

SEMINARIO REGIONAL DE PROTECCION DE DATOS

Montevideo, Uruguay, 1- 4 de junio de 2010

La armonización entre las leyes de transparencia y los estándares internacionales de protección de datos

Dra. Esc. Prof. María José Viega^(*)

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

1. El e-gobierno como Derecho Ciudadano

La misión del gobierno electrónico o gobierno digital apunta básicamente a dos temas, el acceso a la información pública y trámites electrónicos, la transparencia, el fortalecimiento democrático, la participación ciudadana y por otro lado su proyección en la transformación del Estado, centrada esencialmente en la concreción de procesos más eficientes. Esto implica transformaciones en los procesos interinstitucionales, como por ejemplo la interoperabilidad, hay una especie de reorganización, que es nueva y tiene una finalidad diferente, ya que se visualiza a la administración pública como un todo.

Podemos hablar de gobierno electrónico como hacer portales y tendríamos muchas cintas para cortar, pero no vemos los problemas que están en la profundidad. Pongamos por ejemplo la interoperabilidad, para determinados trámites se piden testimonios de partidas de nacimiento, de matrimonio, de defunción que están en poder del Estado, con lo cual no se deberían pedir¹. Debemos entonces comenzar a visualizar al Estado, ya no desgajado, sino único y al gobierno electrónico como un derecho ciudadano, como un derecho de la persona a que el Estado no le exija lo que éste ya posee, mejorando en calidad de servicios y en eficiencia y eficacia.

Por ese motivo, la misión de AGESIC está enunciada como: “Liderar la estrategia e implementación del Gobierno Electrónico del país, como base de un Estado eficiente y centrado en el ciudadano. Impulsar la Sociedad de la Información y del Conocimiento promoviendo la inclusión y la equidad en el uso de las Tecnologías de la Información y la Comunicación”².

El concepto de Gobierno en Red o Gobierno Conectado es el resultado de la búsqueda de un Gobierno integrado, que posicione cada vez más a la tecnología como una herramienta estratégica y como un facilitador para la innovación del servicio público y el crecimiento de la productividad. El eje del Gobierno en Red es la promoción del bien público, mediante la participación de los esfuerzos creativos de todos los segmentos de la sociedad. A través del uso de las TIC, los esfuerzos del Gobierno Conectado están destinados a mejorar la cooperación entre los organismos gubernamentales. Esto permite un mejor acceso, consultas más eficientes y eficaces; mayor compromiso con los ciudadanos y una mayor participación de las partes interesadas, tanto a nivel regional como internacional³.

¹ CLASTORNIK, José. Conferencia Transparencia y Gobierno Digital. Semana Nacional de la Transparencia. México, octubre 2009.

² <http://www.agesic.gub.uy/innovaportal/v/89/1/agesic/Misión-y-Visión-.html> Página visitada el 19 de mayo de 2010.

³ <http://www.agesic.gub.uy/innovaportal/v/26/1/agesic/Gobierno-en-Red.html> Página visitada el 19 de mayo de 2010.

Este concepto de Gobierno Electrónico centrado en el ciudadano motivó la creación de la Dirección de Derechos Ciudadanos de AGESIC por la Ley N° 18.362 de fecha 6 de octubre de 2008, que en su artículo 72 establece como su cometido la atención de consultas y asesoramiento en materia de protección de datos y de acceso a la información pública.

Quiero destacar que el término ciudadano se utiliza en un sentido amplio, el cual se reitera en documentos como la Carta Iberoamericana de Gobierno Electrónico, firmada en Santiago de Chile el 10 de noviembre de 2007, que establece: “A los efectos de esta carta se entiende por ciudadano cualquier persona natural o jurídica que tenga que relacionarse con una Administración Pública y se encuentre en territorio del país o posea el derecho a hacerlo aunque esté fuera de dicho país”.

En Uruguay tenemos una agenda digital que incluyó la protección de datos, la seguridad, el acceso a la información pública. Y en cada uno de esos casos se estructuró un marco regulatorio, que cambiaron en dos años el sistema legal en estos temas. Se creó la Agencia de Gobierno Electrónico y como desconcentrados las Unidades Reguladora y de Control de Datos Personales, de Acceso a la Información Pública y de Certificación Electrónica⁴.

2. Equilibrio entre dos derechos: protección de datos y acceso a la información pública

La AGESIC impulsó la Ley de Protección de Datos Personales y Acción de Habeas Data N° 18.331 de 11 de agosto de 2008. En ese momento, el Parlamento estaba tratando el proyecto de Ley de Acceso a la Información Pública, sobre la cual le solicitaron un informe. En ese contexto la Agencia reformula el proyecto con el objetivo de compatibilizar éste con el proyecto de protección de datos.

Es de destacar que, la ley uruguaya de protección de datos personales está en concordancia con los estándares internacionales aprobados en octubre de 2009 en la Conferencia Internacional de Protección de Datos celebrada en Madrid.

El 17 de octubre de 2008 se aprueba la Ley N° 18.381 de Acceso a la Información Pública, donde en el artículo 10 se establece que se considera información confidencial los datos personales que requieren previo consentimiento informado.

Vemos entonces, la consagración de dos derechos fundamentales, siendo la protección de datos un límite al derecho de acceso a la información pública, ya que ésta puede ser solicitada sin necesidad de poseer un interés legítimo, lo que la transforma en una herramienta para acceder a datos de terceras personas. A la inversa, también el acceso implica un límite a la protección de

⁴ CLASTORNIK, José. Conferencia Transparencia y Gobierno Digital. Semana Nacional de la Transparencia. México, octubre 2009.

datos personales cuando por razones de interés público es necesario un actuar transparente.

Tenemos que tener en cuenta que toda persona es a un mismo tiempo un ser individual y social, por lo que confluyen en ella el deseo de protección de su privacidad y por otro el deseo de obtener cada vez más información, sobre todo aquella en poder de las Administraciones públicas y ésta contiene datos personales del solicitante, pero muchas veces contiene también datos de terceros.

Hay que tener en cuenta que “la búsqueda de una mayor transparencia administrativa no es un fin en sí mismo, sino un medio necesario para que se materialicen otros principios y valores constitucionales⁵.”

La más amplia accesibilidad y visibilidad, lejos de comprometer el correcto funcionamiento del aparato administrativo, refuerza su legitimidad democrática y la configuración esencialmente servicial⁶.

El Dr. Delpiazzo afirma que “el equilibrio entre el derecho a la información (y su desprendimiento, el derecho de acceso a la información pública) por una parte, y el derecho a la protección de datos personales (ubicado concéntricamente con los derechos a la intimidad a la privacidad por otra parte, aboga a favor de este último cuando existen datos personales en poder de la Administración susceptibles de ser accedidos no sólo por el titular sino por terceros”⁷.

Esta afirmación, que se comparte, se encuentra respaldada por varias razones:

1. Debe atenderse a la diferente naturaleza de la información de que se trata en uno y otro caso, no debe confundirse la información pública con los datos personales que se encuentran en los expedientes administrativos. Cuando una persona solicita información a la Administración, tendrá acceso solo a la establecida como pública por la ley, no a la clasificada como reservada o confidencial, así como tampoco a la información secreta.
2. La determinación del bien jurídico tutelado, el cual impone la reserva sobre lo íntimo de cada persona, motivo por el cual la Administración debe respetar el principio de finalidad en la recolección de los datos.
3. Debe considerarse la diversidad de fines que persigue cada derecho. La reserva de datos personales no afecta el derecho de acceso a los documentos administrativos. Pero si el acceso a la información pública no respeta los datos personales, desvirtúa su fin.

⁵ TRONCOSO REIGADA, Antonio. “Transparencia administrativa y protección de datos personales”. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales. Edita La Agencia de protección de Datos de Madrid. 2008. Página 35.

⁶ OCHS, Daniel. “Acceso a la información en poder del Estado y restricciones fundadas en la confidencialidad. Protección de Datos y Acceso a la Información Pública. Instituto de Derecho Informático. FCU, Agesic. Montevideo, marzo 2009. Página 25.

⁷ DELPIAZZO, Carlos. “A la búsqueda del equilibrio entre privacidad y acceso”. Protección de Datos y Acceso a la Información Pública. Instituto de Derecho Informático. FCU, Agesic. Montevideo, marzo 2009.

4. Es necesario determinar el contenido esencial de cada derecho impidiendo su desfiguración.

Se ha realizado un análisis teórico del equilibrio entre los derechos, pero no queremos dejar de comentar algunos casos prácticos, ya que este tema es nuestra tarea cotidiana en la Dirección de Derechos Ciudadanos, en la función de asesoramiento técnico a las Unidades Reguladoras.

Tal es su trascendencia, que la segunda resolución que adopta la Unidad de Acceso a la Información Pública (UAIP) refiere a la excepción consagrada en el artículo 10 de la Ley de Acceso.

La UAIP estableció en la Resolución N° 2/2009 de 7 de julio de 2009, motivada por la solicitud que un Consejero de la Facultad de Ciencias Económicas le hiciera a ésta para acceder a los correos electrónicos de los egresados. Se entiende que los correos electrónicos de los egresados no es información pública, cuyo fundamento es el artículo 10 de la Ley N° 18.381. Por otra parte, se tiene en cuenta la finalidad para la cual fueron recabados los correos por parte de la Facultad para la cual prestaron su consentimiento.

El solicitante recurre la Resolución N° 2/2009 por lo que la UAIP, en forma previa a la toma de una decisión, realiza una consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP), la que se expide mediante Dictamen N° 14/2009 de 25 de setiembre de 2009 estableciendo que: “la solicitud de correos electrónicos de estudiantes y egresados de las Facultades pertenecientes a la Universidad de la República, por parte de un Consejero de la misma no es conforme a derecho”.

Por tanto, el Consejo Ejecutivo de la UAIP por Resolución N° 16/2009 de 22 de octubre de 2009 resuelve confirmar la Resolución N° 2/2009.

La Resolución N° 4/2009 de 14 de julio de 2009⁸ responde a una consulta sobre la armonización de la Ley N° 18.331 y la Ley N° 18.381, en cuanto a la información que puede brindarse respecto a los concursos de oposición y mérito para la provisión de puestos de trabajo en la Administración Pública. Se distingue si la información es solicitada por un interesado y para publicarse en el sitio del organismo, debido a la obligación de transparencia activa que establece la Ley de Acceso a la Información Pública.

La Unidad resuelve recomendar que “se entregue a los concursantes toda la documentación discriminada y existente en los expedientes, con excepción de: a) aquellos datos que nada hacen a la situación evaluada por ejemplo: estados civiles, documentos de identidad, direcciones postales y electrónicas, números de teléfono, y b) datos de carácter sensible como por ejemplo las evaluaciones psicológicas”.

⁸ <http://www.informacionpublica.gub.uy/sitio/consejo-resoluciones.html> página visitada el 21 de mayo de 2010.

Respecto a las personas que no concursaron, así como a los efectos de la publicación en el sitio web, la Unidad recomienda que “se brinde la información con puntajes globales y órdenes de prelación de todos los participantes del concurso; y que en caso de solicitarse, se facilite el acceso también a los curriculum vitae de los partícipes en el concurso, con previsión de segregar u ocultar los datos que no se relacionan con la situación curricular evaluada”.

También la URCDP por Dictamen N° 2/2010 de 12 de enero de 2010 resolvió sobre este tema, en base a una consulta acerca de la información que de acuerdo a derecho debe brindar el organismo en el marco de los concursos públicos, estableciendo que:

- a) Quien participó en un concurso podrá tener acceso a toda la información que sobre su persona se haya procesado en el marco del llamado a concurso (calificación, evaluaciones, informes, etc.) una vez culminado el proceso correspondiente. A ello se añade el listado completo de participantes con su respectivo orden de prelación.
- b) El co-postulante puede acceder sobre los demás participantes, cabe consignar que debe tener acceso a nombres y calificaciones de todos quienes hubieren integrado el proceso de concurso, con las puntuaciones diferenciadas por cada rubro evaluado, por ejemplo: méritos; prueba escrita en caso de tratarse de concurso de oposición; entrevista; prueba psicológica, etc.

Asimismo, también deberá tener acceso a los datos de los curriculum vitae de los ganadores, a efectos de que el co-postulante pueda ejercer el contralor respectivo de la transparencia del concurso. En aras de esa transparencia, solo deberán brindarse aquellos datos que le permitan comparar méritos y experiencia del co-concursante. De manera que aquellos datos que no integren esta categoría, deberán ser restringidos (a título de ejemplo, datos sensibles y otros, como datos de estado civil, edad, teléfono, correo electrónico, etc.)

- c) Cualquier tercero ajeno al concurso podrá -como en la hipótesis anterior- acceder a nombres y calificaciones de todos quienes hubieren integrado el proceso concursal, con las puntuaciones diferenciadas por cada rubro evaluado (méritos, prueba escrita, entrevista, prueba psicológica, etc.) una vez que el acto administrativo que apruebe dichas puntuaciones se encuentre firme.

También el tercero ajeno al concurso podrá tener acceso a los curriculum vitae de todos quienes hayan participado, en versiones públicas, es decir, ocultando aquellos datos que no digan relación con la situación evaluada.

- d) En cuanto a la información que debe figurar en la página web del organismo como forma de garantizar la transparencia activa, al amparo de las previsiones de la Ley N° 18.381 de Acceso a la Información Pública, resulta suficiente la incorporación de los datos de quienes

integren el orden de prelación (nombres y apellidos), junto con las puntuaciones globales de las respectivas etapas.

Por otra parte, la URCDP, por el Dictamen N° 2/009 de 7 de mayo de 2009 resolvió sobre la publicación en la web, de otras actividades laborales declaradas por Inspectores del MSP, en la medida que la mentada publicación forme parte de las funciones propias del Organismo y la finalidad perseguida sea la transferencia en la gestión. De lo contrario será necesario recabar el previo consentimiento informado de acuerdo a lo establecido en el artículo 9 de la Ley de Protección de Datos.

3. Nuevo marco institucional

Las Leyes N° 18.331 y N° 18.381 crearon un nuevo marco institucional, creando las unidades ya referidas, existiendo un contexto relacional, quizá con una perspectiva espejada entre la institucionalización de la protección de datos y el derecho de acceso a la información pública.

Ambas Unidades son órganos desconcentrados de Agesic. En el artículo 31 de la Ley N° 18.331 se dispone que la Unidad Reguladora y de Control de Datos Personales estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de la AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso.

Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico.

Según lo dispuesto por el artículo 32 de la citada Ley, el Consejo Ejecutivo de la URCDP funcionará asistido por un Consejo Consultivo, que estará integrado por cinco miembros:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo que no podrá ser un legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica.

- Un representante del área privada que se elegirá en la forma establecida reglamentariamente.

Dicho Consejo funcionará presidido por el presidente de la URCDP. Sus integrantes durarán cuatro años en sus cargos y sesionarán a convocatoria del Presidente de la URCDP o de la mayoría de sus miembros. El mismo podrá ser consultado por el Consejo Ejecutivo sobre cualquier asunto de su competencia y deberá ser consultado por éste cuando ejerza potestades de reglamentación.

Esta estructura se encuentra replicada en la Ley de Acceso a la Información Pública, con la diferencia que el Consejo Consultivo está integrado por:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, la que no podrá ser un legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica.
- Un representante del sector privado, que se elegirá en la forma establecida reglamentariamente.

La forma de concebir el sistema organizativo quizá pueda parecer un poco extraño en una primera instancia, pero tiene una lógica de funcionamiento que ha demostrado ser exitosa en los hechos. Las decisiones de Protección de Datos y Acceso a la Información Pública son tomadas por Consejo Ejecutivos independientes, pero vinculados operativamente a través del Director Ejecutivo de AGESIC, principal interesado en el cumplimiento de estos derechos. Asimismo, su brazo ejecutor, la Dirección de Derechos Ciudadanos tiene un área especializada en protección de datos y otra en acceso a la información pública, de forma que la búsqueda del balance entre ambos derechos es permanente.

4. Conclusiones

Con el objetivo de lograr el equilibrio entre estos derechos fundamentales, debemos tener en cuenta que “el núcleo duro determinante de la protección de datos es la dignidad humana mientras que el derecho de acceso a la información pública se sustenta en la transparencia connatural a la servicialidad de la Administración”⁹.

⁹ DELPIAZZO, Carlos. “A la búsqueda del equilibrio entre privacidad y acceso”. Protección de Datos y Acceso a la Información Pública. Ob. Cit. Página 21.

Uruguay consagró ambos derechos y está logrando el funcionamiento armónico de los mismos. No es un trabajo sencillo, ya que las zonas grises son muchas y deben ser analizadas caso a caso.

El nuevo modelo institucional sin duda necesita tiempo y cambios de gobierno para darle credibilidad. Tal vez este modelo no sea el mejor dentro de 10 años, pero hoy resulta altamente positivo y se encuentra funcionando en forma eficiente.

Por otra parte, se debe tener en cuenta que ambas leyes establecieron como garantía jurisdiccional la acción de habeas data, propia e impropia, estableciendo un mismo trámite para el ejercicio de los derechos, con las diferencias mínimas que caracterizan a cada uno de ellos.

Montevideo, 22 de mayo de 2010