Sin lugar a dudas el habeas data como acción constitucional garantiza la fuerza de la norma y su carácter cautelar, la rapidez. Una estructura como ésta no es equivalente a las soluciones comparadas. Uruguay la ha incorporado a nivel legal. ¿Es el habeas data una "tercera vía" alternativa a los modelos de protección de datos en la Unión Europea y Estados Unidos? Entendemos que no.

Los desarrollos de los distintos países, si bien se han inspirado en la normativa de la Unión Europea, presentan particularidades. Por otra parte, las motivaciones han sido diferentes, a modo de ejemplo, en el caso de Uruguay fue el desarrollo del gobierno electrónico, cobrando importancia el derecho humano frente al intercambio automatizado de información entre los organismos del Estado.

2. Argentina

En Argentina se inicia el camino a la protección de los datos personales a partir de la reforma constitucional de 1994 en la que se incluye el Habeas Data. Con posterioridad, durante el año 2000, entró en vigor la Ley Nº 25.326, la que fue reglamentada en el 2001 por el Decreto Nº 1.558.

El objeto de la Ley es la protección integral de los datos personales asentados en archivos, registros, banco de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados.

Dentro de los principales temas que regula la ley, se encuentra la definición de datos personales, entendidos éstos como la información de cualquier tipo referida a personas físicas o de existencia ideal, determinadas o determinables. Reconoce como datos sensibles aquéllos que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Es de destacar que la Ley indica como principios generales relativos a la protección de datos personales: la licitud, la calidad de los datos, el consentimiento, la información, la categoría de datos, los datos relativos a la salud, la seguridad de los datos, el deber de confidencialidad, la cesión, y la transferencia internacional.

También regula los derechos de las personas, a saber: información, acceso, contenido de la información, rectificación, actualización o supresión.

Se debe mencionar que el órgano de control creado por la Ley es la Dirección Nacional de Protección de Datos Personales, la cual posee facultades sancionatorias e independencia funcional.

Por último, cabe hacer referencia que Argentina fue el primer país en ser declarado adecuado a la Directiva 95/46/CE, mediante Decisión de la Comisión de las Comunidades Europeas, el 30 de junio de 2003.

3. Bolivia

En Bolivia la protección de datos personales tiene regulación constitucional. La Ley de Necesidad de Reformas a la Constitución, de 1º de agosto de 2002, agregó los artículos 21, 130 y 131.

Según el primero de ellos, las bolivianas y los bolivianos tienen derecho, entre otros, a la privacidad, intimidad y a la propia imagen.

En los artículos 130 y 131 se regula la Acción de Protección de Privacidad, la cual es de contenido similar a un Habeas Data. Procede cuando una persona individual o colectiva, crea estar indebida o ilegalmente impedida de conocer, objetar la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación.

4. Brasil

En Brasil, la protección de datos tiene reconocimiento constitucional. Es así que el artículo 5º de la Constitución de la República, de 1988, reconoce el "Habeas Data" a los efectos de asegurar el conocimiento de informaciones relativas a la persona que consten en registros o banco de datos de entidades gubernamentales o de carácter público, o para la rectificación de datos cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.

Danilo Doneda expresa respecto de esta acción que se trata de una "idea muy ligada con la libertad informática pero con una formulación en tanto acción judicial, como un amparo cuya pretensión fue posibilitar a las personas que tuvieron problemas con el amparo militar, el acceso a sus datos o a los datos de sus familiares, no tratándose propiamente de una herramienta para la protección de datos" [1].

5. Chile

En Chile, la Constitución de 1980 en su artículo 19, establece que se asegura a todas las personas el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

El 28 de agosto de 1999, se aprobó la Ley Nº 19.628, en el entendido de que el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a los extremos de la Ley.

Es de destacar que la Ley establece que son datos personales los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Dentro de éstos, los datos sensibles son definidos como aquellos datos personales que se refieren a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

También en este país se regulan los derechos de los titulares de los datos personales. Éstos son los derechos de información, modificación y eliminación, estableciéndose la posibilidad de bloquear los datos.

La Ley indica que el órgano rector en la materia es el Servicio de Registro Civil e Identificación.

Por último, se debe mencionar que la Ley de referencia fue reglamentada por el Decreto Nº 779/000, que regula el Registro de Bancos de Datos Personales a cargo de los Organismos Públicos.

6. Colombia

En Colombia se registra una evolución normativa interesante. Es así que el artículo 15 de la Constitución incorporó el Habeas Data desde el año 1991. En el año 2008 se legisló el Habeas Data financiero y crediticio. Además, en el año 2009 se consagraron tipos penales de protección de datos.

Posteriormente, el 17 de octubre de 2012, se aprueba la Ley Nº 1581, que tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las

1 Resumen del Plenario V – Protección de Datos Personales en América Latina. Ampliando horizontes en http://privacyconference2012.org/espanol/programa/temas/plenario-iv-2 (Página visitada el 5 de setiembre de 2013).

informaciones que se hayan recogido sobre ellas en bases de datos o archivos y los demás derechos, libertades y garantías constitucionales.

Según estas norma, dato personal es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Además, se indica que son datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como el origen racional o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político, o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

La Ley indica como principios para el tratamiento de los datos personales los siguientes: legalidad en materia de tratamiento de datos, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Por otra parte, establece que los titulares de los datos tienen derecho a conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados de tratamiento; solicitar prueba de la autorización otorgada al responsable; ser informado respecto del uso que le ha dado a sus datos personales; presentar quejas o infracciones a lo dispuesto en la ley; revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales y a acceder en forma gratuita a sus datos personales.

Por último, la Ley indica como autoridad de protección de datos, la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales.

7. Costa Rica

En Costa Rica el derecho partió desde normas individuales dictadas aisladamente hasta la interpretación jurisprudencial, donde en forma paulatina se fue reconociendo el derecho a la protección de datos y el mecanismo de protección de Habeas Data[2].

Costa Rica cuenta desde el año 2012 con una Ley de Protección de Datos Personales cuyo número es 8.968. Esta Ley tiene por objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales. Concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Para la Ley, un dato personal es cualquier dato relativo a una persona física identificada o identificable. Dentro de éstos, se encuentran los datos sensibles entendidos como la información relativa al fuero íntimo de la persona, como por ejemplo, los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

La Ley reconoce como principios la autodeterminación informativa, el previo consentimiento informado y la calidad de la información. También indica que son derechos de las personas, el acceso a la información y el derecho de rectificación.

En Costa Rica, el órgano competente en la materia es la Agencia de Protección de Datos de los Habitantes. Se trata de un órgano con desconcentración máxima adscrito al Ministerio de Justicia y Paz, con las atribuciones de llevar un registro de bases de datos, aplicar sanciones, divulgar el derecho e inspeccionar y sancionar a los infractores.

2 Resumen del Plenario V – Protección de Datos Personales en América Latina. Ampliando horizontes en http://privacyconference2012.org/espanol/programa/temas/plenario-iv-2 (Página visitada el 5 de setiembre de 2013).

8. Ecuador

En Ecuador también encontramos reconocido a nivel constitucional el derecho a la intimidad personal y familiar en el artículo 23 numeral 8º de la Constitución de la República de 1996.

Además, el artículo 94 regula el Habeas Data, en el sentido de que toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en Entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.

9. El Salvador

En El Salvador encontramos un reconocimiento básico en la materia, en tanto en el artículo 2º de la Constitución de 1983 se indica que toda persona tiene derecho a la intimidad personal y familiar, y a la propia imagen.

10. Guatemala

Similar situación encontramos en Guatemala donde el artículo 31 de la Constitución de 1985 expresa que se tiene derecho al acceso a archivos y registros estatales, así como a corrección, rectificación y actualización. También indica que quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.

11. Honduras

En Honduras, el artículo 76 del Decreto Legislativo Nº 381 de 2005, reformó el Capítulo I del Título IV de la Constitución reconociendo el Habeas Data como el derecho a acceder a la información sobre sí mismo o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.

12. México

El primer antecedente en materia de protección de datos personales en México lo encontramos en los artículos 6º y 16 de la Constitución. En estas normas, se establece que la información sobre la vida privada y los datos personales en los archivos gubernamentales serán protegidos conforme a las leyes.

En el año 2002, se incluyen algunos artículos relativos a la protección de datos en la Ley de Transparencia y Acceso a la Información Pública. En esta norma se reconocía el derecho de acceso y rectificación de los datos personales.

El 27 de abril de 2010, se dicta la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, cuyo objeto es la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efectos de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Según esta norma, es dato personal cualquier información concerniente a una persona física, identificada o identificable. Esta norma, al igual que sucede en otros países, identifica como datos

sensibles aquéllos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo para éste, como por ejemplo, el origen racial o étnico, el estado de salud presente y futura, entre otros.

La norma establece que, para el tratamiento de datos personales por parte de responsables, se deben observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

También reconoce como derechos de los titulares de datos personales, el derecho de acceso, la rectificación, cancelación y oposición.

Las competencias en la materia fueron asignadas al Instituto Federal de Acceso a la Información y Protección de Datos. Es de destacar que este organismo tiene poderes de información, de prevención, de regulación, de investigación y resolución.

13. Nicaragua

En Nicaragua, el artículo 26 de la Constitución de la República consagra que toda persona tiene derecho a su vida privada y la de su familia, así como a conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.

El 27 de marzo de 2013 se aprueba la Ley Nº 787 de Protección de Datos Personales. Esta norma tiene como finalidad la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efectos de garantizar el derecho a la privacidad personal y familiar, y el derecho a la autodeterminación informativa.

La norma de referencia determina que dato personal es aquella información sobre una persona natural o jurídica que la identifica o hace identificable. Distingue los datos personales informáticos estableciendo que son aquellos datos personales tratados a través de medios electrónicos automatizados. También expresa que datos sensibles son aquéllos que revelen el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicas financieros, así como información crediticia y financiera, y cualquier otra información que pueda ser motivo de discriminación.

La Ley reconoce como derechos del titular de datos, el de solicitar información y de modificar los datos.

También es de destacar que crea la Dirección de Protección de Datos Personales como órgano rector, con las competencias de control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada.

14. Paraguay

En Paraguay, el artículo 135 de la Constitución Nacional de Paraguay, de 20 de junio de 1992, incorpora a su ordenamiento jurídico el Habeas Data. En ella se establece que toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Además, regula que se podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

Además, en materia de protección de datos, se cuenta con la Ley Nº 1.682, de 16 de enero de 2001,

que reglamenta la información de carácter privado. Por su parte, la Ley Nº 1.969, de 3 de setiembre de 2002, modifica, amplía, y deroga varios artículos de la Ley Nº 1.682.

15. Perú

En Perú, la Constitución de la República de 1993, en su artículo 200 numeral 3º dentro de las "Garantías Constitucionales" reconoce la Acción de Habeas Data. Ésta procede contra el hecho u omisión, parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que refiere el artículo 2º inciso 5º y 6º del mismo cuerpo normativo. A saber: a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública en el plazo legal, y que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

El 3 de julio de 2011, aprobó la Ley Nº 27.933, con el objeto de garantizar el derecho fundamental a la protección de datos personales, previsto en la Constitución.

Según la Ley, son datos personales toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. También identifica como datos sensibles, en el mismo sentido que en otros países, los datos biométricos, el origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical e información relacionada a la salud o a la vida sexual.

La Ley regula como principios rectores los siguientes: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recursos y nivel de protección adecuado.

También sigue la misma línea que en la región en lo que concierne a los derechos de los titulares de los datos, expresando que son: el derecho a tener información del titular de datos personales, el de acceso, a impedir el suministro, oposición, tratamiento objetivo, a la tutela y a ser informado.

En el país, la autoridad nacional de protección de datos personales es la Dirección Nacional de Justicia dependiente del Ministerio de Justicia.

16. República Dominicana

El artículo 44, numeral 2°, de la Constitución de la República de 26 de enero de 2010, reconoce que toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley.

Según esta norma, el tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Expresa que se podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

Por su parte, el artículo 70 de la Constitución, reconoce una acción judicial con los mismos parámetros que una Acción de Habeas Data.

17. Uruguay

En Uruguay el marco normativo referido al derecho a la protección de datos personales se encuentra dado por el artículo 72 de la Constitución de la República de 1967, la Ley Nº 18.331, de 11 de agosto de 2008 y su Decreto Reglamentario Nº 414/009, de 31 de agosto de 2008.

El artículo 1º de la Ley Nº 18.331 indica que el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República. Según dicho artículo "**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"**. Por tanto, podemos afirmar que en Uruguay la protección de datos personales goza de reconocimiento constitucional.

En cuanto a los ámbitos subjetivo, objetivo y territorial debemos decir que abarca toda información, numérica, alfabética, gráfica, acústica, etc. Se identifica al responsable de la base como el propietario o quien decide sobre el uso del tratamiento. Al titular del dato como toda persona física determinada o determinable, incluyendo la protección a las personas jurídicas en cuanto corresponda. Las normas se aplican si el tratamiento se hace por responsable establecido en el país o usa medios en él situados.

La protección de datos personales se encuentra regulado bajo ciertos principios orientadores, a saber: respeto al orden jurídico, a los derechos humanos y la moralidad pública; veracidad de datos, finalidad específica, consentimiento previo, documentado, y gratuito; seguridad, reserva de los datos; y responsabilidad hecha valer ante la administración o ante el juez[3].

La Ley reconoce los derechos a ser informado debidamente y antes de la recolección, al acceso gratuito a toda la información que le concierne, a la rectificación, actualización, inclusión, y supresión sin cargo en 5 días hábiles, por el medio que indique; y a brindar su consentimiento para comunicación o cesión de datos, con excepciones estrictamente establecidas en la Ley [4].

Se indica un tratamiento especial para los datos sensibles, entendidos como aquéllos referidos al origen racial, étnico, preferencias políticas, creencias religiosas, afiliación sindical, salud y vida sexual.

La Ley creó la Unidad Reguladora y de Control de Datos Personales como órgano competente en la materia. Es un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), con atribuciones legales y autonomía técnica.

En Uruguay se reconoce la acción jurisdiccional de Habeas Data a todo titular al que se niegue el acceso, la rectificación, inclusión o supresión de datos en 5 días hábiles o no se le justifique la negativa.

Es de destacar que la Unión Europea, por Decisión de Ejecución de la Comisión, de 21 de agosto de 2012, declaró que Uruguay era un país adecuado de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo en lo que respecta al tratamiento de datos personales, siendo el segundo país de América Latina en lograr este mérito.

Por último, merece destacar que por Ley Nº 19.030, de 27 de diciembre de 2012, Uruguay finalizó el trámite de adhesión al Convenio Nº 108 ante el Consejo de Europa para la protección de las

3 Rotondo, Felipe. "Uruguay: Protección de Datos Personales". La Protección de Datos en la Unión Europea y América Latina del Centro Latinoamericano para las Relaciones con Europa en http://www.celare-alcue.org/eurolat/euro83.pdf (Página visitada el 5 de setiembre de 2013).

4 Rotondo, Felipe. Ob. Cit.

personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos.

18. Venezuela

En Venezuela el reconocimiento es sólo a nivel constitucional. El artículo 28 de la Constitución de la República de 1999 regula la Acción de Habeas Data. El artículo 60 del mismo cuerpo normativo consagra que **"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática"**. Por último, el artículo 281 indica que el Defensor o Defensora del Pueblo, cuenta dentro de sus atribuciones con la acción de Habeas Data.

19. Conclusiones

Luego de realizado este recorrido por las distintas normas latinoamericanas, es indudable que América Latina tiene ya un camino recorrido, si bien con un origen diferente en la consagración del habeas data, en los últimos años con una tendencia clara de seguimiento de la línea Europea de protección, considerando la privacidad como un derecho humano.

La influencia de los avances tecnológicos es sin duda un elemento determinante para la protección de la privacidad de todas las personas, que plantea diariamente nuevos desafíos, en los cuales es necesario lograr un equilibrio entre la tecnología y la protección de los datos personales, con la ayuda de herramientas jurídicas y tecnológicas.

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES