LOS DERECHOS CIUDADANOS

EN EL GOBIERNO

ELECTRONICO

MARIA JOSE VIEGA RODRIGUEZ

LAURA NAHABETIAN BRUNET

(COORDINADORAS)

Montevideo
2013

CAPITULO I – DERECHOS CIUDADANOS

Prof. Dra. Esc. María José Viega

1. GOBIERNO ELECTRÓNICO Y GOBIERNO EN RED

El desarrollo vertiginoso de la tecnología ha derivado en la necesidad de crear un ámbito de protección jurídica vinculado con los derechos a la intimidad y esfera privada de las personas. La informática y la telemática permiten la recolección y trasmisión de información, la manipulación y cruzamiento de datos, permitiendo el almacenamiento masivo de información concerniente a los individuos y la formación de perfiles que pueden emplearse inadecuadamente, provocando muchas veces injerencias arbitrarias o ilegales a la vida privada.

Pero las tecnologías son una herramienta sumamente valiosa, que han creado un cambio de paradigma en el relacionamiento de las personas. Era impensado hace unos años, la potencialidad que podían alcanzar la redes sociales al ser informatizadas, o las relaciones de comercio electrónico, e-learning y por supuesto el gobierno electrónico.

Gobierno electrónico[1] es la posibilidad de acceder a la información de la Administración Pública que interesa, las 24 horas del día, los 365 días del año, en el momento que se necesita, es una realidad inminente. Los trámites y servicios en línea hacen la vida más simple y conveniente brindando las siguientes ventajas:

- El ciudadano no debe trasladarse personalmente.
- No hay hora de cierre, ni esperas.
- Se pueden iniciar trámites desde los hogares, por ejemplo para recargar el teléfono celular a través de la tarjeta de crédito, solicitar comprobantes, certificados y habilitaciones.

Estos son algunos ejemplos de servicios básicos a los que se podrá acceder a través de un simple clic. Estas facilidades, que simplifican la vida cotidiana y que se están incorporando muchas veces sin notarlo, forman parte de lo que se domina Gobierno Electrónico.

La implantación del Gobierno Electrónico debe visualizarse como el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas. Lo que supone que las Administraciones estén interrelacionadas entre sí a fin de simplificar los trámites, servicios y procedimientos.

---

[1] http://www.agesic.gub.uy/innovaportal/v/163/1/agesic/gobierno_electronico_.html Página visitada 23 de setiembre de 2010.

La Carta Iberoamericana de Gobierno Electrónico, adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno en Santiago de Chile, el 10 de noviembre de 2007 lo define de la siguiente forma: "*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*".

El desarrollo del Gobierno Electrónico debe asumirse como un proceso evolutivo que comprende al menos cuatro fases: Presencia, Interacción, Transacción y Transformación. Estas fases no son interdependientes ni tampoco necesitan que termine una para que comience la otra. Cada una de ellas tiene distinto objetivo y requiere distintas exigencias en términos de costos, necesidades de conocimiento y nivel de uso de las TIC.

El concepto de Gobierno en Red[2] 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 internacional.

La Ley de Presupuesto Nacional Nº 17.930 del 23 de diciembre de 2005 creó en su artículo 72 la Agencia para el Desarrollo del Gobierno Electrónico funcionando con autonomía técnica y relacionándose con el Poder Ejecutivo a través de la Oficina de Planeamiento y Presupuesto.

Por Decreto Nº 260/006 de 26 de junio de 2006 se reglamenta el funcionamiento de la Agencia.

Posteriormente, el artículo 54 de la Ley Nº 18.046 del 24 de octubre de 2006 cambió la denominación, pasando a llamarse Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información.

Por Ley Nº 18.172 de 31 de agosto de 2007, se regulan una serie de aspectos referidos a la Agencia en los artículos 118 a 121.

Nos interesa en esta oportunidad, referirnos al artículo 118, que, en primer lugar, cambia nuevamente la denominación, pasando a llamarse Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

---

[2] http://www.agesic.gub.uy/innovaportal/v/26/1/agesic/gobierno_en_red.html Página visitada el 23 de setiembre de 2010.

En segundo lugar se agrega al artículo 55 de la Ley Nº 18.046, de 24 de octubre de 2006, un segundo inciso: "*La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), tiene como misión impulsar el avance de la sociedad de la información y del conocimiento, promoviendo que las personas, las empresas y el Gobierno realicen el mejor uso de las tecnologías de la información y las comunicaciones. Asimismo, planificará y coordinará proyectos en el área de Gobierno Electrónico, como base para la transformación y una mayor transparencia del Estado. A los efectos de promover el establecimiento de seguridades que hagan confiable el uso de las tecnologías de la información, la Agencia tiene entre sus cometidos concebir y desarrollar una política nacional en temas de seguridad de la información, que permitan la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país*".

Por Decreto Nº 618/008 de 22 de diciembre de 2008 se crea la estructura de puestos de trabajo de la Agencia.

La Ley Nº 18.362 de 6 de octubre de 2008, en el artículo 71 establece que el Director de Agesic ejercerá la representación de la misma y fijando dietas por sesión para los miembros del Consejo Directivo Honorario (CHD), con excepción del Director Ejecutivo y el Director de OPP.

Por Ley Nº 18.719 de 27 de diciembre de 2010, se modifica el artículo 72, cambiando la integración del CDH, cambiando al Director de OPP por un representante de la Presidencia de la República.

Actualmente la misión de AGESIC es: "*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*". Y la visión está constituida por "*ser una organización capaz de lograr que el país ocupe un lugar relevante en materia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, dentro del contexto internacional*"[3].

2. EL GOBIERNO ELECTRONICO COMO DERECHO CIUDADANO[4]

La misión del gobierno electrónico o gobierno digital apunta básicamente a los siguientes 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.

El Ing. José Clastornik ha manifestado en múltiples oportunidades que: podemos hablar de gobierno electrónico como hacer portales y tendríamos

[3] http://www.agesic.gub.uy/innovaportal/v/89/1/agesic/mision_y_vision_.html Página visitada 22 de setiembre de 2010.

[4] VIEGA, María José. "La armonización entre las leyes de transparencia y los estándares internacionales de protección de datos". Ponencia presentada en el Seminario Regional de la Red Iberoamericana de Protección de Datos realizado en Montevideo entre el 1 y 4 de junio del 2010.

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 pedir[5]. 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.

Este concepto de Gobierno Electrónico centrado en el ciudadano motivó la creación de la Dirección de Derechos Ciudadanos de AGESIC por la Ley Nº 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".

Uruguay incluyó en su Agenda Digital 2008-2010 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 crearon como desconcentrados de la Agencia de Gobierno Electrónico las Unidades Reguladora y de Control de Datos Personales, de Acceso a la Información Pública y de Certificación Electrónica.

3. PROTECCIÓN DE DATOS PERSONALES

3.1 Orígenes

Las normas surgen debido a una necesidad social, el derecho se plantea la forma de solucionar conflictos que se van produciendo por diferentes motivos. Realizar un análisis de las técnicas de la informática es fundamental como punto de origen para el desarrollo normativo de la protección de datos, porque recién cuando la información puede procesarse informáticamente se plantea el uso lesivo de los datos.

Si bien en 1935 el presidente Roosevelt aprueba la Social Security Act, la cual tenía por objeto la actualización de datos de los trabajadores, no se cumplió plenamente por falta de herramientas técnicas. En ese entonces el Z3 era la herramienta existente descubierta por el profesor Konrad Suze en 1941.

3.1.1 Desarrollo informático

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

1943 - Lo que da impulso a la técnica es la guerra, por lo que se construyó *Colossus*, con la finalidad de descifrar mensajes de los nazis durante la Segunda Guerra Mundial.

1945 - En Estados Unidos se fabrica el ENIAC (Electronic Integrator And Calculator) y el profesor John von Neumann enuncia el considerado primer programa de ordenador, que realizaba una simple operación contable.

1950 - Se realizan aplicaciones civiles y Remington Rand hace el primer ordenador de uso comercial y se fabrica en serie.

1952 – Se utiliza un ordenador en un programa de TV norteamericano, para hacer predicciones electorales sobre la candidatura presidencial de Eisenhower y Stevenson.

1954 – General Electric compra un ordenador UNIVAC (Universal Automatic Calculador) para procesar datos de contabilidad.

1958 – IBM fabrica el SAGE (Semi Automatic Ground Environment).

1960 – Se continúan usando los ordenadores para hacer predicciones electorales, en este caso Kennedy sobre R. Nixon.

1962 – Comienzan los usos civiles en España, cuando RENFE centraliza toda su informática en Madrid.

1968 – IBM introduce el primer sistema de gestión de base de datos. Se procesan entonces datos de personas, por lo que este tratamiento informático multiplica en forma exponencial el uso que puede hacerse de la información y por tanto la posibilidad de producir daño de los derechos individuales.

1969 – Arthur Miller puede considerarse el primer autor consciente de los problemas jurídicos que la informática puede ocasionar a la intimidad de las personas.

1972 – A. Wastin en su monografía “Data Banks in a free society” alerta sobre los usos lesivos de las bases de datos.

3.1.2 Desarrollo normativo

El uso de las computadoras en forma general, no solo por empresas e instituciones, sino también por los particulares, incrementa la preocupación sobre el uso lesivo de la informática. Si bien podría pensarse que la primera norma jurídica sobre protección de datos debería haberse aprobado en Estados Unidos, por ser el pionero en el desarrollo de los ordenadores, no fue así.

1967 – El Consejo de Europa constituyó una Comisión consultiva para el estudio de las tecnologías de la información y su potencial lesividad de derechos de las personas.

1968 - Los estudios de la Comisión concluyeron con la Resolución 509 de la Asamblea del Consejo de Europa, que tiene por objeto poner de manifiesto la posible confrontación entre los derechos humanos y los nuevos logros científicos y técnicos.

1970 - La primera norma que limita el uso de la informática se publica en el Länder alemán de Hesse el 7 de octubre de 1970 llamada "Datenschutz".

1973 - La segunda norma es la Data Lag de Suecia.

El Comité de Ministros de Europa publica la Resolución Nº 73 de 26 de setiembre de 1973, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado.

1974 - El Comité de Ministros de Europa publica la Resolución Nº 74 de 20 de setiembre, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

También en 1974 entra en vigor en Estados Unidos la *Privacy Act,* el mejor texto hasta esa fecha, y e precursor de las normas de protección de datos que le seguirán.

3.1.3 Desarrollo telemático

1965 – Roberts y T. Merril conectan por primera vez dos ordenadores a través de una línea telefónica y transmiten datos de uno a otro. Así nace ARPANET.

1970 - Además de los usos militares, ofrecía correo electrónico y transferencia de ficheros dentro de Estados Unidos.

1973 – Se realizan las primeras conexiones internacionales. Al principio la comunicación era entre ordenadores, pero posteriormente lo que se conecta son redes o conjunto de ordenadores. Esta es una dificultad de ARPANET que fue diseñada para interconectar ordenadores y no redes de ordenadores.

El funcionamiento de ARPANET, al igual que INTERNET, se basa en una serie de protocolos. Estos constituyen un conjunto de reglas que permiten estandarizar un procedimiento repetitivo.

1983 - El 1 de enero se sustituye el protocolo NCP por el de TCP/IP, separando la parte militar, denominada Milnet y surge INTERNET, que coexiste con ARPANET hasta 1990.

1991 – Aparece la Wold Wide Web como la conocemos hoy. No es solo una herramienta de trabajo, es un medio global de intercambio de información de datos y un medio de comunicación.

Todo avance tecnológico que implique un uso social, finaliza requiriendo la intervención jurídica, pero debido a la existencia del ciberespacio, no es suficiente la legislación estatal, sino que se requiere una regulación universal, que plantea dificultades.

3.2 Evolución histórica

A los efectos de analizar el proceso evolutivo de la protección de datos, lo hacemos a través de las diferentes generaciones de las normas sobre la temática[6].

3.2.1 Primera generación

El uso de las bases de datos se utiliza en la Administración Pública. El conocimiento de los datos no es generalizable e instrumentable, por lo que la protección se centra en el espacio físico donde se encuentra la información, es decir el ordenador y la base de datos. No hay conciencia de uso indebido de datos por parte de los ciudadanos. Se aprueban las siguientes leyes: Datenschutz (7 de octubre de 1970), Data Lag (11 de mayo de 1973) y Landesdatenschutzgesetz (24 de enero de 1974). No hacen referencia a ficheros de carácter privado y crean órganos de control del tratamiento de datos, rindiendo cuentas directamente al Parlamento.

3.2.2 Segunda generación

a) Primera fase: las normas refieren a la pretensión de conservar la calidad de los datos y se tiene en cuenta el uso indebido en el ámbito privado, el cual puede lesionar derechos fundamentales.

   Privacy Act (1974): establece que el tratamiento de la información debe estar justificado y ser necesario para las funciones propias del organismo que los utiliza.

   Se establecen los principios básicos: consentimiento del titular, derecho de acceso y de control, obligación de mantener la calidad de los datos, informar en el momento de la recogida de datos la finalidad de los mismos.

b) Segunda Fase: se aprueban leyes que protegen determinado tipo de datos, denominados “datos sensibles” (raza, religión, sexo, ideología, etc.).

   Ley francesa (6 de enero de 1978): el avance radica en extrapolar el problema de la relación informática-derechos fundamentales, de lo personal e individual, a lo colectivo.

---

[6] REBOLLO DELGADO, Lucrecio-María Mercedes Serrano. “Introducción a la Protección de Datos”. Editorial Dykinson S.L. Madrid. 2008.

Ley Datenschutz (27 de enero de 1977): de la entonces República Federal de Alemania refuerza la protección de los datos personales frente al Estado y amplía la vigencia a los ficheros particulares.

3.2.3 Tercera generación

Existen dos desencadenantes concretos en la evolución normativa:

a) La Sentencia del Tribunal Federal Alemán de 15 de setiembre de 1983 en la cual se declaran inconstitucionales algunos preceptos de Ley del Censo de 1982, esta norma imponía sanciones económicas fuertes y la finalidad de los datos no era solo estadística. Otro elemento importante de la sentencia es que consagra el concepto de derecho de autodeterminación informativa, como derecho que tiene el individuo "de decir básicamente por sí solo la difusión y utilización de sus datos personales".

b) La aparición el 1º de enero de 1983 de Internet hace que se requiera un nuevo tipo de normas que contemple las posibilidades técnicas y que tenga presente a internacionalización.

Se modifica la Privacy Act y la norma alemana. En 1991 se publica en Portugal una ley de protección de datos y en 1992 en España.

A nivel supranacional se aprueba la Directiva 95/46/CE y referente a telecomunicaciones, la Directiva 97/66/CE que obliga a los Estados miembros a garantizar la confidencialidad de las comunicaciones a través de redes públicas.

3.3 Fundamentos del Derecho a la Protección de Datos Personales

En todo Estado democrático el poder está sometido al Derecho, por tanto la forma de solucionar los problemas derivados de la tecnología y que puedan lesionar derechos fundamentales es a través de normas jurídicas.

El conocimiento que se tenía del ciudadano, durante 20 siglos fue muy escaso y estaba centralizado en dos instituciones: el Estado y la Iglesia. Pero esto ha cambiado con el desarrollo de la tecnología, por lo que hoy se ha convertido en una herramienta capaz de violar nuestra privacidad y con la cual cometer un sinfín de delitos.

Para entender la protección de datos tenemos que realizar un acercamiento al derecho a la intimidad. Este es un concepto que ha evolucionado y se puede resumir en tres concepciones:

a) Concepto objetivo del derecho a la intimidad: el Diccionario de la Real Academia Española define intimidad como la zona espiritual reservada o íntima

de una persona o grupo, especialmente de una familia. Este es el concepto utilizado por el Tribunal Constitucional Español.

La doctrina alemana refiere a las esferas o círculos concéntricos: el núcleo lo constituye lo íntimo, en una parte más externa encontramos lo familiar, en otra lo secreto o confidencial, siendo la última lo público.

b) Concepto subjetivo del derecho a la intimidad: se identifica con el derecho a la autodeterminación informativa. Existe para el Tribunal Constitucional un ámbito propio de la vida privada que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo que el interesado lo consienta.

Cada persona tiene derecho a controlar lo que se conoce de ella y el ordenamiento jurídico debe establecer mecanismos para que ese derecho sea efectivo.

c) Teoría del mosaico: explicación a la necesidad de protección de la intimidad frente a la informática y a los nuevos ingenios tecnológicos.

Madrid Conesa entiende que: “la teoría de las esferas no es válida, dado que hoy los conceptos de lo público y lo privado son relativos, pues existen datos que a priori sin irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado”.

La concepción de derecho a la intimidad que une la definición objetiva y subjetiva parece la más acorde para Lucrecio Rebollo, tanto con la idea de derecho a la intimidad, como con las necesidades del ordenamiento jurídico.

El concepto a la intimidad no puede ser cerrado, porque varía de una persona a otra, de un grupo a otro, de una sociedad a otra.

En el derecho a la intimidad existe un fundamento inexorable, la dignidad humana y el libre desarrollo y configuración de su personalidad.

Los ordenamientos jurídicos han adoptado dos posturas a nivel normativo, por un lado la legislación americana en la cual se establece que todo está permitido, excepto lo que está prohibido y en segundo lugar, con Alemania como representante principal, se entiende que cualquier actividad relativa al procesamiento de datos personales está prohibida, salvo cuando está permitida.

4. ACCESO A LA INFORMACION PÚBLICA

4.1 Orígenes

De acuerdo a la Dra. Nahabetian el primer antecedente en materia de transparencia y facilitación de acceso a documentación pública se remonta a China, durante el período de la Dinastía Tang y particularmente al reinado del emperador T´ai-tsung entre los años 627 y 649, en que se reestructuró el gobierno chino.

"Durante este proceso se estableció el denominado Buró de Censura Imperial, consistente en un grupo de élite de alto nivel educativo con funcionarios de absoluta competencia académica, los que no solo se ocupaban de la registración de las decisiones oficiales del gobierno y de la correspondencia, sino que también efectuaban severas críticas al gobierno, incluido el emperador. Se trata de una institución fundada en la filosofía humanista de Confucio en la que su rol principal fue controlar al gobierno y sus funcionarios así como denunciar la mala gobernabilidad, la ineficiencia burocrática y la corrupción oficial"[7].

Por otra parte, ACKERMAN y SANDOVAL relatan el origen europeo del tema, con las siguientes palabras: "En el lejanísimo año de 1766, luego de un período convulso, un sacerdote sueco-finlandés que era diputado, economista, tabernero, hombre culto y viajero, Anders Chydenius, impulsó la primera ley de acceso a la información gubernamental de que el mundo tenga memoria: la "Ley para la Libertad de prensa y del Derecho de Acceso a las Actas Públicas".

Era el producto del movimiento político liberal, comandado por Gustavo III, el mismo que configuró una nueva Constitución. (…) Años después de la Constitución, Chydenius y los suyos dieron un paso más allá: inspirado e impresionado por la experiencia china, quiso instaurar algo así como el Buró de Censura Imperial, una institución de la dinastía Ching que se encargaba de vigilar cuidadosamente al gobierno y a sus funcionarios, de exhibir sus competencias, ineficiencias y prácticas de corrupción. La idea le pareció tan poderosa, tan necesaria y tan útil que Chydenius escribió: "si la Constitución no lograra nada más, de todos modos nuestra nación cambiara con la acción de esta ley que ha nacido a su amparo"[8].

A nivel internacional, este derecho fue reconocido en la Declaración de los Derechos del Hombre y del Ciudadano que data de 1791, cuyo artículo 14 indica que todos los ciudadanos tienen el derecho de constatar, por ellos mismos o por sus representantes, la necesidad de la contribución pública, de consentirla libremente, de hacer el seguimiento de su empleo, determinar la cuota, la base imponible, la cobertura y la duración. Y aclara en el artículo 15 que la sociedad tiene el derecho de solicitar cuentas a todo agente público sobre su administración[9].

4.2 Evolución histórica

---

[7] NAHABETIAN Laura. "Acceso a la Información Pública: pilar fundamental del buen gobierno". Amalio Fernández. Montevideo, setiembre de 2010. Página 35.

[8] ACKERMAN John M. y SANDOVAL Irma E. "Leyes de Acceso a la Información en el Mundo". Cuaderno de transparencia Nº 7. IFAI. Página 5.

[9] El Derecho a la Información en América Latina – Comparación Jurídica- Toby Mendel, Pág. 11, Año 2009.

4.2.1 Evolución de normas internacionales

Comenzando la evolución histórica desde un punto de vista internacional, encontramos en 1946 la Resolución de la Organización de las Naciones Unidas Nº 59, que considera que la libertad de información es un derecho humano fundamental y es el punto de partida de todas las libertades a las cuales están consagradas las Naciones Unidas.

En la misma línea, la Declaración Universal de Derechos Humanos de 1948, en su artículo 19 expresa que todo individuo tiene derecho a la libertad de información y de expresión. Este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlos sin limitación de fronteras, por cualquier medio de expresión[10].

También merece destaque el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, que fue adaptada por el Consejo de Europa en 1950. Este documento garantiza la libertad de expresión e información como derecho humano fundamental[11].

El Pacto Internacional de Derechos Civiles y Políticos de la ONU de 1996 regula el derecho a la libertad de opinión y de expresión en términos similares a los contenidos en la Declaración de Derechos Humanos.

La Convención de Aahrus de 1998 es un instrumento internacional que contiene disposiciones sobre el acceso a la información, la participación del público en la toma de decisiones y el acceso a la justicia en materia de medio ambiente, la cual ha sido ratificado por más de 40 países, fundamentalmente de Europa y Asia Central[12].

La Carta de Derechos Fundamentales de la Unión Europea del 2000, expresa en su artículo 42 que se debe conceder el derecho a acceder a los documentos que estén en manos de las instituciones de la Unión Europea[13].

En el año 2002, el Comité de Ministros del Consejo de Europa emitió la Resolución Nº R (2002)2, que versa sobre el acceso a documentos oficiales.

4.2.2 Evolución del derecho a nivel constitucional

Mark Bovens entiende que "debemos conceptualizar el derecho a la información como la cuarta ola de los derechos humanos, equivalente a los derechos civiles, políticos y sociales caracterizados en los textos clásicos de T.H. Marshall. En el umbral del fin de la era industrial y con el advenimiento de

---

[10] Documento disponible en http://www.un.org/es/documents/udhr/, página visitada el 12 de junio de 2012.

[11] Documento disponible en http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/CONVENTION_ESP_WEB.pdf, página visitada el 12 de junio de 2012

[12] Documento disponible en http://www.mediterranea.org/cae/aarhus_convenio.htm, página visitada el 12 de junio de 2012

[13] Documento disponible en http://www.europarl.europa.eu/charter/pdf/text_es.pdf, página visitada el 12 de junio de 2012

la "sociedad de la información" el mundo necesita ajustar sus marcos constitucionales con objeto de incorporar los nuevos derechos universales a la información. En este punto el autor hace una distinción crucial entre transparencia definida como una cuestión de "higiene pública" y los derechos a la información como un asunto de ciudadanía"[14].

Relacionado a los cambios constitucionales que considera Bovens, algunos países han reconocido este derecho a nivel constitucional, tal es así el caso de la Constitución de Grecia de 1975, en su artículo 10 numeral 1, expresa que toda persona, por su propia cuenta o en conjunto con otras, tendrá el derecho, observando la legislación vigente, de presentar peticiones escritas a las autoridades públicas, que estarán obligadas a tomar medidas inmediatas conforme las disposiciones vigentes y a dar una respuesta escrita y razonada al peticionario conforme a la ley. Se aclara que la solicitud de información obliga a las autoridades competentes a contestarla, con tal que la ley así lo establezca" [15].

En la misma línea que la anterior, la Constitución portuguesa de 1976 reconoce el derecho al acceso a la información pública en su artículo 268, numeral 2º, como los derechos de archivos y registros administrativos, sin perjuicio de lo dispuesto por la ley en materias relativas a la seguridad interna y externa, la investigación criminal y la intimidad de las personas[16].

La Constitución española, que data de 1978**,** indica en su artículo 105 que la Ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas[17].

Brasil regula este derecho en su Constitución de 1988**,** cuyo artículo 5º lo regula en los siguientes términos: "todos tienen derecho a recibir de los órganos públicos informaciones de su interés público, o de interés colectivo o general que serán suministrados dentro del plazo de ley, bajo pena de responsabilidad, salvo aquellas cuyo sigilo sea imprescindible para la seguridad de la sociedad o del Estado" [18].

---

[14] ACKERMAN John M. y SANDOVAL Irma E. "Leyes de Acceso a la Información en el Mundo". Ob. Cit., pág. 14.

[15] El derecho de acceso a la información en Europa y América Latina: un enfoque constitucional, documento disponible en http://huespedes.cica.es/aliens/gimadus/10/DERECHOACCESO.htm, página vistada eñ 13 de junio de 2012.

[16] Documento disponible en http://www.viajeuniversal.com/portugal/constitucion2.htm, página visitada el 12 de junio de 2012

[17] Documento disponible en http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCASTELLANO.pdf, página visitada el 12 de junio de 2012

[18] Documento disponible en http://pdba.georgetown.edu/Constitutions/Brazil/esp88.html#mozTocId72227, página visitada el 12 de junio de 2012

Colombia adoptó este derecho en la Constitución de 1991, en donde el artículo 74 indica que todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la Ley[19].

En 1993, la Constitución de Perú indica en su artículo 2º, numeral 5, que se tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional[20].

La Constitución de la Ciudad de Buenos Aires, del año 1996**,** indica que toda persona tiene derecho, a su solo pedido, a recibir libremente información sobre el impacto que causan o pueden causar sobre el ambiente las actividades públicas o privadas" [21].

Merece destaque el reconocimiento constitucional de este de derecho en Noruega, en el año 2004, en el sentido de que toda persona tiene derecho de acceso a los documentos del Estado y a la administración municipal, así como el derecho de estar presente durante las audiencias de las cortes y las sesiones de las asambleas elegidas. La Ley puede limitar este derecho respecto al derecho de la intimidad y otras consideraciones de peso.

La Constitución de Ecuador de 2008 reconoce este derecho en el artículo 91, expresando que la acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquier otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley[22].

4.2.3 Evolución legal del Acceso a la Información Pública

La tabla que sigue muestra la evolución cronológica en que se aprobaron leyes de acceso a la información pública en los diferentes países, a los efectos de aquilatar la importancia del tema y apreciar los momentos significativos en el desarrollo normativo.

AÑO	PAISES
1766	Suecia

[19] Documento disponible en http://www.banrep.gov.co/regimen/resoluciones/cp91.pdf, página visitada el 12 de junio de 2012

[20] Documento disponible en http://www.oas.org/juridico/spanish/mesicic3_per_cons.pdf, página visitada el 12 de junio de 2012

[21] Documento disponible en http://www.buenosaires.gov.ar/areas/com_social/constitucion/completa.php?menu_id=11172, página visitada el 12 de junio de 2012

[22] Documento disponible en http://www.mmrree.gob.ec/ministerio/constituciones/2008.pdf, página visitda el 12 de junio de 2012

1888	Colombia
1951	Finlandia
1966	Estados Unidos
1970	Dinamarca, Noruega
1977	Aland o Islas Gland
1978	Francia, Holanda
1982	Australia, Nueva Zelanda, Canadá
1987	Austria, Filipinas
1990	Italia
1992	Hungría, Ucrania, España
1993	Portugal, Kazajstán
1994	Belice, Bélgica, Groenlandia
1995	Hong Kong
1996	Islandia, Corea del Sur
1997	Tailandia, Irlanda, Uzbekistán
1998	Israel, Letonia
1999	República Checa, Albania, Georgia, Grecia, Japón, Liechtenstein, Trinidad y Tobago, Sudáfrica
2000	Inglaterra, Bosnia y Herzegovina, Bulgaria, Lituania, Moldavia, Eslovenia, Estonia
2001	Rumania
2002	Panamá, Pakistán, México, Jamaica, Angola, Zimbabue, Perú, Escocia
2003	Argentina, Armenia, Croacia, Eslovenia, Turquía
2004	República Dominicana, Serbia, Suiza
2005	Alemania, India, Taiwán
2006	Honduras
2007	Jordania, Nepal, Nicaragua, China
2008	Uruguay, Chile, Guatemala, Bangladesh

4.3 Fundamentos del Derecho de Acceso a la Información Pública

Entendemos que al tratar el tema de los fundamentos del Derecho de Acceso a la Información Pública debemos hacerlo desde una doble dimensión: el acceso a la información pública como un derecho fundamental de las personas y en segundo lugar como un requisito previo de la participación ciudadana y por tanto como un elemento imprescindible para la existencia de un Estado transparente.

Como derecho fundamental, las personas se encuentran inmersas en la sociedad de la información, donde ésta es sinónimo de poder, entendido éste desde distintos puntos de vista. Por lo tanto, cada persona tiene derecho a saber que hace el Estado, cómo lo hace y cuándo lo hace, facilitándole la toma de decisiones tanto de índole personal, empresarial, política o social.

Desde “La Política”, de Aristóteles (384 a.C. – 322 a.C.) se plantea la importancia del desarrollo de la democracia en un marco de libertad, en que los

ciudadanos juzguen las “cuentas públicas” y negocios políticos para un adecuado equilibrio de las fuerzas políticas. La información, como requisito básico para el sostenimiento de la entonces democracia ateniense, fluía en el “ágora”, encontrando una vigencia total las palabras de Aristóteles, que destaca la participación ciudadana como principio democrático real, no como simples electores, sino agentes sociales[23].

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”[24].

El derecho a la información está sólidamente fundado en los principios básicos de la democracia, el buen gobierno y la participación ciudadana. Aún más, de acuerdo a Roberts la participación ciudadana para el control gubernamental no es sólo una posibilidad productiva sino un deber y una responsabilidad[25].

En el ámbito económico, la transparencia genera un clima de inversión más confiable al permitir a los actores económicos calcular dónde y cuándo podrán invertir con mayor seguridad. No es fortuito que el mercado viva y muera con base en la información. Aunque la opacidad y en general la “información desleal” puede resultar altamente rentable para algunos pocos, en realidad la salud del mercado en el largo plazo depende de un continuo y confiable flujo de información[26].

La transparencia también mejora el proceso de toma de decisiones de los servidores públicos al obligarles a conducirse con mayor responsabilidad.

En este sentido, Federico Reyes Heroles dice: “No hay vitaminas para fortalecer la moral”. Pero lo que sí podemos elaborar son contextos, canales, estructuras y mediciones objetivas que contengan, reduzcan y detecten a la corrupción. No se trata pues, de esperar la redentora llegada del “hombre nuevo” ni la caída de querubines en el interior del gobierno, sino de poner en marcha, aquí y ahora, instrumentos mensurables, un conjunto de dispositivos que encaucen y mejoren el trabajo al interior del Estado[27].

---

[23] http://www.nl.gob.mx/?P=transparencia_historia Página visitada 4 de febrero de 2013.
[24] DELPIAZZO Carlos. “marco conceptual de la gobernanza con especial referencia a Internet”. Ponencia presentada en el XII Congreso Iberoamericano de Derecho e Informática. Zaragoza, 2008.
[25] ACKERMAN John M. y SANDOVAL Irma E. “Leyes de Acceso a la Información en el Mundo”. Ob. Cit., pág. 15.
[26] ACKERMAN John M. y SANDOVAL Irma E. “Leyes de Acceso a la Información en el Mundo”. Ob. Cit., pág. 18.
27 REYES HEROLES Federico. “Corrupción: de los ángeles a los índices”. Cuadrenos de Transparencia Nº 1. IFAI. Página 7.

CAPÍTULO II - PRINCIPIOS Y DERECHOS DE LA PROTECCION DE DATOS PERSONALES

Dra. Esc. Beatriz Rodríguez Acosta

1. PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

1.1 Introducción

Cuando estudiamos los datos personales debemos tener en cuenta la existencia de principios que garantizan el ejercicio de los derechos de la protección de datos.

Tanto los principios como los derechos son el eje fundamental de esta protección siendo reconocidos en las legislaciones y la doctrina, sobre todo cuando estos temas son parte integrante de un Derecho que es novedoso, con vocación de universalidad y en formación, requerido de piezas arquitecturales del ordenamiento cuya manifestación se verifica fundamentalmente a través de la práctica aplicativa del Derecho en la especie a la jurisprudencia y a la doctrina como fuentes relevantes del Derecho[28].

Estos principios generales definen las pautas a las que debe atenerse la recolección, el tratamiento y el uso de los datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información registrada como la congruencia y racionalidad de la utilización de los datos[29].

Desde el comienzo de la generación de normas referentes a la protección de datos ha habido un perfeccionamiento de éstas con respecto a los derechos del titular de los datos, pasando de la falta de conciencia de los individuos en cuanto a sus datos personales, a querer conservar la calidad de los datos, llegando en una tercera etapa al llamado derecho a la autodeterminación informativa, es decir aquel derecho que tiene la persona de difundir y utilizar sus datos personales por si solo[30].

La autodeterminación informativa está conformada por diversos principios, los que son incorporados a un conjunto de normas que la regulan. Estas normas son, entre otras, la Directiva 95/46/CE del Parlamento de Europa y el Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que abre camino a la regulación comunitaria, las diferentes leyes

---

[28] DELPIAZZO, Carlos y otra. Lecciones de Derecho Telemático. Tomo I, Montevideo, 2004. FCU, pág. 73.

[29] CEDDET. Principios Básicos de la Protección de Datos. Módulo 2. Curso on line El Derecho a la Protección de Datos Personales. 1ª. Edición, España, 2010. Fundación CEDDET, pág. 47.

[30] RODRIGUEZ ACOSTA, Beatriz. "Los derechos en la protección de datos personales en el derecho español y el derecho uruguayo. Trabajo final del Curso a Distancia Experto Universitario en Protección de Datos Personales de la Universidad Nacional de Educación a Distancia. España. 2009-2010.

especiales de los Estados pertenecientes a la Unión Europea, como ser la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de España (LOPD), de 13 de diciembre de 1999, con su Real Decreto Reglamentario, así como también el Convenio Nº 108, del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Estas normas mencionadas son las que vamos a tomar como referencia en este capítulo para el estudio tanto de los principios como de los derechos de la protección de datos personales.

No solo en las legislaciones se han establecido estos principios y derechos, sino que la comunidad experta en esta materia se ha reunido en la 31ª Conferencia de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid en noviembre de 2009, dejando como saldo la Resolución de Madrid sobre Estándares Internacionales de Protección de Datos Personales y Privacidad, la que había comenzado a gestarse en Montreal en la 30ª Conferencia.

La Resolución tiene por objeto definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal, así como facilitar los flujos internacionales de éstos, necesarios en un mundo globalizado, lo que llevaría a un tratamiento de los datos personales, tanto en el ámbito público como privado, más armónico en todos los niveles ya sean nacionales como internacionales.

La Organización para la Cooperación y el Desarrollo Económico (OCDE), la Red Iberoamericana de Protección de Datos también han establecido diversos principios en relación con los datos personales.

1.2 Principio de calidad de los datos

El principio de calidad de los datos debe ser tenido en cuenta en el momento de la recolección de los datos, debido a que no podrán ser recogidos datos que no se adecuen a sus exigencias, así como en el momento del tratamiento que se realice de ellos, sea cual sea su naturaleza,

Este principio está consagrado en la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como en la LOPD y en el Convenio Nº 108.

La Directiva en su artículo 6º regula este principio, estableciendo que los datos deben ser tratados de manera leal y lícita, recogidos con fines determinados, explícitos y legítimos y no sean tratados luego de manera incompatible con estos fines, a su vez deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente, asimismo deberán ser exactos, actualizados, y conservados por un período no superior al necesario para los que fueron recogidos.

Se establece una diferencia entre el texto inicial de la Directiva en el que se hacía referencia a la licitud de la recogida y del tratamiento, como si se tratara de actividades u operaciones distintas, en cambio en el texto definitivo no existe esta diferencia, sino que con carácter general se refiere a todo tratamiento, se aprecia así el traslado de importancia en cuanto al ámbito de aplicación al concepto de tratamiento, superándose el concepto más rígido de base de datos[31].

Si bien se deben cumplir los requisitos de calidad del dato, éstos sólo podrán ser objeto de tratamiento cuando se cumplan las condiciones establecidas en la Directiva en sus artículos 7º y 8º es decir finalidad, proporcionalidad, así como las garantías necesarias para el tratamiento de los datos sensibles.

En cuanto a la proporcionalidad sólo podrán ser recabados los datos que sean adecuados, pertinentes y no excesivos en relación con la finalidad para la que se hayan obtenido, es decir que ambos principios estarían vinculados entre si.

La adecuación necesaria al ser recolectados los datos y al momento de su tratamiento debe ser correspondida con la finalidad que lo motiva.

La licitud del tratamiento precisa de dos requisitos: que los datos personales cumplan con los principios de calidad establecidos en el artículo 6º y que el tratamiento de éstos se sometan a las condiciones de legitimidad (art. 7º).

El artículo 6º coincide con los artículos 5º y 7º del Convenio Nº 108 del Consejo de Europa en cuanto a lo establecido con respecto al principio de calidad de los datos. Dicho Convenio además regula en su artículo 8º las garantías necesarias para las personas involucradas.

En la LOPD este principio se ve consagrado en el artículo 4º. A diferencia de la Ley Orgánica anterior en la que figuraba que las finalidades no pueden ser distintas, se cambia y se señala que las finalidades no pueden ser incompatibles.

Con respecto a esta diferencia la Agencia Española de Protección de Datos Personales en la Resolución 96/2005 mantiene que los términos “distinta” e “incompatibles” son lo mismo.

Asimismo el Tribunal Constitucional Español se ha referido a la calidad de los datos y en especial a la proporcionalidad de éstos, existiendo variadas sentencias que mencionan el tema.

Con este principio lo que se trata de evitar es que se proceda a una recopilación de datos masiva que se aparte de la necesidad y finalidad para que dichos datos pretendan ser utilizados y tratados. Igualmente en base a dicho principio y a la finalidad del tratamiento se fija la condición de que una

[31] HERRAN ORTIZ, Ana. El derecho a la intimidad en la nueva ley orgánica de protección de datos en la sociedad de la Información. Madrid, España, 2002. Editorial Dikynson, pág. 134.

vez desaparezcan almacenados dichos datos, deberá ser cancelada directamente por el responsable del fichero[32].

Se han dictado, entre otras, la sentencia de fecha 8 de febrero de 2006 con respecto al principio de calidad de los datos, por la Audiencia Nacional, Sala de lo Contencioso Administrativo, Sección Primera que desestima un recurso presentado por una entidad bancaria contra la resolución del Director de la AGPD de 22 de marzo de 2004, por la que se le impone a ésta una sanción de 60.101,21 euros, por la infracción de los artículos 4.3 y 29.4 de la LOPD, tipificada como infracción grave den al artículo 44.3 de dicha norma, de conformidad con lo establecido en el articulo 45.2 de la citada Ley Orgánica y declara ajustada a derecho dicha resolución[33].

1.3 Principio de veracidad

Con este principio lo que se busca es que los datos personales que se recojan y que sean sometidos a tratamiento sean exactos, deben suponer una información al día del interesado, a su situación actual.

La Directiva al regular el principio de calidad de los datos en su artículo 6º menciona en el literal d), el principio de veracidad, al disponer que los datos deben ser exactos y, cuando sea necesario, actualizados, al igual que deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Cuando se recabe el dato personal se tendrá que verificar si realmente es veraz y una vez sometido a tratamiento tendrá que mantenerse actualizado.

Este principio está regulado en la LOPD en su artículo 4º apartado 3, como parte del principio de calidad de los datos, como sucede en la Directiva 95/46/CE.

De acuerdo con Nieves Buisán[34] éste es un principio que no suele destacarse desde el punto de vista teórico tanto como los demás principios establecidos, pero tiene relevancia, en cuanto no sólo resulta necesario que los datos se recojan para su tratamiento de acuerdo con una serie de criterios, y que éstos se empleen para finalidades compartibles a los que motivaron la recolección, sino también que sean exactos y puestos al día, puesto que lo contrario supondría de forma implícita el incumplimiento de los citados principios, aunque fuera posteriormente. Se trata de garantizar y proteger la calidad de la información sometida a tratamiento por la que debe velar quien recoge y trata datos personales.

---

[32] Agencia Española de Protección de Datos Personales. http://www.agpd.es/portalwebAGDP/canalciudadano/preguntasciudadano/principios_lopd/Calidad_Datos/index-ides-idphp.php Página visitada el 10/6/10.

[33] http://www.agpd.es/portalwebAGDP/canaldocumentacion/sentencias/audiencia?nacional/common/pdfs/Recurso-AN-08-02-06-Calidad-de-los-datos-Ficheros-de-solvencia-patrimonial.pdf Página visitada el 15 de junio de 2010.

[34] BUISAN GARCIA, Nieves y otros. La ley de protección de datos: análisis y comentario de su jurisprudencia. Valladolid, España, 2008. Editorial Lex Nova, págs, 154 y sgtes.

Este principio si no es cumplido o es vulnerado puede tener consecuencias para el afectado y se han dictado varias sentencias de la Sala de lo Contencioso Administrativo de la Audiencia Nacional Española, así como resoluciones de la AGPD, cuyo principal tema es el mencionado principio.

Podemos citar como ejemplo la Resolución R/00438/2010 de la AGDP, de 16 de abril de 2010, en la cual se multa a una persona que había alquilado un auto a una empresa que renta automóviles por parte de la Dirección General de Tráfico del Ministerio del Interior, debido a que la empresa envió los datos de quien había arrendado el coche con otra fecha diferente a la de la infracción[35].

1.4 Principio de finalidad

El principio de finalidad supone que los datos personales sólo pueden ser utilizados para finalidades determinadas, explícitas y legítimas; los datos no podrán ser utilizados para objetivos diferentes de aquellos para los que fueron recolectados.

Cuando decimos que la finalidad debe ser determinada significa que los datos deben ser recolectados para una finalidad concreta que justifique su tratamiento; explícita indica que el tratamiento de los datos debe ser fundamentado en una finalidad clara y legítima.

Si los datos son tratados con un fin diferente a aquél para el que fueron recabados es necesario el consentimiento del titular del dato personal. Con esta manifestación aseveramos que la finalidad es única, es decir, que los datos que fueran dados para una determinada función o razón no pueden ser utilizados para otras diferentes. Esta determinación unívoca de la finalidad implica, además, como valor añadido:

a) la interdicción previa del registro de datos para fines no determinados,
b) la necesaria especificación, en aquellos casos excepcionales y predeterminados por la ley de los supuestos de modificación posterior de las finalidades previamente determinadas. Las nuevas finalidades no deben añadirse, no obstante, de manera arbitraria, sino que debe aplicar la compatibilidad de los nuevos fines con los iniciales.[36]

En el Primer Congreso Europeo de Protección de Datos celebrado en Madrid el 31 de marzo de 2006, se llegó a la conclusión entre todas las Autoridades de Control presentes que deben garantizar que los responsables públicos y privados respeten el principio de finalidad.

---

[35] http://www.algpd.es/portalwebAGDP/resoluciones/admon_publicas/ap_2010/common/pdfs/AAPP-00073-2009_Resolucion-de-fecha-16-04-201_Art-ii-culo-4.3-LOPD.pdf Página visitada el 15 de junio de 2010.

[36] SANCHEZ BRAVO, Álvaro. La protección del derecho a la libertad informática en la Unión Europea. Universidad de Sevilla. España, 1998, pág. 84.

Luis López Guerra, Secretario de Estado de Justicia de España terminó su alocución en el Congreso animando a los asistentes a consolidar "una cultura cívica de datos personales"[37]. Asimismo José Luis Piñar manifestó que "las Autoridades de Control debemos poner un empeño especial en garantizar que tanto los responsables públicos como los privados respeten el principio de finalidad en el tratamiento de los datos evitando que éstos se utilicen para fines incompatibles"[38].

Con respecto a este principio el apartado 2 del artículo 4º de la LOPD prohíbe que los datos puedan usarse para finalidades incompatibles con aquéllas para las que fueron recogidas. Sin embargo el mismo apartado considera que no es incompatible el tratamiento posterior de los datos para fines históricos, estadísticos o científicos.

Esta finalidad es la que fija los criterios para juzgar el carácter pertinente, adecuado y no excesivo de los datos registrados, las categorías de personas u organismos en los que pueden guardarse los datos recogidos.

Los fines deben estar determinados previamente a su recolección, siendo su determinación lo más precisa posible, para evitar incompatibilidades, debido a que cuanto más general sea el fin determinado más difícil será controlar si los usos posteriores de los datos son incompatibles con el fin inicialmente previsto.

De acuerdo con lo establecido en la Directiva solo será posible modificar la finalidad del tratamiento si ésta no es incompatible con la inicialmente determinada, y será incompatible el tratamiento posterior "con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas", lo que se traduce en el Considerando 29 en que "dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona".

Con lo mencionado anteriormente vemos que con el principio de finalidad se relaciona directamente el principio de proporcionalidad. Principio éste que se recoge en el apartado c) del artículo 6º de la Directiva al decir que la información debe ser "adecuada, pertinente y no excesiva" con relación a los fines para los que se recabe y trate posteriormente.

A su vez estos datos deberán ser exactos, es decir deberán responder a la realidad del titular del dato en cada momento, por eso la Directiva establece la necesidad de que estén actualizados. Si éstos son inexactos o están incompletos no cumplen con el principio de finalidad, ya que éste exige que la información personal incompleta y obsoleta difícilmente pueda ser necesaria y útil para el cumplimiento de los fines determinados[39].

---

[37] https://www.agpd.es/portalwebAGPD/internacional/Europa/conferencias/I_congreso_europeo/common/pdfs/Nota_clausura_y_conclusionesok_3_4_06.pdf. Página visitada el 15 de junio de 2010

[38] http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2006/notas_prensa/common/Nota_clausura_y_conclusionesok_3_4_06.pdf Página visitada el 15 de junio de 2010.

[39] CEDDET Ob. Cit. Módulo 2, pág. 136.

En cuanto a la conservación de los datos después de cumplida la finalidad, la Directiva establece como excepción, que el responsable de la base puede seguir conservando los datos cuando tengan carácter histórico, estadístico o científico siempre que se cumplan las garantías necesarias del caso.

1.5 Principio de previo consentimiento informado

De acuerdo con lo establecido por el Tribunal Constitucional Español el derecho fundamental a la protección de datos se basa en dos pilares, uno el consentimiento y otro el derecho de los interesados.

En materia de protección de datos personales consiste el consentimiento en un elemento necesario que justifica el tratamiento de datos personales por el responsable de la base de datos.

Debemos tener en cuenta que en la obtención del consentimiento, es necesario diferenciar entre el consentimiento para la recolección y el tratamiento de los datos y el consentimiento para la cesión o comunicación de datos.

El consentimiento, según el Dr. Rebollo[40], para el tratamiento de los datos es una facultad de libertad del individuo para decidir acerca de sus datos; se puede resumir estableciendo que es el interesado el que decide cuándo, dónde y cómo se presentan sus datos al exterior o se dan a conocer sus datos a terceros. Este principio puede tener sus excepciones establecidas por la normativa en su caso.

Al decir que el consentimiento es una facultad de libertad del individuo significa que éste debe ser dado libremente, sin presión física o psicológica.

Otra característica que presenta el consentimiento es que debe ser informado para que el titular del dato tiene la posibilidad de evaluar si es un riesgo o no dar sus datos personales a quien se los solicita, si el tratamiento de éstos va a ser positivo o no.

Debe ser expreso, no necesariamente escrito, característica esta última que se hace efectiva en los datos sensibles. Deberá precisarse qué tipo de datos, formas de tratamientos, y en su caso, qué comunicaciones o transferencias a terceros son las autorizadas.

La Directiva 95/46/CE define en el artículo 2º literal h) qué es el consentimiento estableciendo que “consentimiento del interesado es toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan”.

El artículo 7º establece que el tratamiento de los datos personales sólo puede hacerse si el interesado ha dado su consentimiento de forma inequívoca, salvo en determinadas circunstancias (art. 8), como en el caso de los datos de salud cuando sea necesario utilizar los datos sin el consentimiento del titular, al igual

[40] REBOLLO DELGADO, Lucrecio y otra. Introducción a la Protección de Datos. 2ª Edición, Madrid, España, 2008. Editorial Dykinson SA., pág. 127.

que lo que sucede cuando el tratamiento es necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto que éste estuviera física o jurídicamente incapacitado para dar su consentimiento.

El artículo 8º de la Directiva 95/46/CE regula el tratamiento de las categorías especiales de datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

Así, los datos que por su naturaleza puedan atentar contra las libertades fundamentales o intimidad únicamente pueden ser tratados si existe el consentimiento del interesado de acuerdo con lo establecido en el Considerando 33 de la Directiva. Es decir que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito. Deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales.

El Convenio Nº 108 no establece regulación alguna sobre la forma del consentimiento.

La LOPD al igual que la Directiva define al consentimiento del interesado como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen, (art. 3º literal h).

Las cualidades que menciona el artículo 3º literal h) sobre el consentimiento se refieren a matices concretos, y según la Agencia Española de Protección de Datos Personales, y de acuerdo con los criterios asentados por las Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, son objeto de la siguiente interpretación[41]:

Libertad en la prestación de consentimiento, que alude a la ausencia de alguno de los vicios que afectan a la voluntad según el Código Civil.

Específico, es decir, el consentimiento se refiere a un tratamiento concreto y para una finalidad determinada, explícita y legítima, según se desprende del art. 4.2 de la LOPD.

Informado, lo que supone que ha existido previa información acerca de la existencia del tratamiento y su finalidad, (art. 5.1 LOPD).

[41] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., págs. 128 y sgtes.

Inequívoco, lo cual implica que no se admite un consentimiento presunto, sino que se requiere expresamente una acción u omisión que suponga la existencia de éste. Esta última no significa que el consentimiento haya de ser en todos los casos un consentimiento expreso, sólo en aquellos casos de datos sensibles y los especialmente protegidos.

El artículo 6.3 de la LOPD menciona que los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

El consentimiento puede ser revocado cuando exista una justificación para ello y no se le atribuyan efectos retroactivos.

Como todos los principios mencionados anteriormente éste también tiene sus excepciones tanto en la Directiva como en la LOPD.

Las excepciones al consentimiento en la LOPD están dadas en el artículo 6.2 y el 22.2, es decir que el tratamiento de los datos se puede realizar sin que el titular del dato deba prestar su consentimiento.

Ellas se refieren, de acuerdo con el artículo 6.2, al ejercicio de las funciones propias de las Administraciones Públicas: los datos incluidos en un contrato o relación negocial, la protección del interés vital en los términos cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional de la salud sujeto al secreto profesional o por otra persona sometida a una obligación equivalente de secreto, cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

El artículo 22.2 se refiere a los datos personales que son recogidos y tratados por las Fuerzas y Cuerpos de la Seguridad para fines policiales, pero se deben limitar a los datos necesarios para la prevención del peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

1.6 Principio de seguridad de los datos

Este principio es esencial para la protección de los titulares del dato y su tratamiento, constituyendo parte del derecho fundamental a la protección de datos personales.

El objeto de este principio es garantizar la confidencialidad y la integridad de los datos personales impidiendo que se realice la alteración, pérdida, transmisión y acceso no autorizado de los datos.

El Convenio Nº 108 establece en su artículo 7º que se deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

La Directiva 95/46/CE establece una obligación de adoptar medidas de seguridad para proteger los datos que se encuentran en las bases de datos personales.

El artículo 17 hace mención de la obligación que tienen los responsables del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, sobre todo cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Estas medidas son de carácter técnico y de organización en relación con las personas que realizan el tratamiento de los datos, los que deberán garantizar un nivel de seguridad acorde con los riesgos que presenta el tratamiento y con la naturaleza de los datos que se protegen, de acuerdo con lo determinado en el Considerando 46 de la Directiva.

El responsable del tratamiento deberá tener un encargado de tratamiento que también cumpla con las garantías suficientes en relación con las medidas de seguridad técnicas y de organización de los tratamientos que deban efectuarse, y asegurándose su cumplimiento.

Las medidas de seguridad son un principio y una obligación de quien trata los datos personales, sea como responsable o como encargado, debiendo hacerlas cumplir, estableciéndose además que al adoptarse estas medidas se debe realizar un contrato por escrito o en otro medio que permita acreditar su adopción y cumplimiento.

De acuerdo con la LOPD la seguridad tiene tres conceptos: confidencialidad, integridad y disponibilidad. La confidencialidad protege los datos de manera que sean conocidos solo por las personas autorizadas y permanezcan vedados para el resto. La integridad impide que la información contenida en una base de datos pueda ser alterada o modificada de manera incorrecta y sin autorización de su titular. Por último, la disponibilidad se refiere a la recepción del dato a tiempo de cumplir su finalidad y por parte de los destinatarios autorizados, esto es, la accesibilidad de los datos cuando sea preciso y por quienes están facultados para ello. Garantizar la confidencialidad, la integridad y la disponibilidad es el objetivo de las medidas de seguridad[42].

No se establece cuáles son las medidas de seguridad, pero el Real Decreto Nº 994/1999, de 11 de junio de 1999, que aprueba el Reglamento sobre medidas

[42] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 148.

de seguridad de los ficheros automatizados que contengan datos de carácter personal, estableciendo que los ficheros deben tener nivel básico, medio y severo de seguridad teniendo en cuenta la naturaleza de los datos almacenados.

El Real Decreto Nº 1.720/2007, reglamentario de la LOPD también menciona los tres niveles de medidas de seguridad para la aplicación de todos los ficheros o tratamientos de datos de carácter personal, ya sean informatizados como manuales, siendo estos últimos regulados por primera vez en cuanto a las medidas de seguridad.

1.7 Principio de reserva

Este principio lo podemos encontrar con otra denominación haciendo referencia a la reserva, la confidencialidad y el secreto.

En la Directiva no se menciona este principio, sí se regula la necesidad de confidencialidad de la información.

El artículo 16 hace mención de la obligación de confidencialidad que deben tener las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último; sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o en virtud de un imperativo legal.

El Convenio Nº 108 nada dice sobre este principio, sólo menciona la confidencialidad y el deber de secreto en su artículo 15 numeral 2, al determinar que: cada parte cuidará de que las personas pertenecientes a la autoridad designada o que actúen en nombre de la misma estén vinculadas por obligaciones convenientes de secreto o de confidencialidad con respecto a dicha información.

La LOPD establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable de éste.

Este secreto que establece la LOPD no debe confundirse con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen. Éste es un deber genérico que alcanza a cualquier persona que intervenga en el tratamiento de los datos[43].

1.8 Principio de responsabilidad

[43] VIEGA, Ma. José. Los principios jurídicos en la Protección de Datos Personales. Análisis comparativo de la Directiva de la Unión Europea, la Ley Española y la Ley Uruguaya. Trabajo final del Curso a Distancia Experto Universitario en Protección de Datos Personales de la Universidad Nacional de Educación a Distancia. España, 2009-2010.

El Considerando 55 de la Directiva 95/46/CE menciona levemente el principio de responsabilidad al decir que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito de sus datos personales han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor.

El Convenio Nº 108 nada dice acerca de este principio, al igual que la LOPD.

Como mencionamos al comienzo del capítulo, la comunidad experta en Protección de Datos y Privacidad alude a este principio, incluyendo la responsabilidad por daños, incluso si las operaciones de tratamiento se llevan a cabo por prestadores de servicios que actúen por cuenta del responsable.

Éste deberá adoptar las medidas necesarias para cumplir con los principios y obligaciones que se establecen en el documento y en las legislaciones nacionales que se aplicaren, así como proveerse de los mecanismos necesarios para demostrar el cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias.

2. DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

2.1 Introducción

Los principios no serían tales si el ciudadano no tuviera la posibilidad de ejercer los derechos que nacen por ellos.

Estos derechos se ven reflejados en la normativa que regula la autodeterminación informativa, pero a su vez son consagrados como derechos fundamentales, es decir derechos que son inherentes a la personalidad humana y que están consagrados en las Constituciones de los Estados reconociéndolos y garantizándolos.

En algunos de los Estados, como el Español, el constituyente ha tenido, en el apartado 4 del artículo 18 de la Constitución de 1978, la intención de garantizar algo distinto que el derecho a la intimidad o el secreto de las comunicaciones amparados en apartados anteriores del artículo. Este apartado incorpora una nueva garantía constitucional, en respuesta a las nuevas amenazas que las modernas tecnologías de la información suponen para la dignidad y los derechos de las personas. Sin embargo a diferencia de otras regulaciones constitucionales de la época, no recoge los elementos que formarían el contenido esencial del derecho a la autodeterminación informativa[44]. En cambio en muchas de ellas no los designan directamente como en nuestra Constitución, pero si en la ley.

Pablo Murillo de la Cueva defendió la existencia de un nuevo derecho fundamental, considerando necesario abandonar el concepto clásico de

[44] GARRIGA DOMINGUEZ, Ana. Tratamiento de datos personales y derechos fundamentales. Madrid, España, 2004. Editorial Dykinson, pág. 33.

intimidad y optar por el nuevo concepto de autodeterminación informativa que pretende satisfacer la necesidad de las personas de reservar su identidad, controlando la revelación y uso de los datos que les conciernen, y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos, propia de la informática y de los peligros que esto supone[45].

La normativa mencionada anteriormente nos muestra la aparición de un acervo común europeo que, como se verá en los capítulos siguientes, son el antecedente más cercano de nuestra legislación respecto a la protección de datos personales, en lo que se refiere a los principios como a los derechos.

2.2 Derecho de información

El derecho de información está consagrado en la Directiva 95/46/CE en el Capítulo II, Sección IV "Información del Interesado", artículos 10 y siguientes.

Quien tiene el deber de informar al interesado es el responsable del tratamiento de la base de datos o su representante, acerca de los datos que posee de él, siempre y cuando ya no lo hubiera hecho en otra ocasión.

La enunciación de los datos no es taxativa, al contrario, ya que la propia Directiva establece que se deberá proporcionar al interesado "por lo menos la información que se enumera". Esta comprende: quién es el responsable o su representante del tratamiento, los fines del tratamiento de que van a ser objeto los datos, cualquier otra información como la existencia de derechos de acceso y rectificación, los destinatarios o las categorías de destinatarios de los datos.

Si la información que se tiene no ha sido recabada del interesado sino por otros medios, se deberá informar a éste qué datos se tienen de él, desde el momento del registro de los datos o en caso que piense realizar comunicación de datos a un tercero, a más tardar en el momento de la primera comunicación. También enumera cuáles son los datos a informar al interesado pero como información mínima.

Es de tener en cuenta que no será necesario informar al interesado en los casos que los datos sean usados para el tratamiento con fines estadísticos, investigación histórica o científica, así como cuando la información no puede realizarse porque resulta imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas para proteger los datos personales del individuo.

Siguiendo con el derecho español, la Ley Orgánica Nº 15/1999 de Protección de Datos de Carácter Personal, regula en su artículo 5.1 el derecho de información en la recogida de los datos.

---

[45] MURILLO DE LA CUEVA, Pablo citado por BUISAN GARCIA, Nieves y otros. La ley de protección de datos: análisis y cometarios de su jurisprudencia. Madrid, 2002. Editorial Lex Nova, pág. 326.

A diferencia del derecho de información reglado en la Directiva Europea se establece cuáles son las características de éste al decir que será “expreso, preciso e inequívoco”, es decir que este derecho es anterior al principio del previo consentimiento informado, ya que el interesado para dar su consentimiento es necesario que sea informado. Esto sucederá también en caso que los datos no hayan sido recabados del interesado, en este caso el interesado debe ser informado dentro de los tres meses siguientes al momento del registro.

Se menciona en el artículo 5º de la LOPD cuáles son los datos que se deben informar al interesado, entre otros: finalidad de la recolección de los datos, carácter obligatorio de responder las preguntas o no, consecuencia de la obtención o no de los datos, posibilidad de ejercer los demás derechos de protección de datos personales (acceso, rectificación, cancelación, oposición), quién es el responsable del tratamiento o de su representante.

Al igual que en toda la normativa referente a la protección de datos personales en la LOPD existen excepciones respecto al derecho de información.

Éstas se recogen en el artículo 5.5, y en el artículo 24.1. En el primero de ellos se menciona como excepción la existencia de una ley que expresamente lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, cuando resulte imposible o exija esfuerzos desproporcionados a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias, cuando sean recogidos de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. Esta última excepción tiene como carácter previo a su realización la intervención del órgano de control nacional o de los autonómicos.

En el artículo 24.1 se dice que no serán informados los interesados cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

Con respecto a estas excepciones para precisar la interpretación de los términos y delimitar los conceptos de datos históricos la Agencia Española de Protección de Datos Personales puntualizó siguiendo la Ley Nº 16/1985, de 25 de junio, que regula el Patrimonio Histórico Español, que siempre que se cumpla con los plazos previstos de 25 años (contados desde el momento de la muerte del interesado si es conocido) o de 50 años (contados a partir de los documentos en otro caso) sería posible el tratamiento de los datos, por ser calificados como históricos. Si los datos no cumplen con la antigüedad mencionada se requerirá el consentimiento del afectado para su tratamiento y divulgación.

En cuanto a los datos estadísticos habrá que atenerse a lo mencionado en la Ley Nº 12/1989, de 9 de mayo, y a la normativa de las Comunidades Autónomas, y dependerá del contexto de su utilización la consideración de dato científico.

2.3 Derecho de acceso

En el derecho comparado el derecho de acceso está consagrado en diversa normativa. Entre ella se encuentra el artículo 8º literal b) del Convenio Nº 108 del Consejo de Europa, que reconoce el derecho de los interesados a obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible. En este artículo no se establece cuál es la interpretación de la frase “a intervalos razonables”.

En los artículos 12 y 13, Sección V “Del Derecho de Acceso del interesado a los datos”, Capítulo II de la Directiva 95/46/CE, establece que el derecho de acceso se debe ejercer en forma libre, sin restricciones, en intervalos razonables de tiempo al igual que en el Convenio Nº 108, sin retrasos cumpliendo con el plazo estipulado para la respuesta y sin gastos excesivos para el titular del dato, en forma inteligible para el titular de los datos.

El responsable del tratamiento de los datos debe dar a conocer la existencia o no de la información sobre los datos personales que tenga en sus bases de datos del interesado.

Como mínimo debe proporcionarle información sobre la finalidad del tratamiento de los datos, los destinatarios o las categorías de destinatarios a quienes se comuniquen los datos, el origen, la rectificación, supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, la notificación a los terceros a quienes se hayan comunicado de éstos de toda rectificación, supresión o bloqueo, siempre que no sea un esfuerzo hacerlo.

Este derecho de acceso tiene límites en cuanto a su ejercicio, cuando esta limitación constituya una medida necesaria para la salvaguarda de la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección y represión de infracciones penales o de la deontología de las profesiones reglamentadas, de un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales, una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos de seguridad pública, interés económico o financiero del Estado, de la protección del interesado o de los derechos y libertades de otras personas.

Cuando se trate de personas concretas y para garantizar su intimidad, el Estado puede limitar su ejercicio, mediante una disposición legal cuando los datos se vayan a tratar con fines de investigación científica o se guarden en

forma de bases de datos de carácter personal durante un período que no supere el tiempo necesario para la finalidad de la elaboración de estadísticas.

La legislación española, en la LOPD, artículo 15, regula el derecho de acceso teniendo como antecedente la Directiva 95/46/CE.

Este derecho debe ser ejercido por su titular o su representante. Mediante la solicitud va a obtener información de cuáles son sus datos sometidos a tratamiento, el origen de ellos, las comunicaciones que se han realizado o se pretenden realizar.

Su obtención es gratuita pero se debe realizar en intervalos no inferiores a doce meses, lo que resulta una diferencia con la Directiva y el Convenio Nº 108, ya que ambos establecían un período de tiempo razonable pero no se determinaba cuál era. Existe una excepción al tiempo y es que si el titular del dato personal justifica la necesidad de acceder a los datos en un período más breve, teniendo un interés legítimo puede hacerlo.

Dicho artículo además dispone que la información podrá obtenerse mediante la consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos teniendo el titular que realizar gastos extras para su decodificación.

El responsable de la base de datos o tratamiento tiene un plazo para resolver el pedido de acceso que alcanza un máximo de un mes a contar desde el momento de la solicitud, y el acceso debe hacerse en un plazo de diez días siguientes a la notificación, de acuerdo con lo regulado por el Real Decreto Nº 1.720/2007, de 21 de diciembre de 2007. Si no entrega la información en el plazo estipulado debe comunicarlo al interesado mencionando las razones por qué no lo hace.

Puede denegar el derecho de acceso porque ya se ejercitó en el período establecido de 12 meses, salvo que acredite un interés para volver a solicitarlo, así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso, (artículo 30 LOPD); por último puede dirigirse a la Agencia Española de Protección de Datos, o al órgano equivalente en cada Comunidad Autónoma, con copia de la solicitud y de la contestación recibida, siempre y cuando la tenga, y efectuar la reclamación de la tutela de sus derechos.

En cuanto a la denegación debemos tener en cuenta si la base de datos es pública o privada. Si es de titularidad pública en el caso de los artículos 23.1 y 2º de la LOPD se establecen excepciones mencionando entre ellas los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, de igual forma pueden hacerlo los

responsables de las bases de la Hacienda Pública cuando se pueda obstaculizar algún procedimiento de fiscalización o inspección, por ejemplo.

A las bases de titularidad privada se les aplica también el artículo 15.3 de la LOPD en cuanto al intervalo de tiempo que debe pasar entre cada solicitud de acceso, salvo que tenga un interés legítimo para pedirlo antes de finalizado el plazo de doce meses.

Hay que tener en cuenta que se permite que un órgano administrativo o un particular procedan a calificar un interés legítimo, quizás con unas facultades un tanto desproporcionadas, y que de esa calificación dependa una limitación al ejercicio de un derecho fundamental, como es el ejercicio del derecho de acceso46.

Si son bases de datos de titularidad privada al igual que aquéllas públicas si no es el titular o un tercero que lo represente debidamente, también se le puede denegar el derecho al acceso a los datos del titular.

2.4 Derecho de rectificación, actualización, inclusión, supresión, u oposición

Con respecto a los derechos de rectificación, actualización, inclusión o supresión veremos que la normativa en el derecho comparado no está unificada, ya que pueden aparecer recogidos en alguna de ellas uno o más de estos derechos, o tener diferente denominación como es el caso de la Ley Orgánica Nº 15/1999 que nos habla de derechos de rectificación y de cancelación.

Estos derechos muchas veces se ejercen como consecuencia del derecho de acceso, ya que al conocerse los datos del titular se verifica que no son los correctos.

No pueden ser ejercitados por cualquiera, debido a que tienen el carácter de personalísimos y por ello es muy importante que se tomen las medidas necesarias a la hora de ejercerlos, evitando perjuicios tanto para el interesado como para el responsable de la base de datos.

El Convenio Nº 108 del Consejo de Europa sólo se refiere en su artículo 8º literal c) a la rectificación o borrado de los datos en caso que se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en él.

En la Directiva 95/46/CE se recogen los derechos de rectificación y supresión en su artículo 12 literales b) y c) y en el artículo 14 el derecho de oposición.

Así los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la

[46] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 203.

Directiva, sobre todo a causa del carácter incompleto o inexacto de ellos; también garantizará la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo, si no resulta imposible o supone un esfuerzo desproporcionado.

En cuanto al derecho de oposición el interesado puede oponerse en cualquier momento y por razones legítimas de su situación particular cuando sean necesarios para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección, a que sus datos sean objeto de tratamiento salvo que la legislación nacional disponga de otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos.

También podrá el titular de los datos oponerse previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección, o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Este derecho de oposición lo encontramos en la Directiva mencionada anteriormente y en la Ley Orgánica Nº 15/1999, la que por primera vez lo introduce en el derecho español, ya que la LORTAD no lo regulaba.

El interesado en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos. El responsable del sistema de datos tendrá que proceder a la exclusión de los datos relativos al afectado[47].
Su limitada regulación normativa ha sido suplida por los arts. 34 a 36 de la RD Nº 1.720/2005, de 21 de diciembre, prevé por primera vez este derecho, estableciendo que el interesado tiene derecho a que no se traten sus datos personales o cesen en su tratamiento cuando no sea necesario su consentimiento para el tratamiento, por concurrir un motivo legítimo y fundado, referido a su situación personal, o sea bases de publicidad y prospección comercial, o cuando el tratamiento tenga por finalidad la decisión basada en el tratamiento automatizado de datos.
Retomando los derechos de rectificación y cancelación, la LOPD los regula previendo que se posibilite al interesado, que constate que sus datos personales figuren en una base de forma inexacta o incompleta, a dirigirse al responsable, mediante la correspondiente solicitud, para que proceda a la rectificación de sus datos que resulten pertinente, indicando cuál es el que se

[47] IFAI. Estudio sobre Protección de Datos a nivel internacional. México, 2008, pág. 100.

estima erróneo y la corrección que debe realizarse, debiendo acompañar la documentación que justifique el cambio.
Si éstos hubieran sido cedidos por algún motivo, previamente a un tercero, el responsable de la base tiene la obligación de notificar al cesionario la rectificación realizada.
El derecho de cancelación permite al interesado, titular de los datos, pedirla si sus datos han dejado de ser necesarios o pertinentes para la finalidad para la cual fueron registrados.
Como vemos son dos derechos diferentes ya que la rectificación no significa borrado o destrucción física de la información, sino la sustitución de unos datos inexactos o incorrectos por otros actuales y correctos, pero siempre que no exista una desviación del fin, o un uso desproporcionado de los mismos, o una revocación del consentimiento prestado[48].
Muchas veces en algunas normas se precisa que la cancelación no debe suponer automáticamente el borrado físico de los datos, sino simplemente su bloqueo, es decir que no puede exigir el borrado total y absoluto de los datos. El bloqueo debe contar con todas las características de seguridad, ya que el borrado total de los datos no permitiría atender otras obligaciones, legales o contractuales, por no existir ya rastro alguno sobre los datos, como pueden ser requerimientos especiales para los jueces o la Administración Pública.

2.5 Derecho a la impugnación de valoraciones personales

La legislación regula el derecho a la impugnación de valoraciones personales mediante el tratamiento automatizado de datos como un derecho fundamental que tiene el titular de los datos personales.

El artículo 15 de la Directiva 96/45/CE regula el derecho del interesado a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros.

Respecto a este derecho existen excepciones, tales como: se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo, o esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

La legislación española regula este derecho en el artículo 13 de la LOPD, tiene como base el derecho a ser prejuzgado mediante aspectos relacionados con su personalidad y solamente debe ser pedida por el afectado para que tenga valor probatorio.

Todo titular de datos personales tiene derecho a impugnar una resolución que le afecte significativamente, y que se base en tratamientos que evalúen

[48] CEDDET. Ob. Cit. Módulo 2, pág. 255.

determinados aspectos de su personalidad; quien se vea afectado por tal resolución podrá impugnar estos actos, ya sean administrativos o decisiones privadas que impliquen una valoración de su comportamiento, pudiendo obtener información del responsable de la base de datos sobre cuáles fueron los criterios de valoración y los programas utilizados en el tratamiento, que hicieron que se llegaran a determinadas conclusiones afectándolo.

La LOPD no establece que el tratamiento sea automatizado como lo mencionaba la LORTAD y al decir de Emilio del Peso Navarro[49] es el resultado de una mala transposición de la Directiva 95/46/CE, ya que con el fin de anular la palabra automatizado, se sacó hasta de dónde no se debía.

2.6 Otros derechos referentes a la comunicación de datos

En el derecho comparado se regulan, además de los derechos comunes a las normas mencionadas, otros derechos referentes a la protección de datos como por ejemplo, el derecho de indemnización en el derecho español.

El derecho de indemnización se regula en el artículo 19 de la LOPD, estableciendo que si el responsable de la base de datos o el encargado de tratamiento incumplen con la Ley y los titulares del dato sufren algún daño o lesión en sus bienes o derechos estarán legitimados para ejercerlo.

Hay que diferenciar las bases de titularidad pública de las de titularidad privada. En las primeras la responsabilidad se exigirá de acuerdo con la normativa que regula la responsabilidad de la Administración Pública. En las segundas se ejercitará ante los órganos de la jurisdicción ordinaria. El interesado puede recurrir a Tribunales con objeto de obtener una compensación, cuando éste haya visto vulnerado sus derechos.

Este derecho acoge la responsabilidad extracontractual del artículo 1902 del Código Civil Español, ya que en aquellos supuestos en los que exista una previa relación jurídica entre el interesado y el responsable o encargado, la obligación de indemnizar dimanará del propio contrato, en cuanto se hayan incumplido las obligaciones en él estipuladas[50].

3. CONCLUSIONES

Tanto los principios como los derechos, en su conjunto:

a) rigen el marco del derecho de la protección de datos,

b) fomentan la autodeterminación informativa, el titular del dato tiene el derecho de poner los límites al mal uso de éstos,

c) buscan concientizar al titular del dato, a la Administración Pública y a los privados en general sobre este derecho fundamental,

---

[49] DEL PESO NAVARRO, Emilio. Ley de protección de datos: la nueva LORTAD. Madrid, España, 2000. Editorial Díaz de Santos, pág. 170.
[50] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 61.

d) cambian aspectos relativos al tratamiento de los datos sensibles, de los de solvencia patrimonial y crédito, telecomunicaciones, marketing,

e) evitan la comunicación y la transferencia de datos personales no autorizados.

CAPÍTULO III – LA LEY Nº 18.331 DE PROTECCIÓN DE DATOS PERSONALES

Dra. Ma. José Rodríguez Tadeo

1. INTRODUCCIÓN

Es un hecho de la realidad que tanto empresas, profesionales, como entidades públicas recolectan y tratan datos personales de sus funcionarios, empleados, administrados, clientes, conformando bases de datos en soporte papel o informático, con finalidades múltiples. Ello hace que día a día el procesamiento y automatización de la información se incremente, generando la necesidad de proteger la intimidad y el derecho a la protección de los datos personales.

La Ley Nº 18.331 tiene como objetivo fundamental la protección de este importante derecho que en puridad implica que la persona pueda ejercer un poder de control sobre sus datos.

En el presente trabajo se examinarán aquellos aspectos de la norma que resultan esenciales desde dos perspectivas diferenciadas: contenido y aplicación.

Se hará fundamental hincapié en los derechos que se derivan del derecho a la protección de los datos personales y de los principios generales que le dan sustento y a la vez marcan los requerimientos de su utilización, reforzando, en este marco, el estudio de la comunicación o cesión de datos.

Asimismo, se destacará la importancia que reviste el registro de las bases de datos, no visualizándolo estrictamente como una obligación, sino como una garantía de calidad de la empresa o entidad.

Finalmente, haremos una breve descripción del procedimiento judicial de Habeas Data y de uno de los cometidos que ostenta el Órgano de Control a la hora de evaluar las conductas infractoras a las disposiciones de la Ley, como es la potestad sancionatoria.

2. EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

El derecho a la protección de datos personales es un derecho consagrado en la Constitución de la República, en los artículos 7º, 72 y 332.

También resulta regulado en instrumentos internacionales como el Pacto Internacional de Derechos Civiles y Políticos, Pacto de San José de Costa Rica, Declaración Universal de los Derechos del Hombre, todas ratificadas por Uruguay.

El derecho a la protección de datos personales consiste en el poder de disposición y de control sobre los datos personales que se concretan 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.[51]

Este derecho comprende los datos que afectan a la vida íntima de la persona, pero también a todos aquéllos que la identifiquen o puedan identificarla y, al hacerlo puedan provocar un perjuicio para la persona.[52] Es decir, aspectos vinculados tanto a la intimidad, como a la privacidad del sujeto.

Hasta el momento de la sanción de la Ley Nº 18.331, de Protección de Datos Personales y Acción de Habeas Data (LPDP), existía la Ley Nº 17.838 que sectorizaba la protección de los datos personales a aquéllos que se utilizaban únicamente para fines comerciales.

Con la LPDP se consagró el marco jurídico adecuado para la regulación de este derecho, en sentido amplio, describiéndolo como un derecho inherente a la persona humana, comprendido en el artículo 72 de la Constitución de la República.

2.1. Ámbito subjetivo de aplicación de la Ley

Pese a ser un derecho inherente a la persona humana, el artículo 2º de la LPDP extiende su ámbito de aplicación a las personas jurídicas, en cuanto corresponda.

Es decir que la persona jurídica, como entidad moral, podrá, según el caso, ejercer también el poder de control sobre los datos que la identifiquen o puedan identificarla.

2.2. Ámbito objetivo de aplicación de la Ley

El régimen de la Ley se aplica a aquellos datos personales que se registren en cualquier tipo de soporte y que sean objeto de tratamiento, ya sea en el sector público o privado, conforme lo dispuesto por el artículo 3º de la LPDP).

La Ley involucra dos conceptos, el de dato personal y el de tratamiento o procesamiento de datos.

El primero de ellos implica que los datos deben referir a una persona, ya sea física o jurídica, que la identifiquen particularmente o la puedan hacer identificable, esto es, que de dicha información pueda revelarse su identidad. Es decir, desde su nombre hasta cualquier otro dato que pueda revelar información sobre sus hábitos, gustos, inclinaciones, forma de vida. Así

---

[51] Sentencia del Tribunal Constitucional de España 292/2000, de 30 de noviembre de 2000.

[52] 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, 2009, págs. 13-14.

podemos mencionar nombre, domicilio, teléfono, correo electrónico, número de socio, número de funcionario, una foto, la voz.

Por otra parte, el tratamiento de datos alude a aquellas operaciones sistemáticas que permitan el procesamiento, la cesión o comunicación, así como consultas, interconexiones o transferencias, de acuerdo con lo dispuesto por el artículo 4º literal M.

Aunque la definición que brinda el artículo 4º literal M) no incluye a texto expreso la recolección o colecta de datos personales, entendemos debe considerarse inserta como una operación o procedimiento que permite el procesamiento de los datos.

Sobre este aspecto, tanto la Ley Orgánica Española de Protección de Datos de Carácter Personal 15/1999, como la Ley Argentina de Protección de Datos Personales Nº 25.326, incluyeron a texto expreso la “recogida” y “recolección” como categorías de “tratamiento de datos”, en sus artículos 3º literal c) y 2º, respectivamente.

En consecuencia, todo aquel tratamiento de datos que involucre datos personales, ya sea en la órbita pública como privada y sea registrado informáticamente o en papel, quedará inserto dentro del ámbito objetivo de la norma.

No resultará comprendida, en cambio, la información que registre datos de naturaleza contable o estadística que no revele la identidad de persona alguna.

Ahora bien, el artículo 3º exceptúa del ámbito de aplicación de la Ley a las siguientes bases de datos:

- El literal A) excluye a aquéllas mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Este literal ha traído dificultades interpretativas en mérito a lo previsto en el artículo 28, en su antigua redacción, en tanto establecía la obligación de registro a las personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos personales que no sean para un uso exclusivamente individual o doméstico.

¿Podría entenderse que una persona jurídica privada que tenga las bases de datos de una empresa tipo (clientes, proveedores y empleados) circunscribe sus actividades y tales bases de datos en un ámbito individual o doméstico?

Sin lugar a dudas arribaríamos una respuesta negativa.

El ámbito doméstico alude específicamente a lo hogareño, a lo individual, pudiendo ser portadoras de bases de datos de este tenor, únicamente las personas físicas (clásicas agendas de familiares y amigos), pero de ningún modo las personas jurídicas, donde siempre existe una finalidad lucrativa,

societaria, académica, o de cualquier otro carácter, que las exime de catalogarlas como estrictamente individual.

Quienes entiendan lo contrario, habrán descontextualizado las previsiones contenidas en el artículo 3º literal A) y en todo el cuerpo normativo.

Como decía el Maestro Jiménez de Aréchaga refiriéndose a la interpretación de un texto constitucional –enteramente aplicable a una disposición legal– "(...) la primera técnica de interpretación debe ser el respeto por el texto literal, claro está, sobre la base de entenderlo armonizando el tenor de cada una de las disposiciones con el conjunto de las otras disposiciones. En cuanto el tenor sea claro, aplicarlo rigurosamente. La claridad que debe requerirse no la claridad gramatical, sino la claridad jurídica. Un texto puede ser gramaticalmente claro y resultar jurídicamente absurdo. La tarea de interpretación del Derecho es una tarea para juristas y no para gramáticos. No separarse del texto sin gran cautela (...). Por lo demás, la interpretación no puede hacerse jamás contra el texto".[53]

Por su parte, el Decreto Nº 414/009, de 31 de agosto de 2009, reglamentario de la LPDP, excluye expresamente del régimen jurídico de la protección de datos personales, a las bases de datos mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, entendiéndose por éstas las que se desarrollan en un ámbito estrictamente privado, entre otros, los archivos de correspondencia y agendas personales, de acuerdo con el artículo 2°, literal A).

A lo interior se añade la Ley Nº 18.719, de Presupuesto Nacional, de 27 de diciembre de 2010 que para saldar cualquier atisbo de duda interpretativa que pudiera subsistir, introduce modificaciones al artículo 28 de la LPDP, suprimiéndole la categorización de base de datos que no sea para un uso exclusivamente individual o doméstico.

- El literal B) del artículo 3º de la LPDP, también excluye del ámbito de aplicación de la Ley, a las bases de datos cuyo objeto sea la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

Sin embargo, el artículo 25 de la LPDP incluye dentro del régimen de la Ley, a los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia y aquéllos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

- Finalmente, el literal C) exceptúa a las bases de datos creadas y reguladas por leyes especiales.

---

[53] JIMÉNEZ DE ARÉCHAGA, Justino. "La Constitución Nacional", Tomo I, Edición Cámara de Senadores, Montevideo, 1992, págs. 149-153.

La LPDP exige tres requisitos conjuntamente, es decir que la base de datos no solo debe ser creada, sino también regulada por una ley que debe revestir la naturaleza de especial.

3. DEFINICIONES CONTENIDAS EN LA LEY (artículo 4°)

3.1. Dato personal

Dato personal, según el literal D) es "Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables".

La Ley maneja un concepto amplio de datos personales, incluyendo datos sensibles, sonidos, imágenes, datos biométricos, como por ejemplo, retina e iris, huella dactilar, patrón facial, geometría de la palma de la mano.

Abarca todo tipo de informaciones sobre la persona, ya sean de tipo objetivo o subjetivo, cualquiera sea su clase, incluyendo los datos sensibles.

El concepto de "determinada o determinable" se relaciona con la posibilidad de identificar o hacer identificable a una persona.

El Dictamen 4 del Grupo de Trabajo del Artículo 29 establece que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, características de su identidad física, fisiológica, psíquica, económica, cultural o social". [54]

De manera que no es necesario que la información relativa a una persona la identifique directamente, como por ejemplo su nombre y apellido, sino que de alguna manera la pueda hacer determinable, a través de su documento de identidad, de su teléfono.

Por enunciar algunos ejemplos más, de los ya relatados, se consideran datos personales, una fotografía, la voz, el número de socio de un club deportivo, el correo electrónico, la huella dactilar, el ADN.

3.2. Dato sensible

Existen datos personales que por sus características merecen una protección especial.

Datos sensibles, según el literal E) del artículo 4° son los que revelan origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

Respecto a estos datos la Ley establece que nadie está obligado a proporcionarlos y que es necesario contar con el consentimiento expreso y escrito del titular.

---

[54] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf Página visitada el 7 de abril de 2011.

Para su recolección y tratamiento es necesario que existan razones de interés general autorizadas por Ley o que el organismo esté autorizado por Ley.

Asimismo, se prevé la posibilidad de que se utilicen esos datos con fines estadísticos o científicos, en cuyo caso deberán disociarse de manera que no puedan identificar a su titular.

La Ley, en el artículo 18 establece un principio esencial cual es la prohibición de la conformación de base de datos que almacenen información relativa a datos sensibles, excepto las que refieran a partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro para lograr el cumplimiento de sus finalidades.

Ahora bien, existen entidades públicas o privadas que para cumplir con la finalidad de tratamiento de datos personales de sus recursos humanos necesitan de determinados datos sensibles. Tal es el ejemplo de la afiliación a un sindicato o de la afección de determinadas enfermedades. Toda esta información de carácter sensible puede integrar el conglomerado de datos personales de una base de datos personales de recursos humanos, sin incumplir con la previsión legal referida en tanto resulta imprescindible para el cumplimiento de sus cometidos.

Por otra parte, el artículo 18 prevé que los establecimientos sanitarios públicos o privados y los profesionales de la salud podrán tratar datos personales relativos a la salud de las personas que acuden a ellos, de acuerdo con la legislación sanitaria, y guardando el deber de secreto profesional. También podrán ser tratados estos datos cuando sea necesario para salvaguardar la vida del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para prestar su consentimiento.

Asimismo, los datos personales relacionados con infracciones penales, civiles o administrativas sólo pueden ser tratados por las autoridades competentes. Estas autoridades podrán comunicar o hacer pública la identidad de las personas que estén siendo investigadas o hayan cometido infracciones, cuando una norma lo establezca o cuando lo consideren conveniente.

3.3. Base de datos

“Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso”, conforme lo previsto por el literal A.

La LPDP incluye dentro de su ámbito de aplicación a las bases de datos informatizadas, a las no informatizadas, es decir, las llevadas en soporte papel, y a las mixtas, esto es aquéllas que llevan datos personales, parte en soporte papel y parte de manera informatizada.

El aspecto informático debe entenderse en sentido amplio, esto es, desde aquella base de datos conformada por un programa específico para soportar bases de datos, hasta una planilla Excel o archivos en Word. La nota está dada en la utilización de una herramienta informática para el almacenamiento de los datos personales.

Ahora bien, para que ese conjunto de datos personales adquiera la nota de "Base de Datos" debe estar estructurado de forma organizada de manera que se pueda acceder fácilmente a los datos de una persona en particular.

A modo de ejemplo:

Si una empresa u Organismo almacena los datos personales de sus proveedores o empleados por orden alfabético, cédula de identidad, número de funcionario, estará sometido a la LPDP, en tanto se trata de un conjunto organizado de datos que permite acceder sin esfuerzo a los datos de una persona en concreto.

Si por el contrario, se almacenan por criterios donde no resulta fácil el acceso a la información, tal como por fecha de recepción, no será aplicable la normativa de protección de datos.

Puede darse la hipótesis, asimismo, que una entidad pública o privada tenga información relativa a sus empleados, soportada en herramientas informáticas, pero también posea carpetas en papel donde se identifica al empleado y se anexa toda la información en papel relativa a éste. No se trata en este caso de dos bases de datos diferentes, sino de una única base de datos de recursos humanos, de naturaleza mixta.

3.4. Titular de los datos

"Persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la LPDP", de acuerdo con lo establecido en el literal L.

El titular de los datos puede ser tanto una persona física, como una persona jurídica y no es necesario que sea determinada o identificada, sino que basta que a través de algún dato, pueda resultar determinable o identificable, por su correo electrónico, su dirección o número de socio de una Asociación Deportiva a la que concurre habitualmente.

3.5. Tratamiento de datos

"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", de acuerdo con lo dispuesto por el literal M.

El tratamiento de datos implica una actividad de elaboración, modificación, intercambio o comunicación de datos.

Puede ser manual o automatizado, dependiendo de que se utilice o no la tecnología para realizar el procesamiento, almacenamiento y explotación de los datos personales.

Son ejemplos típicos de tratamiento de datos, una consulta, una comunicación de datos.

3.6. Consentimiento del titular

"Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne", en virtud de lo edictado en el literal C.

El consentimiento es toda manifestación de voluntad por la cual una persona interesada permite el tratamiento de los datos personales que le pertenecen.

Este consentimiento tiene que ser libre, cierto, evidente, referido a una determinada operación de tratamiento y debe revestir la característica de informado, es decir que la persona tiene que conocer la existencia del tratamiento y su finalidad.

El artículo 13 de la Ley establece la obligación que tienen los responsables de bases de datos de informar a los ciudadanos de la finalidad para la que serán tratados sus datos y de los destinatarios de la información, de la existencia de la Base de Datos, de la identidad y dirección del responsable, así como de la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos.

Esta obligación por parte del responsable es la regla general, salvo que la información se deduzca incuestionablemente de la naturaleza de los propios datos personales y de las circunstancias en las que se produce la recolección.

Los datos sensibles, por sus especiales características, siempre requieren el consentimiento en forma previa, expresa e informada para su tratamiento.

3.7. Responsable

"Persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento", de acuerdo con lo previsto por el literal K.

El responsable de la base de datos es aquél que decide su creación, la finalidad, el contenido y uso de los datos personales registrados.
Le compete recabar y guardar la prueba de la existencia del consentimiento o de la negativa del titular a darlo para el tratamiento de los datos, a través de cualquier medio conforme a derecho.

Deberá, también dar respuesta a los titulares de los datos que ejercen sus derechos de acceso, rectificación, actualización, inclusión y supresión, en los plazos previstos por la LPDP, o fundar su negativa.

Por otra parte, tiene a su cargo la adopción de las medidas de seguridad que sean necesarias, a efectos de garantizar la integridad y confidencialidad de los datos personales.

3.8. Encargado del tratamiento

"Persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento".

La característica fundamental del encargado de tratamiento es que actúa por cuenta del responsable.

Es común que determinadas entidades contraten la realización de servicios por cuenta de terceros, por ejemplo para gestionar la contabilidad de la empresa, para la distribución de documentación, para el mantenimiento de los equipos.

En el caso del encargado de tratamiento, no se verifica una comunicación de datos, por lo que no es necesario el cumplimiento de los requisitos establecidos en el artículo 17 de la LPDP.

No obstante, la relación entre el responsable y el encargado de tratamiento debe formalizarse a través de un contrato por el cual se estipulen claramente las obligaciones de éste en cuanto a que observará las disposiciones de la LPDP para el tratamiento de los datos personales y no los comunicará sin el consentimiento de su titular.

3.9. Comunicación de datos

"Toda revelación de datos realizada a una persona distinta del titular de los datos", de acuerdo con lo establecido por el literal B.

El artículo 17 de la LPDP establece como regla general que los datos personales solo pueden ser comunicados a terceros, con el consentimiento previo del titular de los datos.

Sin embargo, la LPDP establece excepciones en las que no es necesario dicho consentimiento para que se efectúe una comunicación o cesión de datos, las que serán analizadas en el numeral 6.

3.10. Disociación de datos

"Todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable", conforme lo dispone el literal G.

Es decir que el dato disociado no permite la identificación de una persona.

De este modo, el dato disociado, pierde el carácter de dato personal y en consecuencia queda fuera de la LPDP, siendo innecesario requerir el consentimiento del titular para el tratamiento de sus datos.

3.11. Destinatario

"Persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero", literal F.

El destinatario se constituye, entonces, en receptor de la comunicación formulada por el emisor.

3.12. Tercero

"Persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento", literal J.

Un ejemplo de tercero es un gestor que se encarga de la recuperación de activos de una empresa que posee una Base de Datos.

4. PRINCIPIOS GENERALES

Los principios generales que enmarca la LPDP se erigen como la base fundamental para el procesamiento o tratamiento de los datos personales a la vez que resultan una herramienta interpretativa esencial a la hora de resolver la aplicación de las disposiciones de la Ley.

De manera que, los responsables de bases de datos, encargados de tratamiento y todas aquellas personas que traten datos personales, deberán ceñirse al cumplimiento de tales principios.

4.1. Principio de Legalidad

El artículo 6º de la LPDP indica que una base de datos será legítima si se ha registrado debidamente ante el Órgano de Control y cumple con las disposiciones de la Ley y las reglamentaciones que se dicten. Asimismo se establece que las bases de datos no podrán tener finalidades violatorias de derechos humanos, ser contrarias a la ley o a la moral pública.

Este principio debe ligarse necesariamente a las disposiciones que prevén el deber de registro. Así, todas aquellas personas físicas o jurídicas que posean bases de datos conforme la definición que brinda la LPDP, tienen la obligación de inscribirse.

Este deber de registro acarrea responsabilidad a sus incumplidores. De manera que si un titular de datos personales se siente agraviado por el tratamiento de sus datos por parte de una empresa o entidad determinada y formula ante el Órgano de Control una denuncia formal, éste al evaluar la conducta infractora,

hará jugar el hecho de no haberse inscripto a efectos de la graduación de la eventual sanción a imponer.

4.2. Principio de Veracidad

El artículo 7º de la LPDP regula el principio de veracidad de los datos, exigiendo a los responsables aplicar un criterio de proporcionalidad en la recolección y en el tratamiento de los datos personales. Éstos deberán ser veraces, adecuados, ecuánimes y no excesivos para el cumplimiento de la finalidad de la base de datos de que se trate. Asimismo, no podrán obtenerse de forma solapada u oculta, por medios fraudulentos o abusivos, sino que la recolección deberá ser clara e informada acerca de la finalidad.

Este principio también indica que la información debe ser exacta y actualizarse una vez que el responsable tome conocimiento de las circunstancias que ameritan la supresión, sustitución, actualización o completitud de los datos sometidos a tratamiento.

Las personas cambian sus domicilios y teléfonos, modifican su estado civil, evolucionan en su edad, de manera que la actualización de esos datos no es una carga de principio, del responsable de la base de datos, sino que ésta pertenece al titular de los datos. Eso sí, una vez que el titular pone en conocimiento del responsable, la modificación, éste debe proceder a su actualización.

Por otra parte, el hecho de que la Ley encauce el tratamiento de los datos a un criterio de proporcionalidad, ceñido a que los datos deban ser los necesarios para la finalidad de la base de datos, no implica una limitación en la cantidad de datos a recolectar. Mientras los datos que se colecten respondan a la finalidad respectiva, serán adecuados y pertinentes.

Si por ejemplo, una entidad que brinda cursos de capacitación tiene una base de datos de ex alumnos cuya finalidad es informarlos asiduamente de los cursos que se realizan y al momento de recolectar sus datos personales solicita información sobre determinadas enfermedades, datos de su cónyuge incluyendo actividad que realiza, edad, sueldo, así como datos de sus hijos, estaremos ante datos excesivos para la finalidad de la base de datos.

4.3. Principio de Finalidad

La aplicación del principio de finalidad regulado en el artículo 8º indica que los datos objeto de tratamiento no podrán usarse para fines distintos o incompatibles con los que motivaron su recolección, y deberán ser eliminados una vez concluida la necesidad
o pertinencia, o una vez modificada la finalidad.

Los responsables de bases de datos, ya sean públicos o privados no podrán establecer finalidades genéricas, sino que deberán delimitarlas expresamente e informar de ellas a los titulares de los datos al momento de la recolección de los datos, no siendo válida la delimitación posterior a la recogida.

La necesidad o pertinencia en la conservación de los datos personales tampoco debe vislumbrarse como un límite impuesto por la LPDP. Mientras existan motivos que expliquen el mantenimiento de la información, la conservación será legítima.

Sobre este aspecto, es muy común que las entidades que posean datos personales de sujetos a quienes los une un vínculo laboral o contractual, conserven la información mientras permanezca dicho vínculo.

De existir alguna norma legal o reglamentaria que exija el mantenimiento de los datos durante un período determinado, deberán conservarse bloqueados de forma tal que su almacenamiento, en lo posible, sea diferenciado del resto de los datos sometidos a tratamiento, estando a disposición de las autoridades correspondientes, para atender las posibles responsabilidades, en consonancia con lo dispuesto por el artículo 4° literal A del Decreto N° 414/009.

A los efectos de conservar la información más allá de cumplida la finalidad, podrán disociarse los datos personales, de modo que la información no pueda vincularse a sus titulares.

4.4. Principio del Previo Consentimiento Informado

Si bien todos los principios generales estatuidos en la LPDP tienen igual jerarquía, podríamos priorizar el principio del previo consentimiento informado, en tanto de alguna manera, legitima todo el tratamiento de los datos personales.

Para el artículo 9º, la regla general es que el consentimiento debe ser prestado de forma libre, previa, expresa e informada, el que deberá documentarse.

A diferencia de la Ley Orgánica Española, de Protección de Datos de Carácter Personal, 15/1999, el consentimiento no puede ser prestado de forma tácita, sino que debe ser expreso, documentándose de alguna manera. La LPDP no regula cómo debe ser esa documentación, dejando este extremo al arbitrio del responsable de la base de datos, quien deberá disponer de algún medio idóneo que pueda acreditar que ese consentimiento fue prestado (a través de una cláusula, en soporte papel, a través de un sitio web, mediante una grabación, etc.).

Sin perjuicio de la regla general, la LPDP dispone una serie de excepciones en las que no es exigible prestar el consentimiento:

a) Cuando los datos provengan de fuentes públicas de información.

En este caso se incluyen a los registros, publicaciones o medios masivos de comunicación (registros públicos, diario oficial, periódicos, revistas).

b) Cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

Aquí la norma encierra dos hipótesis:

- En el primer caso, no sería necesario por ejemplo que un beneficiario de una prestación social del Ministerio de Desarrollo Social (MIDES), preste su consentimiento para su obtención, pues es el MIDES el Organismo que se encuentra legitimado para conceder dicho beneficio.

- El segundo caso hace referencia a la existencia de una norma, que debe ser de rango de ley, es decir que estamos ante una hipótesis de clara reserva legal.

c) Cuando se trate de listados cuyos datos se limiten si son personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento; y en el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

Es decir que aquellos responsables (privados o entidades públicas) que procesen datos personales de los contemplados en este literal, no les será exigible recabar el consentimiento de sus titulares, lo que no quiere decir que la base de datos que se conforme de esos listados no sea registrable ante el Órgano de Control, conforme las disposiciones de la LPDP.

d) Cuando los datos deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

En este caso no es exigible el consentimiento del titular de los datos, pues se entiende que el mismo fue prestado cuando se perfeccionó la relación contractual, científica o profesional referida.

Entendemos que en este caso debe incluirse la relación funcional que puede verificarse en el ámbito de una Entidad Pública estatal o no estatal (cualquiera sea la naturaleza del vínculo, contrato de función pública, consultor, becario).

El sentido de la excepción encuentra su esencia en que cuando se firma un contrato de trabajo, se vincula funcionalmente con una Entidad Pública, implícitamente se está brindando el consentimiento para el tratamiento de los datos personales.

Ahora bien, los datos que colecte la División de Recursos Humanos correspondiente, deberán ceñirse al principio de veracidad supra aludido, es decir que deberán ser adecuados, pertinentes y no excesivos para el vínculo que se está estableciendo de naturaleza laboral o funcional.

Será legítimo, en consecuencia, recabar datos de naturaleza identificatoria, datos de salud, etc.

e) Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

En esta hipótesis pueden incluirse, al tenor de lo previsto en el artículo 2°, literal A) del Decreto Nº 414/009, las clásicas agendas telefónicas y los archivos de correspondencia.

4.5. Principio de Seguridad de los Datos

Al amparo de lo previsto en el artículo 10 de la LPDP, el responsable o usuario de la base de datos debe adoptar las medidas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, evitando su adulteración, pérdida, consulta, tratamiento no autorizado o desviaciones de información.

La norma prohíbe el registro de datos personales que no reúnan las condiciones técnicas de integridad y seguridad.

Si bien nuestra Ley no alude a diferentes niveles de seguridad como sí lo hace la Ley española (alto, medio y básico), insta a quienes traten datos personales a adoptar las medidas que de acuerdo al tipo de datos tratados (si son sensibles o no), al soporte utilizado, al grado de la tecnología, sean necesarias para resguardar su seguridad y confidencialidad.

Sin dudas que una Institución Médica que trata las historias clínicas de sus pacientes requerirá mayores medidas de seguridad que una empresa cuyo giro de actividad es el desarrollo de la actividad deportiva.

Habrá que diferenciar en cada caso si la base de datos es manual o informatizada.

En el primer caso, pueden adoptarse medidas manuales como el guardado de la información bajo llave.

Para una base de datos informatizada, atendiendo a las diferentes características que puede revestir, o bien podrá llevarse un control y registro de acceso a la información a través de usuarios y contraseñas, o bien, si la base de datos compromete información sensible, será aconsejable la confección de un documento que delimite expresamente la política de seguridad de la entidad.

Sobre este aspecto, el artículo 55 de la Ley N° 18.046, de 24 de octubre de 2005[55], con la redacción dada por el artículo 118 de la Ley Nº 18.172, de 31 de agosto de 2007[56], le confiere a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) las facultades legales de promover el establecimiento de seguridades que hagan confiable el uso de las tecnologías de la información, concibiendo y desarrollando una política nacional en temas de seguridad de la

[55] http://www.agesic.gub.uy/innovaportal/file/698/1/ley_18046.pdf
[56] http://www.agesic.gub.uy/innovaportal/file/696/1/ley18172_art_118a_121.pdf

información, que permita la prevención, detección y respuesta frente a incidentes que puedan afectar los activos críticos del país.

Asimismo, el artículo 74 de la Ley Nº 18.362, de 6 de octubre de 2008[57], faculta a AGESIC a apercibir directamente a los organismos que no cumplan con las normas y estándares en tecnología de la información establecidos por la normativa vigente, en lo que refiera a seguridad de los activos de la información y políticas de acceso, entre otras.

El Decreto del Poder Ejecutivo Nº 452/009 de 28 de septiembre de 2009[58], por su parte, establece que las Unidades Ejecutoras de los Incisos 02 al 15 del Presupuesto Nacional, deberán adoptar en forma obligatoria una Política de Seguridad de la Información, tomando como base la "Política de Seguridad de la Información para Organismos de la Administración Pública", que se incorpora a dicho decreto, con el propósito de impulsar un Sistema de Gestión de Seguridad de la Información. Se exhorta a los Gobiernos Departamentales, Entes Autónomos, Servicios Descentralizados y, en general, a todos los órganos del Estado a adoptar las disposiciones establecidas en el Decreto.

4.6. Principio de Reserva

Este principio, regulado en el artículo 11 de la LPDP obliga a todas aquellas personas que manejen información proveniente de una base de datos, a guardar secreto de los datos personales que traten, obligación que subsiste aún después de finalizada la relación con el responsable de la base de datos.

Las únicas excepciones a la reserva se verifican cuando la información sea accesible al público, cuando medie consentimiento del titular de los datos o cuando la difusión haya respondido a una orden judicial.

4.7. Principio de Responsabilidad

El principio de responsabilidad señala al responsable de la base de datos como el responsable de la violación de las disposiciones de la LPDP.

Sin perjuicio de ello, el artículo 35 que regula la potestad sancionatoria del Órgano de Control, señala tanto a los responsables de las bases de datos como a los encargados del tratamiento como sujetos pasibles de ser sancionados.

5. DERECHOS DE LOS TITULARES DE LOS DATOS

Junto a los principios generales que se constituyen en verdaderas obligaciones para todas aquellas personas que traten datos personales, encontramos los derechos que ostentan los titulares de los datos personales.

---

[57] http://www.agesic.gub.uy/innovaportal/file/694/1/ley_18362.pdf

[58] http://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto_n°_452_009_de_28_de_setiembre_de_2009.html

5.1. Derecho de información

Este derecho, regulado en el artículo 13 de la LPDP implica que al momento de la colecta de los datos personales, se le deberá informar al titular de los datos, acerca de los siguientes extremos:

- finalidad para la que serán tratados los datos y sus destinatarios,
- la existencia de la base de datos (electrónica o manual), así como la identidad y domicilio del responsable,
- el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, esencialmente en referencia a los datos sensibles,
- las consecuencias de proporcionar o no los datos o su inexactitud,
- la posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

Tal información deberá ser clara y precisa, de manera que el titular de los datos la conozca en forma previa a prestar su consentimiento.

Como esta información se encuentra inescindiblemente coligada al consentimiento, deberá documentarse de algún modo que esta información fue brindada expresa e inequívocamente al interesado (por ejemplo, en forma impresa, en la misma cláusula del consentimiento, mediante una grabación, etc.).

Ahora bien, este derecho subsiste aún en la hipótesis de que no se requiera el previo consentimiento del titular de los datos, porque se verifica alguna de las excepciones contempladas en la norma. De esta forma, el responsable de la base de datos, aunque pueda recolectar datos y tratarlos sin el consentimiento de sus titulares, deberá informarle de los extremos indicados en el artículo 13.

5.2. Derecho de acceso

El derecho de acceso es el que tiene cualquier titular de datos personales de conocer los datos que sobre su persona figuran en una base de datos determinada, ya sea ésta, pública o privada.

Conforme lo prevé el artículo 14 de la LPDP es un derecho gratuito, que solo exige la presentación de la identificación correspondiente por parte del interesado y que en caso de fallecimiento lo podrán ejercer sus sucesores a título universal y en caso de menores o incapaces, sus representantes o curadores. El artículo 14 exigía la exhibición de la sentencia de declaratoria de herederos, pero la Ley Nº 18.719 en su artículo 152 modificó tal requerimiento, estableciendo genéricamente que el carácter de sucesor universal se podrá acreditar debidamente, redacción que parece más feliz a la anterior en tanto no lo supedita a la tramitación de un proceso judicial.
Este derecho solo podrá ser ejercido a intervalos de seis meses, salvo que el titular acredite un interés legítimo, en cuyo caso podrá ejercitarlo antes.

El responsable debe suministrar la información solicitada dentro de los cinco días hábiles y por el medio elegido por el titular (electrónico, telefónico, de imagen, u otro idóneo a tal fin), en forma clara, sin utilizar codificaciones.

Si vencido el plazo, la solicitud no fuera satisfecha o fuera denegada por razones injustificadas, quedará habilitada la acción de habeas data, sin perjuicio de poder formular la denuncia correspondiente ante el Órgano de Control.

5.3. Derecho de rectificación, actualización, inclusión o supresión

Estos derechos podrán ejercitarse por parte del interesado, al constatar error o falsedad o exclusión en la información de la que es titular.

Al igual que en el derecho de acceso, el responsable deberá proceder a satisfacer el pedido en el plazo máximo de cinco días hábiles de recibido, o en su caso, informar las razones por las que se considera no corresponde proceder a la solicitud.

Vencido dicho plazo o incumplido el pedido, quedará habilitada la acción de habeas data o la posibilidad de denunciar dicho extremo ante el Órgano de Control.

En el caso de la supresión de los datos, el artículo 15 de la LPDP, en la redacción dada por el artículo 152 de la Ley Nº 18.719, establece que procede la eliminación o supresión de datos personales en los siguientes casos:

A) Perjuicios a los derechos e intereses legítimos de terceros.
B) Notorio error.
C) Contravención a lo establecido por una obligación legal.

5.4. Derecho a la impugnación de valoraciones personales

Este derecho habilita al interesado a impugnar las decisiones que tengan efectos jurídicos y que impliquen un tratamiento de datos personales que brinden una definición de sus características o personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad.

Para ejercitar este derecho, el afectado podrá solicitar información del responsable de la base de datos sobre criterios de valoración y sobre el programa utilizado en el tratamiento.

6. COMUNICACIÓN DE DATOS PERSONALES

Si bien la comunicación de datos se encuentra regulada en el artículo 17 de la LPDP bajo el nomen iuris “Derechos referentes a la comunicación de datos”, entendimos que la importancia del tema merecía un tratamiento particular y diferenciado.

6.1. Legitimidad

Para que una comunicación o cesión de datos personales sea legítima deben de confluir los siguientes requisitos:

a) que la comunicación se efectúe para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario,

b) que se cuente con el consentimiento previo del titular de los datos,

c) que se le informe al afectado sobre la finalidad de la comunicación y la identidad del destinatario.

6.2. Excepciones al previo consentimiento del titular de los datos

El requisito esencial para todo tratamiento de datos personales no será exigible en los siguientes casos:

- Cuando la comunicación de datos esté autorizada por una Ley.

No será legítima una comunicación de datos que se realice al amparo de una norma de carácter reglamentario, como por ejemplo un Decreto.

- Cuando los datos provengan de fuentes accesibles al público.

La LPDP define fuentes accesibles al público a “aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.” (artículo 4º, literal I).

Se consideran fuentes accesibles al público, a vía de ejemplo, los diarios y los medios masivos de comunicación.

- Cuando la comunicación de datos sea necesaria para el ejercicio de funciones del Estado.

Tal es el ejemplo de un Organismo Público que para el cumplimiento de sus cometidos, necesita determinada documentación con datos personales y así la solicita a otra Institución.

- Cuando la comunicación tenga como objeto la cesión de listados, cuyos datos refieran a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, cuando se trate de personas físicas, y en el caso de personas jurídicas, razón social, nombre de fantasía, RUT (ex RUC), domicilio, teléfono e identidad de las personas a cargo de la misma.

- Cuando deriven de una relación contractual, científica o profesional del titular de los datos y sean necesarios para su desarrollo o cumplimiento.

Así como no es necesario recabar el consentimiento de las personas que sean parte de un contrato laboral, administrativo, científico o profesional, tampoco lo será para comunicar los datos a un tercero, siempre que se enmarque en el cumplimiento, desarrollo y control de esa relación jurídica.

- Cuando se trate de datos relativos a la salud.

En este caso la anterior redacción exceptuaba del previo consentimiento informado cuando la comunicación de datos fuera necesaria por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preservare la identidad de los titulares de los datos, mediante mecanismos de disociación adecuados.

El artículo 153 de la Ley N° 18.719 introdujo modificaciones a esta disposición agregando “cuando ello sea pertinente”, lo que de alguna manera desobstruye las trabas que la aplicación de ese procedimiento de disociación, con carácter general, podía acarrear, haciendo primar el derecho a la vida e integridad física por sobre el derecho a la protección de datos personales.

- Cuando se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares no sean identificables.

En este caso no se suscitan inconvenientes, puesto que la disociación implica que la información no pueda vincularse a persona determinada o determinable.

Conforme lo expuesto, puede prescindirse en las hipótesis analizadas, del consentimiento previo del titular de los datos personales, pero en todo caso deben verificarse los requisitos que reclama el artículo 17, esto es, que la comunicación se enmarque en el cumplimiento de los fines relacionados directamente con el interés legítimo del emisor y del destinatario.

7. REGISTRO DE BASES DE DATOS

El artículo 29 de la LPDP dispone que toda base de datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control.

Si bien se especifica que la reglamentación regulará los diferentes extremos que deberá contener la inscripción, necesariamente deberá contener los siguientes:

- identificación de la base de datos y responsable de la misma,
- naturaleza de los datos personales que contiene,
- procedimientos de obtención y tratamiento de los datos,
- medidas de seguridad y descripción técnica de la base de datos,
- protección de datos personales y ejercicio de los derechos,
- destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos,
- tiempo de conservación de los datos,
- forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los mismos,

- cantidad de acreedores personas físicas que hayan cumplido los 5 años previstos en el artículo 22 de la Ley,
- cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera, conforme lo previsto en el artículo 22.

7.1. Como Obligación

Como lo expresáramos al analizar el principio de legalidad, en el párrafo 4.1, una base de datos no adquiere la calidad de legítima hasta tanto se registre ante el Órgano de Control, accediendo al formulario de inscripción a través del sitio web www.datospersonales.gub.uy.

Es decir que en virtud de lo previsto en los artículos 6º y 29 de la LPDP, existe una conminación hacia los responsables de bases de datos a fin de que éstos encuadren sus operaciones a los principios que se establecen en la Ley y legitimen sus bases de datos a través de la inscripción correspondiente.

7.2. Como Garantía de Calidad

No obstante lo anterior, el hecho de que una empresa o entidad pública haya cumplido con todos los requisitos para la formalización de su registro y ostente la correspondiente resolución que dispone la inscripción de su/s base/s de datos, se erige en un verdadero certificado de calidad.

Se trata de una garantía que otorga beneficios a la empresa o entidad registrada y al titular de los datos personales.

En efecto, los clientes, proveedores, empleados, administrados, que suscriben las cláusulas de consentimiento informado, que ejercen sus derechos, que tienen conocimiento de que sus datos se encuentran seguros, depositan mayor grado de confiabilidad en las empresas o entidades, a la vez que éstas se permiten ostentar un plus en lo que dice relación con su gerenciamiento o dirección.

8. POTESTAD SANCIONATORIA

El artículo 35 de la LPDP prevé que la Unidad Reguladora y de Control de Datos Personales (URCDP) podrá aplicar sanciones a los responsables de bases de datos o encargados del tratamiento de datos personales, en caso que se violen las disposiciones de la Ley.

El artículo 31 del Decreto reglamentario N° 414/009, de 31 de agosto de 2009, por su parte, establece el procedimiento relativo al ejercicio de la potestad sancionatoria, disponiendo que ante una posible infracción de la Ley Nº 18.331 y su reglamentación, la URCDP podrá:
“a) Realizar las inspecciones que el Consejo Ejecutivo entienda pertinente, las que serán dispuestas por resolución fundada.
b) Solicitar ante la justicia competente las medidas pertinentes, cuando exista riesgo de pérdida de la prueba. La solicitud de dichas medidas necesitará resolución fundada del Consejo Ejecutivo.

c) Comunicar las actuaciones al responsable de la base de datos o tratamiento a efectos de otorgarle vista, confiriéndole un plazo de diez días, contados a partir del siguiente al de su notificación para evacuarla. Transcurrido el plazo establecido, se elevarán las actuaciones para resolución del Consejo Ejecutivo, el que tendrá un plazo de treinta días para expedirse. La resolución que recaiga será impugnable de acuerdo con las normas vigentes en la materia".

8.1. Infracciones

El artículo 35 de la LPDP, supra referido establecía que la URCDP podía aplicar las siguientes sanciones:
1) Apercibimiento.
2) Multa de hasta quinientas mil unidades indexadas.
3) Suspensión de la base de datos respectiva. En este caso se faculta a la Unidad a promover ante los órganos jurisdiccionales competentes, la suspensión de la base de datos, hasta por un lapso de seis días hábiles.

El artículo 32 del Decreto Nº 414/009, referido a las multas, dispone que el monto de éstas, será recaudado por AGESIC y la totalidad de lo producido por su cobro se verterá a Rentas Generales.

A su vez, el artículo 33 del mismo cuerpo normativo que regula el procedimiento de suspensión de bases de datos, establece que AGESIC promoverá la suspensión de la base de datos de acuerdo con lo previsto en el artículo 35 numeral 3º de la LPDP, previo pronunciamiento del Consejo Ejecutivo de la URCDP, en los casos que se comprobare que se han infringido o transgredido la Ley y/o su reglamentación.

Ahora bien, la Ley N° 18.719 introdujo modificaciones al artículo 35 de la LPDP indicando que el Órgano de Control podrá aplicar las siguientes sanciones:
1) Observación.
2) Apercibimiento.
3) Multa de hasta quinientas mil unidades indexadas.
4) Suspensión de la base de datos respectiva por el plazo de cinco días.
5) Clausura de la base de datos respectiva. A tal efecto se faculta a AGESIC a promover ante los órganos jurisdiccionales competentes la clausura de las bases de datos que se comprobare que infringieren o transgredieren la Ley.

Es decir que la norma modificativa adiciona las sanciones de observación, como llamado de atención y la clausura de la base de datos, como máxima sanción, reservada para aquellas hipótesis de infracciones muy graves.

El presupuesto de hecho de la infracción está constituido por la transgresión por parte del responsable de la Base de Datos, de los mandatos emergentes de las disposiciones de la LPDP y su reglamentación (Decretos Nos. 664/008 y 414/009).

El hecho constitutivo de la infracción consiste en la realización de conductas activas u omisivas, en tanto las obligaciones derivadas de la LPDP y su reglamentación imponen deberes de "hacer" o de "abstenerse".

Si bien la LPDP no distingue entre conducta infractora dolosa o culposa, como tampoco lo hace la reglamentación, esta última es de difícil configuración analizado el marco contextual de la Ley, sin perjuicio de la expresa previsión que hace el artículo 10 de la LPDP al referir a "...detectar desviaciones de información, intencionales o no...".

8.2 Graduación de las sanciones

Conforme lo dispone el artículo 35 de la LPDP en la redacción dada por la Ley N° 18.719, las sanciones se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida.

Asimismo, el acto administrativo que disponga la sanción, deberá observar las notas de razonabilidad y proporcionalidad como condiciones indispensables para su validez.

Como dice Cajarville, citando a Couture, la razonabilidad "es uno de los más valiosos standards jurídicos de nuestro tiempo" y alcanza, en tanto que principio, a toda la actividad del Estado. [59]

Según Susana Lorenzo "...la razonabilidad juega en distintas etapas de la secuencia del dictado del acto administrativo sancionatorio" En primer lugar, se exhibe en la coherencia lógica que debe informar el hilo conductor del razonamiento de la Administración, que a partir de determinadas premisas concluye en la aplicación de la sanción. En segundo término en la apreciación del supuesto de hecho (no ya en su simple constatación). Y, finalmente, en función de dicha apreciación, que sin duda comporta operaciones lógicas, en la elección del medio punitivo concreto. Claro está, en los casos en que la ley otorga a la Administración una cierta gama de sanciones posibles".[60]

La razonabilidad y su implícito -la proporcionalidad- juegan un papel fundamental cuando la ley solo se limita a mencionar varios instrumentos punitivos y no le impone la aplicación de una pena única y específica, como en el caso.

Para determinar cuál de las sanciones es razonable y proporcional a los hechos cometidos, se apreciarán los derechos personales vulnerados, el volumen de los tratamientos efectuados, los beneficios obtenidos, sean económicos o de otra índole, al grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceras personas, y cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la conducta infractora específica. Asimismo, deberán tenerse en cuenta eventuales eximentes de responsabilidad que puedan conjugarse, como la fuerza mayor o el caso fortuito.

---

[59] LORENZO DE VIEGA JAIME, Susana. "Sanciones Administrativas". Editorial Julio César Faira, Montevideo, 1996, pág. 97.
[60] LORENZO DE VIEGA JAIME, Susana. Ob. y pág. cit.

Se interpreta que la mención que hace la ley no es de grado, por lo que podría perfectamente aplicarse la sanción de multa, sin antes haber aplicado, por ejemplo, la sanción de apercibimiento. Dependerá de la gravedad ontológica de los hechos constitutivos de la infracción.

En cuanto a las obligaciones de seguridad, éstas deben ser vistas desde la órbita de la URCDP, como obligaciones de resultado, en tanto el Órgano de Control tiene el derecho de exigir por parte de los responsables de Bases de Datos, la seguridad y confidencialidad de los datos personales que tratan.

Teniendo en cuenta las disposiciones contenidas en la LPDP y su decreto reglamentario, las obligaciones de seguridad, pueden consistir en:

- Registrar datos personales en Bases de Datos que no reúnan condiciones técnicas de integridad y seguridad. (artículo 10, inciso 3°).

- No adoptar las medidas de seguridad necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos, de acuerdo con lo establecido en el artículo 10 de la LPDP, 7º y 8º del Decreto 414/009. Para la graduación de la sanción se evaluará el estado de la tecnología, el tipo de datos tratados y los riesgos de exposición, sean éstos de carácter tecnológico, humano o provengan del medio físico o natural.

En lo que refiere a los Operadores que explotan redes públicas o que prestan servicios de comunicaciones electrónicas disponibles al público, la normativa prevé disposiciones específicas:

- No garantizar la protección de los datos personales, adoptando medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios. (artículo 20 de la LPDP).

- No informar a los abonados, en caso de que exista riesgo de violación de la seguridad de la red pública de comunicaciones electrónicas, sobre el riesgo y las medidas a adoptar. (artículo 20 de la LPDP).

Si bien en principio podría decirse que toda vulneración a la seguridad de los datos personales implica una infracción de carácter grave, deberá atenderse en cada caso a las circunstancias que hayan coadyuvado a su acaecimiento.

En efecto, ésta es un tipo de infracción, donde puede confluir tanto la intencionalidad como la culpa, dos aspectos muy importantes a evaluar para graduar la sanción a imponer.

Ello se extrae de lo dispuesto por el artículo 10, en tanto establece que las medidas necesarias que el responsable o usuario de la Base de datos debe adoptar, tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Si existió dolo sin duda estaríamos ante una infracción de entidad y la sanción debe ser en consonancia, pero si la violación a la seguridad respondió a título de culpa, por ejemplo, a negligencia o imprudencia en el manejo de la información, o a impericia de los técnicos responsables, la solución diferirá y podrá ameritar la imposición de una sanción menos gravosa, según el caso.

Como ha dicho el Tribunal de Apelaciones en lo Civil de 2° turno, en sede de graduación de la culpa, en el Derecho Privado "actualmente se diferencian cuatro categorías (vide Starck-Roland-Boyer: Obligations...1, p. 147-149 5ª Ed.): a) la intencional (la voluntad se ajusta al acto y consecuencias, es el dolo); b) la inexcusable (es la culpa de gravedad excepcional derivada de un acto o de una omisión voluntaria, de la conciencia del peligro que debía tener su autor y de la ausencia de toda causa justificativa (esto la separa de la culpa intencional: la voluntad no se aplica a las consecuencias dañosas del acto incriminado); c) la grave o lata (revela un error grosero, una impericia imperdonable, una incuria patente (no comprender lo que todo el mundo comprende); d) la leve o muy leve es el error de conducta al cual todo individuo está expuesto y es paradigmática la negligencia (defecto de atención) o imprudencia (insuficiente reflexión sobre las consecuencias del acto)".[61]

La LPDP no alude a medidas concretas que deben adoptar los responsables de la Base de Datos, sino que genéricamente refiere a "medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales...", a contrario de lo que sucede en la Ley Orgánica española 15/1999 que alude a la indicación de tres niveles de seguridad: básico, medio y alto, de acuerdo con la información personal contenida en cada Base de Datos.

En mérito a ello, deberán analizarse por parte de la URCDP si los responsables adoptan las medidas y políticas de seguridad que ésta exige como básicas o adecuadas, en los formularios de inscripción de Bases de Datos, precisándose que las básicas están indicadas con asterisco *

- Si adopta medidas de seguridad.*
- Si dichas medidas son físicas o lógicas.*
- Si dispone de políticas de seguridad.*
- Si tiene documentados los procedimientos relacionados con el acceso y tratamiento de la información.*
- Si tiene documentadas las funciones y obligaciones del personal claramente definidas.
- Si existe un responsable de seguridad.
- Si realiza un control periódico del cumplimiento de las políticas de seguridad.*
- Si realiza auditorías del sistema de información periódicamente.
- Si las auditorías son realizadas por auditores externos o internos.
- Si se atiende a las correcciones realizadas por los auditores.
- Si emite informes al responsable de la Base de Datos.

[61] Sentencia del T.A.C. 2º T. Nº 393/05. Fecha: 21/XII/05, publicada LJU. Tomo 134 - Año 2006, caso 15.308.

- Si dispone de un procedimiento de respaldo seguro.*
- Si realiza respaldos en el mismo lugar donde se encuentran los servidores.*
- Si realiza respaldos en un lugar diferente al que se encuentran los equipos.
- Si realiza respaldos periódicamente, Diario, Semanal, Mensual, Otros. *
- Si verifica la realización de los respaldos y la recuperación de los datos.*
- Si la base de datos permite recuperar los datos al momento exacto de producirse la pérdida o destrucción.
- Si posee diferentes niveles de seguridad para los usuarios según sus funciones.*
- Si posee acceso a la información a través de usuario y contraseña.*
- Si se establecen mecanismos de identificación de usuarios en forma inequívoca y utilizando contraseñas que se actualizan periódicamente.
- Si posee mecanismos que controlen los accesos no autorizados.*
- Si posee un registro de accesos y modificaciones a su Base de Datos, con usuario, hora, tipo de acceso, registro accedido y tarea realizada.*
- Si conserva las diferentes versiones de registros ante cada modificación.
- Si controla el acceso físico a los locales donde se encuentran ubicados los sistemas de información.
- Si el acceso remoto mantiene las medidas de seguridad del acceso local.

Teniendo en cuenta que la información es un activo vital para el éxito y la continuidad de cualquier organización, los responsables de Bases de Datos deberán adoptar políticas de seguridad adecuadas al grado de protección de cada Base de Datos, adoptando diferentes niveles de seguridad, según la naturaleza de la información incorporada (datos personales propiamente dichos, datos relativos a la salud, entre otros).

En el ámbito de la Administración Pública, deberán observarse las previsiones contenidas en el Decreto N° 452/009, de 28 de septiembre de 2009 [62], referido al analizar el Principio de Seguridad de los Datos, en el párrafo 4.5, atendiendo a la preservación de la confidencialidad, integridad y disponibilidad de la información.

9. ACCIÓN DE HABEAS DATA

La LPDP, regula en su capítulo VIII la Acción de Protección de Datos Personales como un proceso a través del cual toda persona puede acudir a los tribunales judiciales a fin de que se efectivicen los derechos consagrados en la Ley.

Aunque la doctrina ha reservado la denominación de la acción de habeas data para identificar a la acción jurisdiccional que protege los datos personales, por extensión, dicho nombre se ha usado también para designar la acción

[62] http://www.agesic.gub.uy/innovaportal/v/299/1/agesic/decreto_n°_452/009_de_28_de_setiembre_de_2009.html?menuderecho=1 Página visitada el 7 de abril de 2011.

jurisdiccional que tiene por objeto la obtención del acceso a archivos y registros documentales de la Administración. [63]

La acción judicial de habeas data propio permite a cualquier persona tomar conocimiento de los datos referidos a su persona, su finalidad y uso que consten en bases de datos públicas o privadas, y en caso de error, falsedad, prohibición de tratamiento, discriminación, desactualización, exigir su rectificación, inclusión, supresión o lo que entienda corresponder.

9.1 Procedencia

Se trata de un proceso breve, sumario, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

a) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le ha sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.

b) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley.

Es decir que para acudir a la vía jurisdiccional a deducir la acción de habeas data es preciso, como cuestión previa, haber formulado una petición ante el responsable público o privado de la base de datos y que esta petición haya sido denegada expresa o tácitamente, o por razones que el interesado juzgue no amparadas por la ley.

Solo luego de sorteado este obstáculo legal que opera como un requisito de procedibilidad, se puede efectivizar la acción correspondiente.

9.2 Competencia y Legitimación

Los Órganos Judiciales competentes son:

- En la capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos.

- Los Juzgados Letrados de Primera Instancia del Interior a quienes se haya asignado competencia en dichas materias.

[63] DELPIAZZO, Carlos. Ob. Cit., págs. 21-22.

La acción podrá ser ejercida por el propio titular afectado o sus representantes, ya sean tutores o curadores y en caso de fallecimiento, sus sucesores universales.

En el caso de personas jurídicas, la acción podrá impetrarse por sus representantes legales o los apoderamos designados a tales efectos.

9.3 Aspectos Procesales

Se trata de un proceso específico, que difiere del proceso de amparo de naturaleza residual que hasta la sanción de la LPDP se venía instaurando como forma de garantizar la protección de los datos personales.

Su naturaleza jurídica es en puridad una acción pero a su vez una garantía.

En primera instancia, salvo que la demanda sea rechazada por manifiestamente improcedente, se convoca a las partes a una audiencia pública dentro del plazo de tres días de presentada la demanda donde se oirá al demandado, se recibirán las pruebas y se producirán los alegatos.

El Tribunal podrá rechazar las pruebas manifiestamente impertinentes o innecesarias y podrá ordenar diligencias para mejor proveer, pudiendo asimismo, disponerse medidas provisionales.

La sentencia se dictará en la audiencia o a más tardar dentro de las veinticuatro horas de su celebración, pudiendo prorrogarse hasta por tres días, solo en casos excepcionales.

La sentencia que haga lugar a la acción de habeas data deberá:

- Identificar a la autoridad o particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.

- Determinar de forma precisa lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si corresponde fijarlo.

- Establecer el plazo para el cumplimiento de lo dispuesto, que será evaluado por el tribunal en cada caso y que no podrá exceder de quince días corridos e ininterrumpidos, computados a partir de la notificación.

Solo serán apelables la sentencia definitiva y la que rechaza la acción por manifiestamente improcedente.

El recurso de apelación debe interponerse en escrito fundado, dentro del plazo perentorio de tres días.

Si la apelación fuera contra la sentencia que rechazó la acción por manifiestamente improcedente, el Tribunal elevará el expediente al de alzada, sin más trámite. Si la sentencia apelada fuere la definitiva, lo sustanciará con un traslado a la contraparte por tres días perentorios.

El Tribunal de segunda instancia resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos.[64]

10. CONCLUSIONES

La protección de datos personales constituye un aspecto de los derechos de privacidad o intimidad, sin embargo, la configuración de aquél derecho humano ha tomado un camino propio, con características particulares.

En la consagración de ese derecho fundamental, la Ley Nº 18.331 implica un gran avance para los ciudadanos en relación con el respeto y control que han de observar aquellos particulares o Entidades Públicas que traten datos personales.

Para las empresas establecidas en Uruguay, también ha significado un progreso, ya que se están cumpliendo con los estándares internacionales de protección de datos personales, lo que otorga un acceso libre y ventajoso a la industria del tratamiento de datos personales de los mercados europeos. El ingreso a este mercado representa un impulso para el desarrollo del comercio internacional. Así, el derecho ha de servir como marco mínimo regulatorio, pero sin obstaculizar la libertad comercial ni obstruir el flujo transfronterizo de datos personales.

Como reforzamiento de lo que se viene exponiendo, Uruguay, en su trámite de adecuación de la Ley a los estándares del Derecho Internacional, ya obtuvo con fecha 12 de octubre de 2010 el Dictamen favorable N° 6/2010, del Organismo Consultivo Europeo en Protección de Datos y Privacidad, creado por el artículo 29 de la Directiva del Consejo de Europa 95/46/CE.[65]

Asimismo, la norma traza las pautas adecuadas para el desarrollo de los mecanismos de defensa de los derechos de los ciudadanos, propulsando la tutela efectiva de derechos, ya no solo a nivel jurisdiccional, sino administrativo. En esta tarea es fundamental el rol que desempeña el Órgano de Control en la tramitación de las denuncias de violaciones a la norma, formuladas por los titulares de datos; y la función que cumple la Justicia competente en el ámbito jurisdiccional, a través de la acción de habeas data.

---

[64] GAIERO, Bruno; SOBA, Ignacio. "La regulación procesal del habeas data", Editorial BdeF, 2010, pág. 144 y sgtes.

[65] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_es.pdf Página visitada el 7 de abril de 2011.

CAPÍTULO IV - DECRETOS Nº 664/008 y Nº 414/009

Dra. Flavia Baladán

1. INTRODUCCIÓN

La Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data (LPDP), estableció en su artículo 49 la necesidad de su reglamentación por parte del Poder Ejecutivo.

A manera de dar cumplimiento a esta obligación se trabajó, en primera instancia, en la elaboración de un decreto que reglamentase lo relacionado con la creación del registro de base de datos personales y la forma de su inscripción. Asimismo, este decreto efectivizó el traslado de los expedientes existentes en el anterior órgano de control (Comisión Consultiva del Ministerio de Economía y Finanzas) a la URCDP. Este Decreto es el Nº 664/008, de 22 de diciembre de 2008.

Posteriormente, se elaboró un decreto reglamentario que regulase en forma general la LPDP. Es así que se promulgó el Decreto Nº 414/009, de 14 de setiembre de 2009. Su importancia radica en que es el primer decreto reglamentario general de la Ley y ha derogado algunos artículos del Decreto Nº 664/008.

En cuanto a los antecedentes que se tuvieron en consideración a la hora de la elaboración de ambas normas, se deben mencionar principalmente como fuentes de inspiración, el Real Decreto Nº 1.720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de desarrollo de la Ley Orgánica Nº 15/1999, de 13 de diciembre, de protección de datos de carácter personal de España. También se consideraron la Ley Nº 25.326 de Argentina así como la Directiva Nº 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

2. DECRETO Nº 664/008, DE 22 DE DICIEMBRE DE 2008

La LPDP derogó la Ley Nº 17.838, de 24 de setiembre de 2004, de Protección de Datos Personales para ser utilizados en informes comerciales y acción de habeas data, la cual disponía en sus artículos 1º, 13 y 20 la creación de un registro permanente y actualizado de los archivos, registros, bases de datos o similares alcanzados por la referida ley.

Asimismo, quedó sin efecto el Decreto Nº 399/006, de 30 de octubre de 2006, que había creado y reglamentado el Registro de Bases de Datos Personales de carácter comercial, el que funcionaba en el Ministerio de Economía y Finanzas, y en el cual se habían realizado registros de bases de datos que con la vigencia de la LPDP, era necesario trasladar hacia el nuevo Órgano de Control.

Es a esos efectos, que entra en vigencia el Decreto Nº 664/008, el cual creó el Registro de Bases de Datos Personales, dispuso el traslado del los registros

realizados ante el Ministerio de Economía y Finanzas, y reguló la inscripción de las bases de datos relativas a la actividad comercial o crediticia establecidos por el artículo 22 de la LPDP.

2.1 Ámbito de aplicación

En primer lugar, se debe delimitar a quiénes alcanza este Decreto. Según el artículo 3º, es aplicable a las personas físicas o jurídicas, públicas o privadas comprendidas en lo dispuesto en el artículo 22 de la LPDP, quienes debían inscribirse en el Registro directamente o por intermedio de sus representantes. A esos efectos, se establece un plazo de 90 días corridos, que se cuentan a partir del inicio de su actividad o de la vigencia del decreto en el caso de las bases de datos ya existentes no inscriptas en el Registro.

2.2 Creación del Registro de Bases de Datos Personales

La LPDP establece la obligación de inscripción de todas las bases de datos existentes en el registro que a tales efectos habilite el Órgano de Control. De forma de dar observancia a esta obligación, el artículo 1º del Decreto Nº 664/008, creó el Registro de Bases de Datos Personales y el responsable de su funcionamiento es la URCDP.

Este Registro funciona como una garantía para los interesados cuyos datos son tratados, ya que mediante la identificación de las bases de datos, de su responsable, y su contacto, los titulares de los datos podrán enviar solicitudes de ejercicio de los derechos que la Ley les reconoce. [66] Asimismo, el Registro funciona como una forma de publicidad, y garantiza que las bases de datos se adecuan a los requisitos exigidos en la normativa vigente.

Por último, cabe mencionar que la inscripción de las bases de datos en el Registro es una garantía, en tanto otorga a los responsables un plus de calidad en el tratamiento de la información.

2.2.1 Requisitos de inscripción

El artículo 4º del Decreto regula los requisitos necesarios para inscribir una base de datos. En este sentido se exige brindar la siguiente información: identificación de la base de datos y el responsable de la misma; procedimientos de obtención y tratamiento de los datos; medidas de seguridad y descripción técnica de la base de datos; protección de datos personales y ejercicio de derechos; destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos; tiempo de conservación de los datos; forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos; cantidad de titulares que hayan cumplido los 5 años previstos en el art. 22 de la Ley Nº 18.331; cantidad de cancelaciones por cumplimiento de la obligación de pago si correspondiera, de acuerdo a lo previsto en el artículo 22 de la Ley Nº 18.331; y datos sometidos a tratamiento en dicha base. Además, se establece

[66] IFAI. Estudio sobre la Protección de Datos a nivel internacional. Disponible en: http://www.ieaip.org.mx/biblioteca_virtual/datos_personales/4.pdf), 2004. México, pág. 105.

que la URCDP está facultada para agregar los elementos que considerase necesarios, en un todo de acuerdo con la LPDP.

El literal d) del artículo 5º indicaba que la inscripción tenía un año de vigencia y debía renovarse dentro de los 10 días hábiles siguientes a su vencimiento, debiendo la URCDP expedir constancia del registro inicial y de sus sucesivas renovaciones. Esta norma fue derogada por el artículo 40 del Decreto Nº 414/009 por la cual el registro no necesita ser renovado anualmente.

En la práctica se debe realizar el registro a través del sitio web de la Unidad, que contiene un formulario on line en el cual se requiere completar todos los datos referidos en el Decreto y otros que se solicitan a efectos estadísticos, cumpliendo con el procedimiento actualmente regulado en el Decreto Nº 414/009.

2.2.2 Presentación de actualizaciones

A este respecto cabe mencionar que el Decreto establecía en su artículo 6º, siguiendo las soluciones preexistentes, que las actualizaciones de la base de datos debían realizarse mensualmente, comunicándolo al Registro.

Este artículo fue expresamente derogado por el artículo 40 del Decreto Nº 414/009, cuyo artículo 20 establece el régimen vigente.

2.3 Traslado del órgano de control de Bases de Datos destinadas a brindar informes objetivos de carácter comercial

El artículo 47 de la LPDP establecía un plazo de ciento veinte días corridos para que el órgano de control de datos existente en ese momento – Comisión Consultiva del Ministerio de Economía y Finanzas – realizara el traslado de la información y documentación a la URCDP.

En ese sentido, el Decreto dispuso el trasladado de la información y documentación del Registro de la Comisión Consultiva al Registro de Bases de Datos Personales creado por el artículo primero del Decreto, manteniéndose sus inscripciones en iguales términos, condiciones y vigencia.

Este traslado se realizó conforme a derecho, recibiéndose la documentación de la Comisión Consultiva en tiempo y forma y su contenido analizado por la URCDP, con lo cual se dio cumplimiento a esta obligación.

3. DECRETO Nº 414/009, DE 31 DE AGOSTO DE 2009

3.1 Ámbito de aplicación

Los artículos 1º a 3º del Capítulo I del Título I, denominado “Disposiciones Generales”, regulan el ámbito de aplicación de esta norma. La delimitación del ámbito de aplicación es esencial pues el resto de la normativa se vinculará a ella. El ámbito de aplicación se divide en tres aspectos:

En primer lugar, el subjetivo, por el cual el Decreto se aplica a todas las personas físicas, ya sea directa o indirectamente. Se especifica que puede ser a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas y se extiende a las personas jurídicas en cuanto corresponda.

Esta referencia a las personas jurídicas ha sido discutida a nivel internacional. Algunos países, como por ejemplo España, entienden que el derecho a la protección de los datos personales sólo alcanza a las personas físicas, ya que los bienes jurídicos tutelados sólo abarcan a éstas.

Otros países como Argentina y parte de la doctrina, entienden que es correcto que las personas jurídicas tengan derecho a la protección de datos personales. Por ejemplo, el Dr. Augusto Durán Martínez expresa que "… en el caso de las personas jurídicas no se puede hablar de datos sensibles, como inclinaciones sexuales u origen étnico, en la misma medida que de las personas físicas, pero sí corresponde reconocer que el uso indebido de datos de una persona jurídica puede lesionar bienes jurídicos de sus integrantes, aparte del daño que puede causar a la propia entidad". [67]

La Ley y el Decreto reafirman su aplicación por tanto, a las personas jurídicas en cuanto corresponda.

En cuanto a qué se considera información personal, es interesante destacar la enumeración que refiere el artículo 1°. Se adopta un concepto abarcativo de los tipos de información que son considerados datos personales. Puede tratarse de imágenes, como las contenidas en una filmación con fines de videovigilancia, huellas genéticas derivadas, por ejemplo, de la utilización de las huellas dactilares o de la pupila como clave de acceso para una empresa. También puede constituir dato personal la información patrimonial o el estado financiero de una persona física o jurídica.

En segundo lugar, el ámbito objetivo. En este sentido el artículo 2º indica que "se aplica a su recolección, registro y todo tipo de tratamiento, automatizado o no, bajo cualquier soporte y modalidad de uso, tanto sea en el ámbito público como privado". Por tanto, el presente artículo define que el tratamiento puede darse en diferentes etapas: desde su recolección hasta su registro y posterior tratamiento.

Tengamos presente que el artículo 4º literal m) de la LPDP define al tratamiento como aquellas operaciones o procedimientos sistemáticos, sean automatizados o no, que permiten el procesamiento de datos personales así como su cesión a terceros, por consultas, interconexiones o transferencias.

Lucrecio Rebollo Delgado ha dicho que "la norma no exige que el dato personal haya sido tratado conforme al procedimiento descrito, para que se incardine en su ámbito de aplicación, sino simplemente que sea susceptible de ello".[68] Por

[67] DURÁN MARTÍNEZ, Augusto. "Derecho a la protección de datos personales y al acceso a la información pública". 1° Edición 2009. Amalio Fernández, pág. 47.
[68] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 57.

tanto, no es necesario que efectivamente se traten los datos, sino que sea posible su tratamiento.

Además en su inciso segundo, se regulan los casos en que no será aplicable el Decreto, reiterando la solución recogida en el artículo 3º de la LPDP. Es importante tener presente que quedan excluidas de la aplicación del Decreto las bases de datos mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, las relacionadas con la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, así como para la investigación y represión del delito.

Por último, tenemos el ámbito territorial. Aquí el Decreto busca definir más el ámbito de aplicación de las normas de protección de datos. A esos efectos, diferencia dos hipótesis en las cuales se aplicará el Decreto.

a) Cuando los tratamientos de datos sean efectuados por un responsable de base de datos o tratamiento establecido en territorio uruguayo. Se especifica que se encuentra establecido en territorio uruguayo cuando se trate del lugar donde ejerce la actividad cualquiera sea su forma jurídica. Atento a ello, cualquier empresa que desarrolle su actividad en Uruguay, y posea una base de datos conforme lo describe la Ley, será alcanzada por la normativa vigente de protección de datos personales, debiendo aplicar ésta.

b) Cuando no se encuentre establecido en territorio uruguayo, pero utilice en el tratamiento medios situados en el país. Por ejemplo, un call center cuya base de datos se encuentra en un tercer país pero utiliza la base de datos para realizar llamadas, promociones; o un banco que tiene su base de datos en la casa matriz, pero la sucursal en nuestro país realiza tratamiento sobre la base de datos.

El inciso final del artículo 3º establece una excepción que es muy común en la práctica, sobre todo en empresas multinacionales. Se trata del caso en que los citados medios se utilicen exclusivamente con fines de tránsito, y en este caso es necesario que el responsable de la base de datos o tratamiento, designe un representante en el país ante la URCDP a efectos de cumplir con las obligaciones establecidas. Este representante deberá tener domicilio y residencia permanente en nuestro país. De esta forma, el Decreto busca identificar un responsable que garantice que el tratamiento de los datos se hará cumpliendo con las normas nacionales.

Ahora bien, se aclara que la designación de un representante, no impide la promoción de medidas legales contra el responsable ni disminuye su responsabilidad en cuanto al cumplimiento de las obligaciones. Estamos ante un caso de responsabilidad solidaria, donde ambos responderán por cualquier incumplimiento que se produzca de la LPDP o su reglamentación.

3.2 Definiciones incluidas

El Decreto Nº 414/009 aporta nuevas definiciones que merecen un estudio particular debido a la incidencia que tienen en la materia.

En primer lugar, el literal a) del artículo 4º define al bloqueo de datos como aquel "procedimiento mediante el cual se reservan los datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado o instituciones que estén legalmente habilitadas a los efectos de atender las posibles responsabilidades surgidas del tratamiento".

El procedimiento consiste en la eliminación del dato extinguida la razón de su recolección. Solamente cuando exista una obligación legal podrán conservarse bloqueados datos personales, pero no se podrá realizar ningún tratamiento a su respecto.

Este procedimiento es de importancia para aquellos estudios jurídicos, contables, etc., que necesitan conservar datos por diferentes obligaciones legales. Podemos mencionar como ejemplos, la responsabilidad contractual de los clientes de un estudio jurídico, o el mantenimiento de los datos a efectos de dar cumplimiento a la normativa de seguridad social de los trabajadores de las empresas.

El literal b) del mismo artículo define qué es la cancelación o supresión de datos indicando que es aquel "procedimiento mediante el cual el responsable cesa en el uso de los datos, la supresión o cancelación implicará el bloqueo de dichos datos durante el plazo establecido en la normativa vigente; vencido éste se deberá proceder a su eliminación definitiva".

Según María Mercedes Serrano Pérez "la vida del dato como elemento que aporta información acaba con su cancelación". [69] La cancelación del dato se encuentra íntimamente relacionada con el principio de finalidad, por el cual los datos deben ser eliminados cuando hayan dejado de ser necesarios para el propósito para el cual se recabaron.

Esto es, una vez extinguida la razón por la cual se tiene la información, se debe proceder a su cancelación o supresión. En caso de existir una obligación legal de conservar la información, se debe mantener ésta bloqueada, conforme lo expresado ut supra.

Por ejemplo, en caso de poseer datos personales de empleados una vez que se extinga la relación laboral, se debe mantener la información mientras existan obligaciones legales, y cuando ya no existan éstas, se debe proceder a su cancelación.

El literal c) refiere a un tema interpretativo estableciendo que la cesión de datos es "comunicación de acuerdo con lo establecido en el artículo 4º literal B) de la Ley que se reglamenta". Por lo tanto, se puede hablar tanto de cesión como de comunicación de datos en forma indistinta.

El literal d) define un tema de importancia, ya que conceptualiza al dato personal relacionado con la salud. Aquí nos encontramos frente a un dato de

[69] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 240.

tipo sensible que posee un régimen específico, a tal grado que la LPDP los califica como datos especialmente protegidos. Entonces, existen datos personales relacionados con la salud cuando se trata de "informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona. Entre otros, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad o a su información genética".

Se adopta una definición amplia, conforme las tendencias de derecho comparado. De esta manera se "permite incluir también las informaciones relacionadas con el cuerpo humano, la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo, los trastornos mentales, las enfermedades, las adicciones. Incluso podrían formar parte también del concepto de datos sobre la salud las dificultades de aprendizaje, la ludopatía, los conflictos de pareja, problemas de desadaptación, de desarraigo, es decir, todas aquellas informaciones relativas a un individuo que, en un contexto sanitario, pudieran afectar a la situación de la salud presente, pasada o futura de la persona". [70]

Ahora bien, corresponde el estudio conjunto de las tres próximas definiciones, ya que son parte de una misma relación jurídica. Hablamos de las transferencias internacionales que son definidas en el literal h) como aquel "tratamiento de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo".

En forma complementaria se define al exportador de datos personales como "la persona física o jurídica, pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos con carácter personal a otro país" y al importador como la "persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de éstos, ya sea responsable de tratamiento, encargada de tratamiento o tercero".

Estas definiciones siguen los lineamientos contenidos en la legislación española. En líneas generales podemos decir que se debe tener presente que la transferencia internacional de datos implica un flujo de datos entre diversos países, por lo que es necesario que se garantice a los individuos el efectivo goce del derecho a la protección de datos personales.

Tampoco se debe perder de vista que las transferencias internacionales son muy comunes y encuentran sus motivos tanto en las necesidades de los organismos públicos, como puede ser el auxilio de justicia o la represión de delitos, o estar motivadas en transacciones de comercio electrónico de diversa índole.

---

[70] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 173.

Por último, cabe destacar que sólo se podrán realizar transferencias internacionales cuando el país de destino tenga un nivel adecuado de protección de datos, cuando se esté ante una de las excepciones tasadas en la Ley, o cuando se haga uso de un mecanismo contractual que garantice el cumplimiento de las normas de protección de datos personales aún cuando el país de destino no tenga un nivel adecuado de protección. [71]

Por último, también por razones interpretativas se define al interesado como el "titular del dato de acuerdo con lo establecido en el artículo 4º literal l) de la Ley que se reglamenta". Por tanto, se puede utilizar en forma indistinta titular de datos o interesado.

3.3 Regulación del previo consentimiento del titular

El Capítulo III del Decreto Nº 414/009 regula el consentimiento. A esos efectos, establece una serie de requisitos que deben ser considerados por los responsables de bases de datos o tratamiento cuando lo recaben. Estos requisitos complementan el régimen general regulado en la LPDP y refieren a aspectos formales y probatorios.

En primer lugar, el artículo 5º del Decreto refiere al consentimiento, el que debe ser informado, de forma que la persona conozca inequívocamente la finalidad a la que se destinarán los datos y el tipo de actividad desarrollada por el responsable. Se establece además, la consecuencia de no realizarlo conforme lo indicado: será nulo.

Mucho se ha dicho sobre las características que debe tener el consentimiento. La mayoría de la doctrina se ha puesto de acuerdo en que debe ser libre, esto es, no debe existir ninguno de los vicios que afectan la voluntad según el Código Civil. Corresponde que sea específico; se debe prestar el consentimiento para un tratamiento concreto y con una finalidad determinada, explícita y legítima. También se exige que sea informado, debe habérsele instruido previamente sobre el tratamiento y su finalidad. Por último, se requiere que sea inequívoco, no se admite el consentimiento presunto, como por ejemplo deducir de los actos de la persona su consentimiento, sino que requiere específicamente una acción u omisión del titular. [72]
En el referido artículo 5º del Decreto se establece que se deberá informar la finalidad, lo cual constituye una aplicación del derecho a la información contenido en la LPDP así como la actividad desarrollada por el responsable de la base de datos. Esa referencia a la actividad sirve como medio para controlar por el titular del dato el cumplimiento del principio de veracidad regulado en la Ley. Esto es, conforme al principio de veracidad yo puedo tratar datos que no sean excesivos en relación con la finalidad para la cual se hubieren recabado. Cuando se conoce la actividad que desarrolla el responsable, se podrá controlar que los datos que se soliciten sean los necesarios y no otros. Desde un punto de vista práctico, un responsable podrá recabar datos de sus proveedores referidos a su identificación pero no podrá solicitarle datos de

[71] En razón de la amplitud y trascendencia de este tema, nos remitiremos al estudio realizado en el Capítulo VII de este libro.
[72] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., págs. 128 a 129.

salud, en tanto, son datos excesivos en relación con la finalidad que desarrolla la empresa.

En segundo lugar, el artículo 6º regula la forma de recabar el consentimiento. Es así que se indica como necesario la existencia de un medio sencillo, claro y gratuito para que manifieste su consentimiento o su negativa. Se prevé la posibilidad de que se realice a través de dos casillas identificadas, las cuales no pueden estar premarcadas. Se destaca la gratuidad del ejercicio de los derechos que regula la Ley, de forma de garantizar su efectivo goce y la prohibición de usar casillas premarcadas.

Con respecto a la prueba, se regula que será el responsable quien debe guardarla a través de cualquier medio conforme a derecho. Se admite a texto expreso la adopción de cualquier otra forma que ofrezca más garantías que las mencionadas. Se adopta este criterio en base a que se entiende que el responsable de la base de datos está en mejores condiciones para dar cumplimiento a esta obligación.

Por último, se prevé una presunción negativa, que consiste en que vencido el plazo de diez días hábiles desde que el titular recibe la solicitud de consentimiento sin que la acepte expresamente, su silencio equivaldrá a una negativa. De esta forma, sólo podrán tratarse datos con el consentimiento expreso del titular, a excepción de los datos que la LPDP admite que no requieren el consentimiento de su titular.

3.4 Regulación de la seguridad de las Bases de Datos

La LPDP establece el principio de seguridad de los datos, siguiendo las principales tendencias del derecho comparado. En ese sentido, establece que todo responsable de bases de datos o tratamiento debe adoptar las medidas necesarias que garanticen la seguridad y confidencialidad de los datos personales, evitando de esa manera su adulteración, pérdida, ente otros tratamientos no autorizados.

La seguridad en protección de datos personales es esencial para impedir el acceso a las bases de datos de personas no autorizadas o evitar el desvío de información, así como para garantizar el tratamiento de datos dentro de los límites que marcan las normas y respetando los derechos de los titulares de datos personales.

El artículo 7º del Decreto refiere a que se deben adoptar medidas técnicas y organizativas idóneas para garantizar su integridad, confidencialidad y disponibilidad.

Ahora bien, corresponde determinar qué es la confidencialidad, integridad y disponibilidad. La doctrina ha entendido que "la confidencialidad protege los datos de manera que sean conocidos sólo por las personas autorizadas y permanezcan vedadas para el resto. La integridad impide que la información contenida en un fichero pueda ser alterada o modificada de manera incorrecta y sin autorización de su titular. Por último, la disponibilidad se refiere a la

recepción del dato a tiempo para cumplir su finalidad y por parte de los destinatarios autorizados, esto es, la accesibilidad de los datos cuando sea preciso y por quienes están facultados para ello". [73]

Son el responsable, o el encargado de tratamiento en su caso, quienes deberán adoptar las medidas y responderán por su no funcionamiento. Dependiendo del tipo de base de datos, serán las medidas que deberán adoptarse.

Además, específicamente se regula la vulneración de la seguridad del artículo 8º del Decreto. En el momento en que ocurra una vulneración de los datos personales, sin importar la fase de tratamiento en la cual se encuentre, de forma significativa y pudiendo configurar una vulneración de los derechos de los interesados, el responsable deberá informar a todos los involucrados.

Como no se establece la forma de comunicación, queda librado al responsable de la base de datos la forma de realizar la mencionada comunicación, siendo de su cargo la prueba de su realización.

3.5 Regulación de los derechos de los titulares

3.5.1 Requisitos para su ejercicio

A este respecto el artículo 9º regula la forma en que se podrán ejercer los derechos. Los requisitos exigidos son un máximo y no un mínimo que debe adoptar el responsable de la base de datos o tratamiento ante el ejercicio de alguno de los derechos que consagran la LPDP y el decreto reglamentario. O sea, cuando una persona ejerza algunos de los derechos reconocidos a los titulares de los datos ante los responsables de las bases de datos, éstos podrán exigir determinados requisitos, pero nunca podrán exceder los límites contenidos en este artículo.

Específicamente, se prevé que los derechos deberán ser ejercidos por su titular o por su representante, necesitando en ambos casos acreditar su identidad, como por ejemplo mediante la exhibición de la cédula de identidad en el caso de las personas físicas, o de una carta – poder o certificado notarial en el caso de las personas jurídicas.

Los derechos se pueden ejercer en forma conjunta o independiente. Pensemos en el caso en el cual una persona quiere acceder a sus datos contenidos en una base de datos que desconoce como figura. En este caso puede suceder, que una vez ejercido el derecho de acceso, se constate un error y ejerza el derecho de rectificación. También puede suceder que una persona ya conozca los datos contenidos en una base de datos y sepa que son erróneos, en este caso, la persona ejercerá en forma concomitante, los derechos de acceso y rectificación o supresión.

---

[73] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 148.

El ejercicio de los derechos debe ser exento de formalidades y en forma gratuita. Como se ha dicho anteriormente, no se puede cobrar ningún tipo de gravamen para el ejercicio por sus titulares, ya que se verían limitados en el efectivo goce de los mismos. Tampoco se pueden imponer restricciones de otra índole para su ejercicio. El límite de la responsabilidad del responsable de la base de datos consiste en la comprobación de la identidad del titular del dato pero no en la limitación de sus derechos.

El Decreto establece la posibilidad de que los titulares de los datos ejerzan su derecho mediante una comunicación dirigida al responsable que deberá contener la identificación del titular, el motivo por el cual la solicita (recordemos que la LPDP establece que el derecho de acceso sólo puede ejercerse cada seis meses, excepto razón fundada), domicilio real y constituido –los cuales podrán coincidir-, fecha y firma del solicitante así como documentos acreditantes de su solicitud. Con respecto a este último elemento, cabe señalar que en los casos de rectificación de datos es necesario comprobar que el dato cambió. Por ejemplo, en el caso del estado civil de las personas, para comprobar el casamiento o el divorcio de una persona, se podrá pedir la exhibición de una partida que compruebe tal estado.

Siguiendo lo establecido por la LPDP se reitera que el responsable deberá contestar la solicitud dentro del plazo de cinco días hábiles desde su presentación y la información que se brinde debe ser proporcionada en forma legible e inteligible, sin utilizar claves o códigos. Con esta previsión se busca que el titular entienda la información que se le brinda, de manera que tenga efectivo goce de sus derechos.

3.5.2 Particularidades

Se regulan en forma autónoma los derechos reconocidos de rectificación, actualización, inclusión y supresión, siguiendo las previsiones contenidas en el artículo 15 de la LPDP.

Nuestro derecho innova en esta materia, creando el derecho de inclusión. El Decreto N° 414/009 lo regula en los siguientes términos: “es el que tiene el titular a ser incorporado con la información correspondiente en una base de datos cuando acredite un interés fundado”. Cabe pensar en un ejemplo en el cual se podría efectivizar este derecho. Sería el caso en el cual el hecho de no figurar en una base de datos le causara perjuicio a un sujeto. Por ejemplo, no figurar en una lista de beneficiarios de un plan de beneficios estatales, cuando se cumplen con los requisitos para estar incluido en él. La finalidad de este derecho radica en obtener igual trato ante iguales condiciones, contemplando la hipótesis en la cual una persona no es incluida en una base de datos, y la mencionada situación le causa un perjuicio.

3.5.3 Comunicación o cesión de datos

Un tema de vital trascendencia en la protección de datos es la comunicación de datos. Se ha dicho que la cesión de datos es un punto conflictivo cuando se trata de proteger la denominada “privacidad” de una parte, ya que cediendo los

datos a otras bases de datos se posibilita el cruce de éstos, aplicando con toda intensidad las posibilidades de tratamiento de la información que posee la informática, y porque la propia cesión facilita la utilización de los datos para un uso que no es el mismo para el cual se habían recabado. [74]

Cuando se realiza tratamiento de datos personales, puede intervenir además del responsable de la base de datos, un tercero que la LPDP denomina "encargado de tratamiento", el cual accede a los datos personales a efectos de prestar algún servicio. Se considera que esta relación debe estar regulada y que el acceso por parte del encargado de tratamiento deba ser informado al titular de datos personales.

En este sentido, el artículo 14 del Decreto regula los derechos referentes a la comunicación o la cesión de datos. Este artículo busca complementar lo estatuido en el art. 17 de la LPDP que posee el mismo nomen iuris.

Se establecen una serie de requisitos que refieren a que se puede realizar comunicaciones de datos cuando es para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario. Aquí vemos una aplicación del principio de veracidad, en tanto se estatuye que es necesaria la existencia de interés por ambas partes. También se cumple con el principio de previo consentimiento del titular del dato, al establecerlo como requisito de la comunicación. Por último, vemos otra aplicación del derecho a la información, al hacer referencia a la necesidad de informar de la finalidad de la comunicación, el tipo de destinatario y el tipo de actividad.

El segundo inciso realiza una excepción. Estatuye que no existe comunicación de datos cuando el que accede es el encargado de tratamiento, y este acceso tiene como finalidad la prestación de un servicio al responsable. Un ejemplo sería el caso de un estudio contable contratado por el responsable para realizar la liquidación de sueldos del personal de la empresa.

La norma realiza una salvedad e indica que cuando existe un nuevo vínculo entre el encargado del tratamiento y el titular es necesario recabar el consentimiento. La razón de ser de esta excepción estaría dada para el caso que el encargado de tratamiento realice tareas distintas a las prestadas originalmente. Ante ello, es necesario cumplir con el principio de previo consentimiento en tanto ha variado la finalidad del tratamiento. Esto es, si este mismo estudio empieza a realizar tratamiento de la base de datos de empleados con otras finalidades, será necesario recabar el consentimiento de los titulares. [75]

3.6 Inscripción de base de datos

[74] IFAI. Ob. Cit., pág. 70.
[75] Debido a la importancia de este tema nos remitimos al estudio realizado en el Capítulo III de este libro a su respecto.

La LPDP establece que para ser considerada lícita una base de datos es necesario que se encuentre debidamente inscripta, de forma de dar cumplimiento al principio de legalidad.

Asimismo, indica específicamente que la creación, modificación o supresión de bases de datos de titularidad pública o privada debe registrarse conforme los artículos 24 y 28 de la LPDP.

Además, el artículo 29 de la LPDP refiere a que deben inscribirse ante un Registro que al efecto habilite el órgano de control, conforme con los criterios reglamentarios que se establezcan, y se indica el contenido mínimo que debe tener tal inscripción, sin perjuicio de que por vía reglamentaria se establezcan más especificidades.

Como ya se mencionó ut supra, el Decreto Nº 664/009 creó el Registro de Bases de Datos Personales que se encuentra en funcionamiento desde la entrada en vigencia de esta norma.

Ahora bien, actualmente el Título III del Decreto Nº 414/009, bajo el nomen iuris de "Régimen Registral", instaura el procedimiento que se debe seguir para la inscripción de bases de datos personales. Se regulan específicamente los actos y documentos inscribibles, el contenido y la forma de inscripción, el plazo, la inscripción provisoria, la fecha de inscripción, y la forma de presentación de las actualizaciones.

3.6.1 Requisitos formales

En primer lugar, corresponde delimitar qué es lo que se debe inscribir ante el Registro de Bases de Datos Personales. En este sentido, el artículo 15 establece que deben inscribirse:

a) La creación, modificación o supresión de bases de datos que contengan datos personales que pertenezcan a personas físicas, siempre y cuando no sean utilizadas para fines exclusivamente personales o domésticos.

Con relación a la finalidad personal o doméstica, el Consejo Ejecutivo de la URCDP mediante Dictamen Nº 10, de 11 de setiembre de 2009, ha establecido que: "III. Que con esa base se entiende por actividades exclusivamente personales o domésticas áquellas circunscriptas a la vida privada y familiar de las personas físicas.

IV. Que el adverbio "exclusivamente" contenido en la LPDP art. 3 lit. A) apunta a que las bases de datos mixtas, o sea áquellas en las cuales se comparten datos personales y profesionales, queden incluidas en el ámbito objetivo de la Ley, en virtud de no tener como finalidad exclusiva el uso personal.

V. Que es independiente el hecho que la información no se brinde a terceras personas, ya que tal circunstancia no define la calificación de actividades exclusivamente personales o domésticas a la que refiere la Ley".

A mayor abundamiento, el Dictamen Nº 19, de 17 de diciembre de 2009, delimita: "III. Que, por definición, una persona jurídica, carece de "ámbito personal o doméstico", atento a que el reconocimiento y las manifestaciones de la "personalidad jurídica", en el caso de las personas morales, resulta absolutamente incompatible con la ausencia de control estatal externo que supone aquél ámbito, estando una persona moral, cualquiera sea ella, sometida en todo momento a los poderes del control del Estado, cosa que no sucede con la persona física".[76]

La Ley Nº 18.719, de 27 de diciembre de 2010, modificó el artículo 28 de la LPDP referido a la creación, modificación o supresión de bases de datos por parte de personas físicas o jurídicas, eliminando la referencia al uso personal o doméstico, de forma que se puso fin a esta discusión, siendo obligación la inscripción de las correspondientes bases de datos.

b) La creación, modificación o supresión de bases de datos que contengan datos personales que pertenezcan a personas jurídicas, salvo las excepciones previstas en el artículo 3º de la LPDP. Como se refirió en el inciso anterior, las personas jurídicas no pueden aplicar la excepción de uso personal o doméstico. El Consejo Ejecutivo de la URCDP ha recibido varias consultas sobre el alcance de la obligación de inscripción de determinadas bases de datos que podrían estar incluidas dentro de las excepciones del artículo 3º de la LPDP y ha pronunciado dictámenes a su respecto, que se encuentran disponibles en el sitio web de la Unidad. [77]

c) Los códigos de conducta de práctica profesional que establezcan normas para el tratamiento de datos personales. Conforme el artículo 36 de la LPDP las asociaciones o entidades representativas de responsables o usuarios de bases de datos de titularidad privada pueden elaborar códigos de conducta de práctica profesional, cuyo contenido sea la regulación del tratamiento de los datos personales, que aseguren y mejoren las condiciones de operación de los sistemas de información en función de los principios que contiene la LPDP. El procedimiento de inscripción es el mismo que para las bases de datos, variando solamente el contenido de la solicitud. También cabe aclarar que se puede tratar de códigos que sean completamente referidos a la protección de datos personales o que mayoritariamente refieran al tema, no siendo inscribibles áquellos cuyo objetivo es otro y sólo se hace una referencia general a la protección de datos personales.

d) Las autorizaciones de transferencias internacionales. A este respecto, también el Decreto establece un procedimiento especial que se detallará más adelante. Asimismo, debe tenerse presente que solo procede la solicitud de autorización de transferencias internacionales, cuando éstas no se encuentren dentro de las excepciones contenidas en el artículo 23 de la LPDP, o se destinen a países que no garantizan un nivel de protección adecuado, o cuando el responsable del tratamiento ofrezca garantías suficientes respecto

[76] Se puede consultar el texto completo de ambos dictámenes en el sitio web de la URCDP, http://www.datospersonales.gub.uy/sitio/dictamenes.aspx
[77] http://www.datospersonales.gub.uy/sitio/dictamenes.aspx

de la protección de la vida privada, de los derechos y libertades fundamentales de las personas así como respecto al ejercicio de los respectivos derechos. Dichas garantías pueden derivarse de cláusulas contractuales apropiadas conforme lo establece con el artículo 23 in fine de la LPDP.

Por último, se establece que la inscripción se realizará conforme los criterios brindados por la Ley, el Decreto Nº 664/008 y el Decreto Nº 414/009 u otras disposiciones que establezca la URCDP.

En cuanto al contenido y a la forma de inscripción el artículo 15 del presente Decreto establece que se hará de conformidad con el artículo 5º del Decreto Nº 664/008. Entonces, es necesario que la solicitud y el formulario de inscripción sean suscriptos por el responsable de la base de datos. Se debe realizar con todos los requisitos exigidos, dentro del plazo establecido, admitiéndose de forma provisoria la inscripción a través del sitio web de la URCDP, bajo condición de regularizar la misma dentro de los 10 días hábiles siguientes. Para proceder a la regularización, se deberá agregar la firma auténtica del responsable y aquellos datos o documentos que el medio electrónico no admitiera. Por último, la URCDP expedirá una constancia de la solicitud. [78]

La información que debe proporcionar el responsable relacionada con la bases de datos consiste en la identificación de la base y el responsable de la misma, el procedimiento y obtención y tratamiento de éstos, las medidas de seguridad y descripción técnica de la base, la protección de los datos personales y el ejercicio de los derechos, su destino y las personas físicas o jurídicas a las que pueden ser transmitidos, el tiempo de conservación, la forma y condiciones en que las personas pueden acceder a ellos y los procedimientos a realizar para la rectificación o actualización, los datos sometidos a tratamientos en dicha base, y la certificación de firma del responsable de cada base, y el domicilio constituido y correo electrónico a efectos de las notificaciones. Sin perjuicio de ello, la URCDP podrá agregar otros elementos que sean necesarios.

A los efectos de dar cumplimiento a esto, y en virtud del Decreto Nº 664/008, se diseñaron formularios que contemplan los referidos requerimientos y que se encuentran disponibles en el sitio oficial de la URCDP y los responsables podían descargarlos, consignar la información y presentarlos para solicitar el procedimiento de inscripción ante el Órgano de Control. [79]

Cuando entró en vigor el Decreto Nº 414/009, se puso en forma concomitante en funcionamiento el Registro de Base de Datos en el sitio web de la URCDP, cuyo contenido es muy similar al de los formularios.

3.6.2 Inscripción provisoria

[78] Solo se refiere a los aspectos que no quedaron derogados expresamente por lo establecido en el artículo 40 del Decreto Nº 414/009 que deroga el inciso d) del mencionado artículo 5º del Decreto Nº 664/008.

[79] Se puede consultar en la viñeta registro del referido sitio http://www.datospersonales.gub.uy/sitio/registro.aspx

El artículo 18 del Decreto establece que todas las inscripciones on line, vencido el término de diez días hábiles previsto en el literal b) del artículo 5º del Decreto Nº 664/008, sin que se regularice la inscripción provisoria, caducarán de pleno derecho.

Esto es, el literal b) del artículo 5º del Decreto Nº 664/009 admite que de forma provisoria se solicite la inscripción a través del sitio web de la URCDP y se condiciona a que se regularice ésta dentro de los 10 días hábiles siguientes. El artículo 18 viene a establecer la consecuencia en caso que no regularice la inscripción, que consiste en la caducidad de la solicitud. Quiere decir que se tendrá por no realizada.

Ahora bien, se debe determinar en qué consiste la regularización de la solicitud. En este sentido, se entiende que es la presentación personal de la solicitud realizada a través del sitio. En el caso de personas – físicas o jurídicas – domiciliadas en Montevideo deberán concurrir personalmente ante la URCDP munidos del formulario generado por el sistema y con la documentación requerida (fotocopia de la cédula de identidad en el caso de personas físicas o certificado notarial en el caso de personas jurídicas); y en el caso de las personas domiciliadas en el interior, podrán hacer llegar la documentación a través de sobre cerrado o de correo postal.

3.6.3 Fecha de inscripción

La fecha de inscripción definitiva de una base de datos es dada por la Resolución que emite el Consejo Ejecutivo de la URCDP. Esta Resolución contendrá un código de identificación que en el caso de bases de datos consiste en la letra “B” seguido de un número que es correlativo, y en el caso de códigos de conducta, es la letra “C” seguido de un número correlativo.

Una obligación que establece el Decreto en este aspecto, es la vinculada con la exhibición en lugar visible, accesible a los usuarios, el número y fecha de la citada Resolución.

3.6.4 Actualizaciones

Una vez finalizado el proceso de inscripción, la base de datos queda inscripta en el Registro de Base de Datos Personales, lo cual constituye una innovación respecto a los sistemas existentes anteriores en esta materia, ya que lo usual era que la inscripción tuviese una validez de un año. Específicamente así lo establecía el Decreto Nº 664/008, lo que fue derogado expresamente por el artículo 40 del Decreto Nº 414/009.

En el régimen vigente, es necesario presentar las actualizaciones que sufra la base de datos, comunicándolas trimestralmente.

En cuanto al contenido de las actualizaciones, el Consejo Ejecutivo ha entendido que sólo se deben presentar éstas, cuando exista una variación importante, no menor a un 20 % en lo que refiere a datos numéricos (por ejemplo, la cantidad de personas físicas o jurídicas sometidas a tratamiento), o

el cambio de un requisitos esencial de la base de datos (por ejemplo, se cambia un requisito para modificar datos respecto a los indicados en la solicitud original).

3.7 Normas de actuación

El Decreto N° 414/009, de 11 de setiembre de 2009, regula determinados procedimientos que tienen su origen en la LPDP pero que ésta no regula directamente o establece que será la reglamentación quien lo hará. En ejecución de ello, el Decreto regula los aspectos generales que regirán los procedimientos llevados en la URCDP e instaura determinados requisitos para algunos de ellos. A efectos de una mejor visualización del tema, se fracciona el tema en dos aspectos, administrativos y procedimentales, los que se pasan a detallar.

Asimismo, se regula el procedimiento relativo al ejercicio de la potestad sancionatoria, el de autorización de transferencias internacionales de datos, el de inscripción de códigos de conducta y el de autorización de conservación de datos para fines históricos, estadísticos o científicos.

3.7.1 Aspectos administrativos

El artículo 29 del Decreto establece el principio general, por el cual, la actividad administrativa de la URCDP se realizará conforme los principios que rigen el Derecho Administrativo.

A mayor abundamiento, se indican los principios de imparcialidad, celeridad, eficacia, verdad material, informalismo, debido proceso, impulsión de oficio, buena fe, motivación y simplicidad.

La importancia de estos principios radica en que se utilizarán como criterios interpretativos en todas aquellas cuestiones que deriven de la tramitación de los diferentes procedimientos iniciados ante la Unidad.

Siguiendo la línea establecida por el referido artículo 30 del Decreto, se establece específicamente que cualquier procedimiento - ya sea externo o interno, seguido de oficio o a petición de interesado- se deberá completar en el menor tiempo posible, lo cual es una clara aplicación del principio de celeridad de los procesos, como consecuencia del debido proceso, lo cual se instituye en una clara intención de dar cumplimiento a esta garantía constitucional.

Con respecto a aquellos aspectos no regulados específicamente por el Decreto, se indica que se aplicará el Decreto Nº 500/991, de 27 de setiembre de 1991 y sus modificativos.

3.7.2 Aspectos procedimentales

A continuación se adjunta cuadro comparativo de los distintos procedimientos regulados por el Decreto Nº 414/009 donde se consigna cuándo procede, cuáles son los requisitos exigidos en cada uno de ellos así como las

especificidades de cada uno y en los casos en que existan, los plazos previstos.

	Ejercicio de la potestad sancionatoria	**Autorización de transferencias internacionales**	**Inscripción de códigos de conducta**	**Autorización de tratamiento con fines históricos, estadísticos o científicos**
Procedencia	Se ejerce ante una posible infracción a la LPDP o su reglamentación.	Se inicia siempre a solicitud del exportador que pretenda realizarla.	Se inicia siempre a solicitud del responsable de la base de datos.	Se inicia siempre a petición del responsable que pretenda obtener la declaración.
Requisitos formales	Para adoptar determinadas medidas se debe solicitar a la justicia las medidas pertinentes para evitar la posible pérdida de la prueba, siendo necesario la existencia de una Resolución del Consejo Ejecutivo de la URCDP	La solicitud deberá contener: - identificación de la base de datos y su código de inscripción en el Registro de Base de Datos Personales - descripción de la transferencia e indicación de la finalidad que se pretende, adjuntando la prueba existente (si se trata de un contrato se requiere copia de éste y se deberá acreditar poder suficiente de sus otorgantes)	La solicitud debe acompañarse de: - identificación de la institución, - identificación del código de conducta, - contenido del código de conducta. El procedimiento de inscripción es el mismo que para las bases de datos.	La solicitud deberá contener: - identificación del tratamiento de datos que se pretende exceptuar, - establecer las causas que justifican la declaración, - presentar las medidas que el responsable propone implantar para garantizar el derecho de los ciudadanos, - acompañar los documentos necesarios para justificar la solicitud.
Especificidades	Cuando se está ante una suspensión de una base de datos, se realizará previo pronunciamiento del Consejo Ejecutivo de la URCDP, cuando surja probado que se han infringido o	Podrán realizarse transferencias internacionales cuando se trate de empresas multinacionales entre la casa matriz y sus filiales o sucursales, o entre éstas cuando posean códigos de conducta		La URCDP tiene la facultad de solicitar informes a instituciones u organismos públicos o privados con competencia o mérito sobre el caso. La URCDP

	transgredido la LPDP o su reglamentación.	debidamente inscriptos ante la URCDP. Este procedimiento también es aplicable a los casos de organismos internacionales.		también puede, a solicitud del responsable conforme el mencionado procedimiento, autorizar el mantenimiento íntegro o parcial de los datos. La presentación de la solicitud suspende la obligación de eliminar la base de datos hasta que se decida sobre la misma.
Plazos	Comunicar las actuaciones al responsable de la base de datos o tratamiento mediante una vista por un plazo de diez días. Transcurrido el plazo el Consejo Ejecutivo tiene 30 días para expedirse mediante una resolución que será pasible de ser impugnada (artículo 31 literal g).			

4. CONCLUSIONES

Los decretos reglamentarios de la Ley constituyen herramientas que complementan lo establecido en la misma, regulando algunos aspectos que, ya sea por su detalle o por tratarse de aspectos instrumentales, no fueron incluidos en la Ley.

El Decreto Nº 664/008 aporta la creación de un registro de base de datos que funciona como una garantía para las personas. Se regula el procedimiento de inscripción que hace que los responsables cuenten con una especie de certificado de calidad que genera más confianza en la ciudadanía, en el tratamiento de sus datos personales.

El Decreto Nº 414/009 complementa la LPDP, especificando aspectos relativos a las personas físicas y jurídicas sujetas a su aplicación, añade definiciones de mucha trascendencia práctica, regula aspectos referidos a los derechos, al consentimiento y a la seguridad e instaura un procedimiento de inscripción sencillo y claro. Por último, establece procedimientos para casos específicos.

La práctica ha demostrado que ambos Decretos han llevado al país a tomar conciencia de la necesidad de este derecho, han generado más confianza en el tratamiento de datos personales, y han dado lugar a ejercicios de derechos que aunque vigentes antes por el bloque de constitucionalidad, no eran conocidos por las personas.

Ambos Decretos son pasos consistentes en la búsqueda de lograr el efectivo goce de la protección de los datos personales.

CAPÍTULO V – AUTORIDADES DE CONTROL EN PROTECCIÓN DE DATOS

Esc. Sandra Mazzone

1. INTRODUCCIÓN

De acuerdo con la definición adoptada por el Supervisor Europeo de Protección de Datos se entiende generalmente por "protección de datos" la protección de las libertades y los derechos fundamentales de las personas físicas, especialmente de su vida privada, en lo que respecta al tratamiento de datos personales. En consonancia con ello el tratamiento de datos personales al estar ligado a un derecho personal, hizo necesaria la institución de ciertas garantías a fin de hacer efectiva su aplicación, surgiendo en tal sentido las leyes de protección de datos personales y con ellas los órganos de control como los garantes necesarios para la aplicación de lo dispuesto en las mismas. Con el objetivo de garantizar el cumplimiento efectivo y el respeto del derecho a la protección de los datos personales, los distintos ordenamientos jurídicos han creado órganos de control encargados de velar por el cumplimiento efectivo del derecho a la protección de los datos personales. En tal sentido han establecido distintos mecanismos de protección, tanto a nivel constitucional y legal, habiéndose creado a nivel institucional órganos de contralor dentro de la esfera estatal, organizados generalmente como descentralizados, con autonomía técnica, encargados de velar por el cumplimiento efectivo y la plena vigencia de este derecho humano.

Su surgimiento se remonta a la década de 1970, vislumbrándose en forma incipiente en la Ley de Privacidad de 1974 de los Estados Unidos de América, donde se encomendó la defensa del derecho a la protección de los datos personales a los tribunales de justicia.

De todas maneras, cabe puntualizar que la existencia de leyes protectoras de los datos personales no se traduce necesariamente en la creación de órganos de control.

2. CLASES DE ÓRGANOS DE CONTROL

Al decir del Profesor Lucrecio Rebollo existen tres modelos de órganos de protección o de control en lo relativo a la protección de datos:

- órganos unipersonales,
- órganos colegiados,
- sistemas que atribuyen la defensa de este derecho a los tribunales ordinarios.[80]

A. Órganos Unipersonales. En la década de 1970 aparecen los primeros antecedentes de órganos de control en este sentido; así la Datenschutz del

[80] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., págs. 105-124.

Land de Hesse y la Data Lag sueca crearon instituciones independientes nombradas por el Parlamento, de carácter unipersonal, encargadas de velar por los derechos reconocidos en las respectivas normas[81]. En el año 1984 la Data Protection Act de Reino Unido instituyó un órgano unipersonal denominado "Data Protection Register" encargado de promover jurídicamente los asuntos relacionados con la protección de datos.

Dentro de esta categoría se ubican el Comisario Federal de Protección de Datos de Alemania, así como el órgano de control creado en Argentina por la Ley N° 25.326 del año 2000, que más adelante se desarrollarán específicamente.

B. Órganos Colegiados. Este género de órganos, fundamentalmente cumplen funciones informativas y de publicidad en lo referente a la normativa de datos personales, así como sancionatorias, inspectivas y registrales.

Al igual que los Unipersonales, gozan de plena autonomía e independencia.[82]

Algunos de los países que poseen este sistema son, a modo de ejemplo: España, Francia, Portugal, Italia, Uruguay. Asimismo la labor desarrollada por la Unión Europea se ubica en esta categoría, encomendándose a una Comisión.

C. Tribunales Ordinarios. Este sistema funciona en los Estados Unidos de América donde "la tutela de los derechos fundamentales contenidos en la Constitución o en sus distintas Enmiendas, quedan sometidas a los tribunales ordinarios, siendo el Tribunal Supremo quien en última instancia, dictamina la posible vulneración o no de derechos, así como la interpretación jurídica que debe realizarse de los mismos.

El inconveniente de este modelo es que la actuación de los tribunales se realiza a posteriori, una vez que se produjo la lesión del derecho, quedando en manos del gobierno, o por delegación de éste, en la Administración, la labor de promoción y control, del citado derecho."[83]

3. DERECHO COMPARADO

Veremos en forma particular cada uno de los órganos de control reseñados a fin de tener una idea general de su integración y funcionamiento.

3.1 Alemania

El modelo de órgano unipersonal acogido por este país es adoptado a través de la figura del Comisario Federal de Protección de Datos, el que goza de independencia plena en su labor y está sometido únicamente a la ley.

---

[81] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 106.
[82] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 107.
[83] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., págs. 108 y109.

Posee facultades en todo el territorio nacional así como atribuciones inspectivas y sancionatorias[84], careciendo de facultades para ordenar el bloqueo, supresión o destrucción de datos e imponer el cese temporal o definitivo del tratamiento.

3.2 Argentina

Con igual esquema de funcionamiento que Alemania, se ubica Argentina. La Ley N° 25.326 del año 2000, dispone la existencia de un órgano de control dotado de autonomía funcional que funcionará en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Estará dirigido por un Director Nacional designado por el plazo de cuatro años por el Poder Ejecutivo, con el acuerdo del Senado de la Nación, entre personas con antecedentes en la materia, quien se dedicará en forma exclusiva a su función, siendo el jerarca máximo.

A su vez cuenta con un Consejo Consultivo encargado de asesorar al Director, pudiendo actuar en determinadas circunstancias de importancia exclusivamente.

El órgano de control de este país, denominado Dirección Nacional de Protección de Datos Personales posee facultades de asesoramiento, inspectivas, sancionatorias, así como registrales.

3.3 España

La Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) –actualmente derogada por la Ley N° 15/999-, en su artículo 34 creó la Agencia de Protección de Datos, como "un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria."

De su artículo 35 resulta que el Director de la Agencia será quien la represente durante un período de 4 años y será nombrado entre quienes conformen el Consejo Consultivo, siendo la misión de este último asesorar a aquél, hallándose ambos en igualdad jerárquica.

Dicho Consejo Consultivo está conformado por integrantes de diferentes áreas, a fin de integrar las más diversas inquietudes sociales. Si bien la integración actual del mismo, con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) ha variado, mantiene algunos rasgos característicos.

---

[84] REBOLLO DELGADO, Lucrecio y otra. Ob. Cit., pág. 106.

Dentro de las funciones de éste órgano de control, la Agencia cumple las siguientes:

a) informativa y de publicidad: brindando publicidad y acceso a los ficheros a través del Registro General de Protección de Datos;

b) consultiva: constituye un soporte al Gobierno, asesorándolo en materia de protección de datos;

c) normativa: a través del dictado de normas e instrucciones;

d) inspectiva: se traduce en la posibilidad de la Agencia de solicitar la colaboración e información que requiera respecto de los responsables de los ficheros, así como de supervisar el funcionamiento de los mismos;

e) sancionatoria: a través de la posibilidad de aplicar medidas sancionatorias a los responsables de los ficheros en caso de violación de las normas;

f) de representante español en el Grupo del artículo 29 de la Directiva 95/46/CE y de cooperación internacional en lo relativo a su actividad.

Otro elemento a favor de la independencia de la Agencia es el aspecto financiero, ya que si bien carece de fuentes de financiamiento propio, elabora su anteproyecto de presupuesto anual a fin de ser incluido dentro del Presupuesto General del Estado.

Asimismo la LORTAD posibilitó la creación por las Comunidades Autónomas y la Administración Local de órganos de control independientes y autónomos en el ejercicio de sus funciones, con la salvedad que estas autoridades de control sólo podrán hacerse cargo de registrar ficheros de carácter de públicos.

Las funciones de estas agencias autonómicas coinciden con las de la Agencia Española, excepto para el caso antes señalado, así como en cuanto al movimiento internacional de datos y a la publicidad periódica respecto a la existencia de ficheros. Si bien estas agencias pueden establecer sus propios ficheros también han de inscribirse en la Agencia Española de Protección de Datos (AEPD).

Su existencia tiene su razón de ser en el hecho que cumplen funciones de asistencia a la AEPD tanto en cuanto a la inscripción de ficheros, como sancionatorias e inspectivas, asimismo implican un incremento en la calidad en el ejercicio de sus funciones.

Dentro de esta categoría de órganos creados por las Autoridades Autonómicas aparecen la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

3.4 Francia

La Comisión Nacional de Informática y Libertades (CNIL) fue creada por la Ley de 6 de enero de 1978, por lo que es una de las más antiguas autoridades de control en el dominio de la protección de datos personales.

Es un organismo único con competencia nacional, con estatuto específico. Constituyó en su creación la primera de las llamadas "autoridades administrativas independientes" (AAI), una nueva categoría de ente de derecho público.

Es una institución del Estado, que no está sometida a la autoridad jerárquica de ningún ministro. A las AAI les encarga el Estado la regulación y el control de sectores o problemáticas particulares, con una gran libertad de acción, aunque en el marco de una legislación específica. Los únicos controles que pueden ejercerse son los esenciales en un Estado de Derecho.

Es un órgano colegiado, compuesto de 17 miembros provenientes de diferentes sectores, nombrados por un período de 5 años.

La misión general de la CNIL es velar por el respeto de los derechos y las libertades de las personas, y asegurar que los tratamientos de datos personales sean de acuerdo a la Ley.

Las funciones que desempeña la autoridad de control son las siguientes:

a) Informar y asesorar a los interesados y a los responsables de tratamientos sobre sus derechos y obligaciones; contestar las solicitudes de los poderes públicos y de las empresas y formular recomendaciones; emitir dictámenes sobre proyectos de leyes y reglamentos relacionados con la protección de datos y sobre reglas profesionales y productos y otorgar certificaciones;

b) reglamentar y controlar el cumplimiento de los trámites previos a la realización de los tratamientos, y autorizarlos en los casos previstos por la ley;

c) garantizar el derecho de acceso (directo e indirecto);

d) instruir las peticiones y quejas;

e) controlar los ficheros y en su caso sancionar las infracciones a la ley.

La CNIL ejerce sus potestades principalmente a través de dos tipos de control: el control previo sobre la creación de los tratamientos, y el control a posteriori especialmente a través de la instrucción de las quejas, las inspecciones y el ejercicio de la potestad sancionadora.

3.5 Portugal

La Comisión Nacional de Protección de Datos es una entidad administrativa independiente que ejerce sus competencias a nivel nacional, cuyas atribuciones son controlar y fiscalizar el cumplimiento de las disposiciones legales y reglamentarias en materia de protección de datos personales.

Asimismo corresponde que sea consultada acerca de las disposiciones legales u otras que se estuvieren gestando en instituciones comunitarias o internacionales, relativas al tratamiento de datos personales, de acuerdo con lo dispuesto por la Ley N° 67/1998 de 26 de octubre.

Este órgano de control dispone de:

a) poderes de investigación y contralor;

b) poder de emitir pareceres previos al tratamiento de datos personales, asegurando su publicidad;

c) poder sancionatorio;

d) posee legitimidad para intervenir en procesos judiciales en caso de violación de las disposiciones de la ley, debiendo denunciar ante el Ministerio Público las infracciones penales que tuviere conocimiento, en ejercicio de sus funciones o por causa de ellas.

De acuerdo con lo dispuesto en la citada Ley está integrada por siete miembros de integridad y méritos reconocidos que duran cinco años en sus cargos.

3.6 Italia

La composición de esta autoridad independiente, denominada “el Garante” la establece el artículo 30.3 de la Ley N° 675, de 31 de diciembre de 1996 la cual dispone que el Garante es un órgano colegiado constituido por cuatro miembros, elegidos dos por la Cámara de Diputados, más dos miembros elegidos por el Senado de la República, entre personas que aseguren la independencia y que sean expertos de reconocida competencia en derecho o informática.

El legislador italiano optó por el modelo del comisionado parlamentario para la protección de datos. Además dotó al órgano de autonomía para la elección de su presidente y estableció requisitos que comportan la presencia de especialistas provenientes de los campos de la informática y el derecho.

Al Garante se atribuye un importante elenco de funciones que le permiten ejercitar un amplio grado de control sobre los ficheros de datos personales. Sus poderes son de muy variada naturaleza y comportan facultades de inspección, recomendación, denuncia y comunicación con otros poderes, entre otros, hasta el punto que, a salvo de las competencias de la "Autorità per l’informatica nella pubblica amministrazione" (AIPA) configuran al Garante como un órgano de competencia general en materia de protección de datos. Además, debe informar las disposiciones reglamentarias y los actos administrativos susceptibles de incidir en las materias reguladas por la Ley.

3.7 Unión Europea. Supervisor Europeo de Protección de Datos

Esta figura fue creada en el año 2001 por el artículo 286 del Tratado de la Comunidad Europea, aunque su funcionamiento comenzó a partir de 2004, traduciéndose en un control externo independiente encargado de supervisar la aplicación a las instituciones y organismos comunitarios de los actos comunitarios relativos a la protección de las personas físicas respecto al tratamiento de los datos de carácter personal y a la libre circulación de estos datos.

El Supervisor Europeo de Protección de Datos tiene la responsabilidad de garantizar que las instituciones u organismos de la UE respeten el derecho de las personas a la intimidad en el procesamiento de sus datos personales.

Las funciones del Supervisor Europeo de Protección de Datos se establecieron por la Decisión 1247/2002 que estableció el estatuto y las condiciones generales de ejercicio de sus funciones.

El Supervisor y un Supervisor Adjunto son designados por el Parlamento Europeo y el Consejo de la Unión Europea por un período renovable de cinco años.

Entre sus principales objetivos se encuentran los de asesorar a las instituciones y órganos comunitarios sobre el tratamiento de datos personales y el de cooperar con las autoridades nacionales y órganos de control.[85]

De esta forma, a nivel de Derecho Comparado se observa que los diversos órganos de control analizados han adoptado diferentes formas, así han sido organizados como:

a) Agencias con carácter autónomo de los Poderes del Estado, como es el caso de España;

b) Direcciones dependientes del Poder Ejecutivo, como es el caso de Argentina, y

c) Unidades Reguladoras generalmente organizadas como órganos desconcentrados con autonomía técnica, como es el caso de Uruguay. [86]

4. ÓRGANO DE CONTROL URUGUAYO. UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES

4.1. Creación

La creación del órgano de control uruguayo tiene como antecedente en la materia la Ley N° 17.838 de 24 de setiembre de 2004, por la cual se dictaron

---

[85] http://www.jcyl.es/web/jcyl?c=Page&cid=1162493472261&pagename=Portal_Eucyl%2FPage%2FEucylPlantillaAreaTrabajoCompleta. Página visitada el 17 de agosto de 2010.

[86] RODRIGUEZ ACOSTA, Beatriz Marlene. “Control de Tratamiento de Datos Personales” en Anuario de Derecho Informático. Tomo X, 1era. Edición Año 2009. FCU, pág. 146.

normas para la protección de los datos personales a ser utilizados en informes comerciales. En el artículo 20 se disponía lo siguiente:

"Artículo 20.- El Ministerio de Economía y Finanzas actuará como órgano de control en el tratamiento de datos personales comprendidos en esta ley y tendrá como cometido implementar, vigilar y asesorar en todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley.

Dicha función de control será ejercida por el Ministerio de Economía y Finanzas asistido de una Comisión Consultiva integrada por siete miembros, tres de los cuales serán representantes de dicho Ministerio, uno de los cuales la presidirá; dos representantes del Ministerio de Educación y Cultura, un representante de la Cámara Nacional de Comercio y de Servicios y un representante de la Liga de Defensa Comercial……."

Asimismo el artículo 21 de la citada Ley permitía establecer sanciones al órgano de control, las cuales se graduaban desde apercibimiento, multa, hasta clausura del archivo, registro o base de datos.

Es de hacer notar que la Ley N° 17.838 sólo era aplicable al tratamiento de datos destinados a brindar informes objetivos de carácter comercial, según lo disponía su artículo 1°, quedando expresamente excluido del mismo el tratamiento de datos que no fueren de carácter comercial (artículo 2º).

El Decreto N° 399/006, de 30 de octubre de 2006, en su artículo 2º dispuso que: "El Registro estará a cargo de la Comisión Consultiva creada por la Ley N° 17.838, de 24 de setiembre de 2004.

La Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, de 11 de agosto de 2008 (LPDP), en su artículo 31 creó como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), la Unidad Reguladora y de Control de Datos Personales (URCDP), la cual funcionará con amplia autonomía técnica.
Está integrada por tres miembros, el Director Ejecutivo de AGESIC y dos miembros que son 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 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 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.

Actualmente ocupa el cargo de Director Ejecutivo de AGESIC el Ingeniero José Clastornik, nombrado por Resolución N° 626/007 de Presidencia de la República, de 24 de setiembre de 2007.

De acuerdo con la Resolución Nº 316/009, de 14 de abril de 2009 fueron designados por el Poder Ejecutivo el Dr. Felipe Rotondo Tornaría y el A/S Federico Monteverde para ocupar los cargos de Miembros del Consejo Ejecutivo de la Unidad, los cuales tomaron posesión de sus cargos el 24 de abril siguiente.

De acuerdo con lo dispuesto por el artículo 21 del Decreto Reglamentario N° 414/009 de la citada Ley, de 31 de agosto de 2009, la Presidencia de la URCDP será rotativa anualmente entre los integrantes del Consejo Ejecutivo, a excepción del Director Ejecutivo de la AGESIC. En caso de ausencia del Presidente de la Unidad, la Presidencia será ejercida interinamente por el miembro restante nombrado por el Poder Ejecutivo.

El 5 de junio de 2009 en sesión del Consejo Ejecutivo de la URCDP se resolvió designar como primer Presidente de la misma al A/P Federico Monteverde, cargo que desempeñó hasta el 18 de junio de 2010 fecha en que fue nombrado como nuevo Presidente de la Unidad, el Dr. Felipe Rotondo.

Los cometidos del Presidente están expresamente establecidos en el artículo 22 del referido Decreto Reglamentario.

4.2 Cometidos

Serán atribuciones del Consejo Ejecutivo de la URCDP de acuerdo con lo dispuesto por el artículo 34 de la Ley N° 18.331 y el artículo 155 de la Ley N° 18.719 de 24 de diciembre de 2010, las siguientes:

“Asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

- Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.
- Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de esas bases.

- Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos pudiendo, a tales efectos, realizar las actuaciones de inspección pertinentes. Esta atribución fue modificada por la Ley N° 18.719 estableciendo lo siguiente: Controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.

A tales efectos la Unidad Reguladora y de Control de Datos Personales tendrá

las siguientes potestades:

1) Exigir a los responsables y encargados de tratamientos la exhibición de los libros, documentos y archivos, informáticos o convencionales, propios y ajenos, y requerir su comparecencia ante la Unidad para proporcionar informaciones.
2) Intervenir los documentos y archivos inspeccionados, así como tomar medidas de seguridad para su conservación, pudiendo copiarlos.
3) Incautarse de dichos elementos cuando la gravedad del caso lo requiera hasta por un lapso de seis días hábiles; la medida será debidamente documentada y sólo podrá prorrogarse por los órganos jurisdiccionales competentes, cuando sea imprescindible.
4) Practicar inspecciones en bienes muebles o inmuebles ocupados a cualquier título por los responsables, encargados de tratamiento y demás sujetos alcanzados por el régimen legal. Sólo podrán inspeccionarse domicilios particulares con previa orden judicial de allanamiento.
5) Requerir informaciones a terceros, pudiendo intimarles su comparecencia ante la autoridad administrativa cuando ésta lo considere conveniente o cuando aquellas no sean presentadas en tiempo y forma.

La Unidad Reguladora y de Control de Datos Personales podrá solicitar el auxilio de la fuerza pública para el desarrollo de sus cometidos.

- Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran.
En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.

- Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.
- Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.

- Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.”

Asimismo de acuerdo con lo dispuesto por el artículo 35 de la Ley N° 18.331 y la modificación introducida por el artículo 152 de la Ley N° 18.719, es potestad del órgano de control aplicar las sanciones correspondientes a los responsables de las bases de datos o encargados del tratamiento de datos en el caso de violación de las normas expresadas. Dichas sanciones se graduarán en atención a la gravedad, reiteración o reincidencia de la infracción cometida desde:

a) observación,
b) apercibimiento,
c) multa de hasta quinientas mil unidades indexadas,
d) suspensión de la base de datos respectiva por el plazo de cinco días,
e) clausura de la base de datos respectiva. A tal efecto se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes la clausura de las bases de datos que se comprobare que infringieren o transgredieren la presente ley.

Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales. La clausura deberá decretarse dentro de los tres días siguientes a aquél en que la hubiere solicitado la AGESIC, la cual quedará habilitada a disponer por sí en caso que el Juez no se pronunciare dentro de dicho término.

En este último caso, si el Juez denegare posteriormente la clausura, ésta deberá levantarse de inmediato por la URCDP.

Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la suspensión, no tendrán efecto suspensivo.
Para hacer cumplir dicha resolución, la URCDP podrá requerir el auxilio de la fuerza pública.

La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura, Nº 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Las resoluciones firmes de la URCDP que impongan sanciones pecuniarias, constituyen título ejecutivo a sus efectos.

En este sentido, en la Resolución N° 890/010, de 16 de julio de 2010, dictada por el Consejo Ejecutivo de la URCDP se estableció lo siguiente:
“1) Las sanciones se graduarán como muy leves, leves, graves y muy graves.

2) La sanción de apercibimiento corresponderá cuando la infracción a las disposiciones de la LPDP sea de carácter muy leve.

3) Para la imposición de la sanción de multa se tendrá en cuenta si el grado de la conducta infraccional encuadra en la categoría de leve, grave o muy grave y se graduarán, en cada una de las categorías, por tres escalas:

Mínimo, Medio y Máximo, apreciándose las circunstancias atenuantes o agravantes que puedan confluir en cada caso, teniendo en cuenta los siguientes guarismos:

Leves: Mínimo de 100 a 3.000 Unidades Indexadas
Medio de 3001 a 6.000 Unidades Indexadas
Máximo de 6001 a 12.000 Unidades Indexadas

Graves: Mínimo de 12.001 a 30.000 Unidades Indexadas
Medio de 31.001 a 60.000 Unidades Indexadas
Máximo de 60.001 a 90.000 Unidades Indexadas

Muy Graves: Mínimo de 90.001 a 150.000 Unidades Indexadas
Medio de 150.001 a 300.000 Unidades Indexadas
Máximo de 300.001 a 500.000 Unidades Indexadas

4) Cuando la infracción a las disposiciones de la LPDP sea de carácter gravísimo, podrá considerarse la imposición de la sanción de suspensión de la Base de Datos respectiva.

5) En todo caso, para determinar qué sanción es razonable y proporcional al hecho cometido, se apreciará el tipo de datos personales objeto de tratamiento, las medidas de seguridad, los derechos personales vulnerados, el volumen de los tratamientos efectuados, los beneficios obtenidos, sean económicos o de otra índole, el grado de intencionalidad, la reincidencia, los daños y perjuicios causados a las personas interesadas y a terceras personas, y cualquier otra circunstancia que sea relevante para evaluar la conducta infraccional cometida. Asimismo, deberán tenerse en cuenta eventuales eximentes de responsabilidad que puedan conjugarse, como la fuerza mayor o caso fortuito."

De acuerdo con la modificación dispuesta por la Ley N° 18.719, el Consejo Ejecutivo de la URCDP aprobó la Resolución N° 320/2011 el 17 de marzo de 2011 por la que dispuso lo siguiente: " …….1) Las sanciones se graduarán como muy leves, leves, graves y muy graves.

2) La sanción de observación corresponderá cuando la infracción a las disposiciones de la LPDP sea de carácter muy leve.

3) Se aplicará la sanción de apercibimiento cuando la infracción a las disposiciones de la LPDP sea de carácter leve y no existan antecedentes de infracciones anteriores.

4) Para la imposición de la sanción de multa se tendrá en cuenta si el grado de la conducta infraccional encuadra en la categoría de leve con antecedentes, grave o muy grave.

5) Las sanciones de suspensión o clausura de la base de datos respectiva se impondrán cuando la infracción a las disposiciones de la LPDP sea de carácter muy grave y, en aplicación de los principios de razonabilidad y proporcionalidad, la sanción de multa no resulte lo suficientemente adecuada, atendiendo a la violación de las disposiciones de la Ley.

4.3 Actuación de la URCDP

La labor del Consejo Ejecutivo de la URCDP se formaliza a través de resoluciones y dictámenes.

Las resoluciones versan sobre inscripciones de bases de datos y códigos de conducta, autorizaciones de transferencias internacionales, y denuncias.
Los dictámenes versan sobre consultas realizadas a la Unidad acerca de diferentes asuntos relativos a la protección de datos personales.

De acuerdo con lo dispuesto por el artículo 24 del Decreto Reglamentario N° 414/009 las resoluciones se tomarán por mayoría, en el caso de empate el asunto se pospondrá para la próxima sesión y en caso de subsistir, el voto del Presidente se computará doble.

A los actos dictados por el Consejo Ejecutivo se le dará la correspondiente publicidad mediante la publicación en su sitio web, posteriormente a la notificación del caso, aplicando criterios de disociación de los datos personales que figuren en los mismos.

En caso de tratarse de actos de carácter general la publicidad se dará a través del referido sitio web además del Diario Oficial.

4.4 Consejo Consultivo

El Consejo Ejecutivo de la URCDP funciona asistido por un Consejo Consultivo, integrado por cinco miembros:

- Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser Legislador en actividad.
- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica. De acuerdo con lo dispuesto por el artículo 28 del citado Decreto Reglamentario, este representante será designado por la Facultad de Derecho de la Universidad de la República a propuesta del Instituto de Derecho Informático.
- Un representante del sector privado, que se elegirá en la forma establecida reglamentariamente. De acuerdo con lo dispuesto por el artículo 28 del Decreto Reglamentario N° 414/009, este representante será designado por la Cámara Nacional de Comercio y de Servicios.

Sesiona presidido por el Presidente de la Unidad Reguladora y de Control de Protección de Datos Personales.

Sus integrantes duran cuatro años en sus cargos y sesionan a convocatoria del Presidente de la Unidad Reguladora y de Control de Datos Personales o de la mayoría de sus miembros.

Puede ser consultado por el Consejo Ejecutivo sobre cualquier aspecto de su competencia y debe ser consultado por éste cuando ejerza potestades de reglamentación.

Según lo dispuesto por el artículo 26 del Decreto Reglamentario N° 414/009, el Consejo Consultivo es convocado por el Consejo Ejecutivo, con una antelación mínima de cinco días y sesionará con una mayoría simple de sus integrantes.

Habiendo quórum para sesionar, el Presidente deberá declarar abierta la sesión, disponiendo leer el acta o actas anteriores correlativas si las hubiera.

De todo lo actuado por el Consejo Consultivo se deja constancia en acta, la cual una vez aprobada será firmada por todos los asistentes.

De acuerdo al artículo 27 las decisiones se toman por mayoría de sus miembros, el Presidente tendrá voz pero no voto.

En función de lo establecido por el artículo 32 de la citada Ley, el Consejo Ejecutivo de la URCDP ha convocado a cada uno de organismos correspondientes a la designación de sus representantes, habiéndose realizado los siguientes nombramientos:

a) el Poder Legislativo no ha designado a su representante.
b) en representación del Poder Judicial se designó a la Dra. Ivonne Carrión Ramos;
c) en representación del Ministerio Público y Fiscal se designó como titular a la Fiscal Letrado Adjunta Dra. Patricia Marquisá Horgales.
d) en representación del área académica fue designada la Dra. Maricarmen Pascale.
e) en representación del sector privado fue designado el Dr. Juan Mailhos Gutiérrez.

5. CONCLUSIONES

Los derechos instituidos en los diferentes ordenamientos jurídicos, con el fin de amparar a las personas en su derecho fundamental a la protección de los datos personales, y los principios que se deben cumplir en el tratamiento de los datos personales, determinaron el surgimiento de una nueva institucionalidad a fin de asegurar la aplicación efectiva de los mismos. En tal sentido los órganos de control se han transformado en garantes reales y efectivos del cumplimiento de las legislaciones en la materia, cuya existencia se ha tornado de vital importancia al momento de efectivizar la protección de este derecho humano, como afianzadores y reguladores del mismo.

CAPÍTULO VI – DATOS ESPECIALMENTE PROTEGIDOS

Dr. Marcelo Bauzá

1. INTRODUCCIÓN

Para la Ley uruguaya ingresan a esta categoría (Capítulo IV, artículos 18 a 23), las siguientes especies de datos personales: datos sensibles, datos relativos a la salud, datos relativos a las telecomunicaciones, datos relativos a bases de datos con fines de publicidad, datos relativos a la actividad comercial o crediticia, y datos transferidos internacionalmente.

En todos estos casos, el registro y tratamiento de los datos personales goza de un nivel de protección superior al estándar o de regla contenido en la misma ley, lo que se traduce en restricciones de diversas clases o alcances. El legislador entendió que debía imponer mayores regulaciones o requisitos a los que de por sí ya rigen en la misma ley de modo general, atendiendo la presencia de factores de riesgo mayores al común u ordinario.

En definitiva, se trata de ciertas categorías de datos personales, y también de actividades ("tratamientos" para el lenguaje sectorial) a las que adscriben tales datos, que quedan sujetas no solamente a la normativa general contenida en la Ley Nº 18.331, sino también a las previsiones especiales o particulares contenidas de modo más específico en este Capítulo, primando las últimas en caso de conflicto con las primeras.

2. DATOS SENSIBLES

2.1. Concepto y alcances

El legislador define los datos sensibles como aquellos datos personales que revelen origen racial y ético, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual" (artículo 4º lit. E) de la Ley). Se trata de una definición que proviene de la ley argentina (Ley de Protección de Datos de Carácter Personal Nº 25.326, de 30 de octubre de 2000).

Estamos ante una familia de variada tipología, pero todas ellas calificadas por la "posibilidad de generar por su contenido, actitudes discriminatorias respecto de sus titulares"[87].

2.2. Antecedentes nacionales y derecho comparado

El antecedente normativo nacional inmediato de este Capítulo lo encontramos en la Ley N° 17.838, de 24 de setiembre de 2004, cuyo artículo 2° excluye de

[87] PEYRANO, Guillermo F. "Régimen Legal de los Datos Personales y Hábeas Data", publicado por Lexis-Nexis, 1ª Edición, Año 2002. Depalma, pág. 36, Buenos Aires.

su ámbito a los “datos sensibles sobre la privacidad de las personas, entendiéndose por éstos, aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas filosóficas o morales, afiliación sindical o información referente a la salud o a su sexualidad y otra zona reservada a la libertad individual”. La exclusión practicada de modo nominal y evitando regular con mayor extensión este tipo de datos, resultó coherente en su momento con el alcance de la citada norma hoy derogada, sectorizada al registro y tratamiento de datos exclusivamente de naturaleza comercial.

Habrá que recurrir a las fuentes del derecho comparado para conocer un poco más sobre el origen y modelo de la regulación estatuida, tanto en el régimen anterior como en el actual, para este tipo de datos personales.

El artículo 6º del Convenio 108 de 1981 del Consejo de Europa de protección de las personas en relación con el tratamiento automatizado de datos de carácter personal establece que “los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.”

Por su parte la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos mantiene con algunos ajustes la conceptualización del Convenio 108, pero dedicando alguno de sus “Considerandos” a la temática en examen, y articulando un régimen más detallado que el contenido en el Convenio 108.

En los Considerandos 33 a 36 de la precitada Directiva Europea se expresan ricos conceptos que inspiran todo el devenir normativo europeo en la materia, y por añadidura también el latinoamericano, incluyendo el uruguayo, todos ellos en fases de desarrollo bastante posteriores en el tiempo. No escapan a este paradigma los datos sensibles, desprendiéndose de la lectura de estos Considerandos el natural y último fundamento en cuanto a prohibir como regla su registro y tratamiento (33- “…los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad, no deben ser objeto de tratamiento…”), así como las excepciones autorizadas por las que se permite levantar la prohibición (necesidades específicas, consentimiento explícito del interesado, interés público importante).

Todo esto ya figura anunciado en los precitados Considerandos de la Directiva 95/46/CE. Pero la Directiva enuncia igualmente la regla prohibitiva en su parte dispositiva, concretamente en el primer numeral del artículo 8º: “Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad”. El mismo artículo, en su segundo numeral, desarrolla el régimen de excepciones al que hacen referencia los Considerandos.

2.3. Análisis de la definición contenida en el art. 4º lit. E) de la Ley Nº 18.331

La definición legal uruguaya sigue el modelo europeo enunciado en el apartado precedente si bien pueden advertirse algunas pequeñas variantes, provenientes de haber tomado en este caso, como fuente directa, una norma no originaria sino derivada, como fue la norma argentina.

Ante todo se advierte que, al igual que en el sistema jurídico europeo, nos encontramos con una definición que contiene conceptos o hipótesis de entendimiento acotado (numerus clausus), restando margen al intérprete para incluir otro tipo de situaciones que las señaladas en la norma, aunque las mismas, llegado el caso, fueran igualmente susceptibles de convertirse en factores o peligros de discriminación contra la persona.

Más allá de esta apreciación inicial o básica, de todos modos las hipótesis efectivamente contempladas prevén en conjunto la mayoría o totalidad de razones o ideas bajo las que se han edificado históricamente los atavismos y juicios críticos sobre individuos y pueblos enteros de la especie humana, significando factores de segregación jurídica y éticamente inadmisibles. De ahí la restricción al registro y tratamiento de este tipo de datos, y la especificación de las categorías o tipos considerados a tales efectos.

El "origen racial y étnico" comprende aquella información que revela la pertenencia a cierta etnia, pueblo o nación, con independencia de los vínculos meramente estatales de la persona o grupo de que se trate; incluye el color de piel y otros rasgos antropomórficos de fuerte distinción entre seres humanos, como ser el color y forma de los ojos, forma del cráneo, grado de pilosidad, entre otros.

Las "preferencias políticas, convicciones religiosas o morales" y en buena parte también la "afiliación sindical", son aspectos que hacen o se vinculan a la ideología y creencias fundamentales de las personas. Incluso la falta o prescindencia de estas preferencias (apoliticismo, ateísmo) resulta ser igualmente un dato sensible, manteniéndose un ligamen profundo de estos factores con las libertades públicas, y por ende el peligro del alto poder discriminatorio que emana de la disponibilidad y manipulación de este tipo de informaciones.

Los datos personales relativos a la "salud" han sido catalogados como "supersensibles", tanto que en ciertos casos se justifica restringir el acceso incluso a su propio titular, mediatizándolo por un profesional de la Medicina cuando el conocimiento liso y llano de una enfermedad, por ejemplo, pudiera sumir al individuo en una grave crisis psicológica llevándolo, en casos extremos, al suicidio[88]. Se trata de un vasto campo que incluye la salud

[88] TONIATTI, Roberto. "Libertad Informática y Derecho a la Protección de Datos Personales: Principios de Legislación Comparada", pág. 158 sgtes., cita tomada de SÁNCHEZ BRAVO, Álvaro A. "La Regulación de los Datos Sensibles en la LORTAD" Informática y Derecho N° 6-7. UNED, Mérida, España, 1994, págs. 117 sgtes..

pasada, presente y futura, física y mental, de los afectados. Refiere tanto a personas sanas como enfermas, vivas y fallecidas; se extiende al abuso del alcohol y el consumo de drogas, estupefacientes y psicotrópicos.

En lo que refiere a comportamientos o rasgos vinculados a la "vida sexual", se alude con ello a todo dato que señale o distinga las actividades y costumbres sexuales de los ciudadanos, y las consecuencias o deducciones que de ello puedan extraerse. Las referencias indirectas a ciertos hábitos grupales o desviados de una regla ética y/o social común, también entran en esta categoría de datos. Así, por ejemplo, la suscripción a publicaciones de contenido erótico, y la pertenencia o militancia en ciertos colectivos u organizaciones vinculadas a la llamada diversidad sexual. Existen enfermedades vergonzantes o estigmatizantes del punto de vista social, cuyo conocimiento más allá del ámbito requerido para su tratamiento, puede resultar netamente perjudicial para la reputación del individuo (ej. portadores de VHI-SIDA), por lo que también ingresan al ámbito en examen.

Finalmente, si bien no incluida en la definición objeto de examen, los datos personales relativos a la "comisión de infracciones penales, civiles o administrativas" también deben ser considerados como especies de datos sensibles. Así los considera el propio legislador en otra parte de la Ley (artículo 18). Se trata, como en los casos incluidos expresamente en la definición del artículo 4º, de informaciones cuyo tratamiento sin restricciones puede poner en grave e injustificado riesgo la intimidad de las personas. Sobre todo cuando se trata de procesos judiciales o administrativos aún no culminados, o de sentencias ya cumplidas o extinguidas.

2.4. Régimen legal aplicable a su recolección y tratamiento

Siguiendo los modelos europeo y argentino, el artículo 18 de la Ley uruguaya establece como regla, desde el primer inciso, factores limitantes para el tratamiento de los datos sensibles. No conforme con enunciar de este modo la regla, el legislador ratifica más adelante en el mismo artículo, el carácter drástico de la misma, empleando para ello un giro más severo, preciso y particularizado: "Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles" (inciso 3°).

La norma es extensa, abordando ciertas excepciones y su forma de aplicación. Algunas de estas excepciones son de tipo general. Otras más particulares en tanto se las afecta o vincula con cierto tipo de datos y finalidades que justifican el levantamiento o flexibilización de la prohibición.

Como excepciones generales, en las que la regla de la interdicción se revierte para dar paso a la legitimidad de la recolección y tratamiento de datos sensibles, se prevén las siguientes:

Consentimiento expreso y escrito del titular.
Razones de interés general autorizadas por ley.
Mandato legal del organismo solicitante.

Finalidades estadísticas o científicas, con disociación de sus titulares.

La expresión “sólo pueden ser recolectados y objeto de tratamiento…” prevista en el inciso 2° para las hipótesis 2 a 4 mueve a la duda sobre qué sucede con el consentimiento del titular previsto en el inciso 1º de un modo que prima facie aparenta carácter excluyente.

En la necesidad de tener que asumir una postura clara y unívoca sobre el punto, parece razonable sostener, cuanto menos de modo genérico, que los datos sensibles pueden tratarse cuando existen alguna de las razones o hipótesis previstas con ulterioridad (hipótesis 2 a 4) y, aún en caso que no se dieran estas razones, cuando el titular preste su consentimiento expreso y escrito. O sea que no le atribuimos carácter acumulativo al requisito del consentimiento.

El artículo 18 contempla otras excepciones a la prohibición de tratar datos sensibles, para ámbitos más específicos que los que vienen de examinarse:

1- Bases de datos de asociados o miembros de partidos políticos y otras agrupaciones (sindicatos, iglesias, asociaciones, fundaciones y otras entidades sin fines de lucro).

2- Datos personales relativos a la investigación y comisión de infracciones penales, civiles o administrativas.

Estos últimos solo pueden ser objeto de tratamiento por las autoridades públicas competentes y en el marco de las leyes y reglamentaciones respectivas. Y ello no inhibe la comunicación o publicidad de la identidad de personas físicas o jurídicas que están siendo investigadas o han cometido infracciones a la normativa vigente, con arreglo a otro tipo de normas.

3. DATOS RELATIVOS A LA SALUD

3.1. Salud y datos personales

No está demás reiterar el cariz amplio e importante que asume este tipo de datos, dentro de las fuentes normativas propias del régimen de protección de datos personales. La doctrina es conteste en resaltarlo: “…la consideración de datos sanitarios o de datos médicos es muy amplia en la concepción de las autoridades europeas de protección de datos y de las legislaciones europeas. ¿Por qué? Porque todas ellas nacen o beben del Convenio 108 de protección de datos de las personas físicas en lo que respecta a su tratamiento automatizado, del Consejo de Europa. Y en el memorando explicativo, en el preámbulo de este Convenio, se definen los datos personales como todos aquellos datos referentes a la salud física o mental de un individuo, pasados, presentes o futuros, incluidos aquellos que hacen referencia al consumo de alcohol o consumo de drogas. Con lo cual, el concepto de datos de salud, el concepto de datos sanitarios, es muy amplio dentro de la legislación europea. Y por eso las salvaguardias aplicables a los datos de salud no se aplican sólo a

aquellos datos que están en manos de los médicos, sino a aquellos datos que fluyen dentro de otros ámbitos".[89]

Contribuye a esa necesaria amplitud de criterio, la definición contenida en el acápite de la Carta de Constitución de la Organización Mundial de la Salud (1946), que considera a la salud como "un estado completo de bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades".

La Ley Nº 18.331 en su artículo 19 refiere si se quiere con mayor parquedad al mismo tema ("…salud física o mental…") pero nada impide dar por válida la interpretación extensiva propuesta, recogiendo las citadas fuentes, dada la generalidad de la fórmula empleada por el legislador.

Por lo tanto estamos ante una de esas categorías de datos personales en las que cabe hablar de numerus apertus, lo que posibilita recoger los avances de la ciencia y las interpretaciones actualizadas de lo que puede llegar a constituir una cuestión de salud, tal la obesidad, enanismo, consumo de alcohol, genética, entre otros fenómenos, siempre que hagan mención a una persona física determinada o determinable.[90]

3.2. Sujetos alcanzados por el régimen legal

El artículo 19 de la Ley Nº 18.331 regula este tipo de datos personales (a los que desde luego se les aplica también, y en lo pertinente, lo consignado en el artículo inmediato anterior para los datos sensibles), y comienza por delimitar los sujetos que pueden recolectarlos y tratarlos.

Se trata de dos clases de sujetos solamente: los "establecimientos sanitarios públicos o privados" y los "profesionales vinculados a las ciencias de la salud". Hay aquí, pues, un régimen estricto y cerrado en cuanto a quiénes están legitimados para tomar y tratar este tipo de datos.

No resulta vano recordar que cuando la Ley Nº 18.331 refiere a "tratar los datos personales", ya sea en el artículo 19 como en otras partes del articulado, debemos remitirnos a la definición de "tratamiento de datos" contenida en el artículo 4º literal M, que abarca actividades de toda índole, incluyendo consultas, interconexiones y transferencias.

Desde luego también resulta aplicable en lo pertinente el artículo 11 inciso 2 de la misma Ley, en cuanto a que también quedan alcanzados por el ámbito del artículo 19 "las personas que, por su situación laboral y otra forma de relación con el responsable de una base de datos…" (en este caso con los establecimientos y los profesionales a que alude esta norma) "…tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales…".

---

[89] ACED FELEZ, Emilio. "La visión del sector en España" en "¿Seguridad, privacidad, confidencialidad? El desafío de la protección de datos personales", Trilce, Montevideo, 2004, pág. 139.

[90] BRIAN NOUGRERES, Ana. "La protección de los datos concernientes a la salud de las personas" en Anuario de Derecho Informático. Tomo VII. 1era. Edición Año 2007. FCU, págs. 191 y sgtes.

3.3. Requisitos especiales para su recolección y tratamiento

El artículo 19 establece otro tipo de requisitos sustantivos para legitimar la recolección y tratamiento de datos relativos a la salud, además de los ya analizados referidos a sujetos autorizados a hacerlo.

Tales requisitos son de dos órdenes:

1º- Que los datos a tratar refieran a pacientes que acuden o hubieren estado bajo tratamiento de tales sujetos.

2º- Que se respeten los principios del secreto profesional, la normativa específica y lo establecido en la Ley Nº 18.331.

En cuanto a los principios del secreto profesional y su normativa específica, resultaría excesivo a los fines de esta publicación ingresar con detalle a su régimen normativo, rico en pormenores.

El "secreto profesional" está previsto en normas estatuidas a diferentes fines, con sus reglas y excepciones propias (Código Penal, Código del Proceso Penal), e incluso en expresiones de autorregulación como es el Código de Ética Médica del SMU y FEMI.[91]

En cuanto a la "normativa específica" a la que alude el artículo 19, debe tenerse en cuenta primordialmente la Ley Nº 18.335, de 15 de agosto de 2008, sobre "pacientes y usuarios de servicios de la salud, derechos y obligaciones" que entre otros aspectos, regula el derecho al conocimiento de la situación de salud, comprendiendo la historia clínica, y el derecho de privacidad. Esta ley ha sido reglamentada por el Decreto Nº 274/010, de 8 de setiembre de 2010.

3.4. Casos de jurisprudencia

En el ámbito nacional no se registran prácticamente casos judiciales relativos a protección de datos personales de salud. Apenas hemos podido relevar uno que fue denegado, atinente a un reclamo de daños y perjuicios en torno a la entrega a un paciente de su historia clínica. Se trataba de un demanda por daño moral y físico, basada en la negativa de la entidad médica a entregar la historia clínica, mala atención y falta de información sobre los resultados de estudios efectuados, afirmaciones todas que no prosperaron. En lo referente a la historia clínica quedó acreditado que "le fue entregada cuando la actora lo solicitó y siendo un derecho del paciente acceder a la misma (Decreto Nº

[91] www.smu.org.uy/elsmu/institucion/documentos/doc/cem.html Página visitada el 14 de setiembre de 2010. Un escrito doctrinario referido específicamente al campo de la profesión médica, puede encontrarse en ADRIASOLA, Gabriel, "Análisis del secreto profesional del médico" www.mednet.org.uy/dml/bibliografia/nacional/tx-020917.htm Página visitada el 14 de setiembre de 2010.

258/1992, art. 42), la actora pudo haberla pedido aún antes de desafiliarse e interrumpir el tratamiento". [92]

4. DATOS RELATIVOS A LAS TELECOMUNICACIONES

4.1. Telecomunicaciones y datos personales

Las telecomunicaciones en todas sus variedades (por hilos, por aire, redes, telefonía, fax, mensajes de texto, televisión por cable y satelital, etc.) representan una dimensión diferente, y al mismo tiempo merecedora de especial atención, a los efectos de la protección de los datos personales.

No en vano en Europa se le ha prestado particular tratamiento jurídico a esta dimensión, a través de una normativa especial contenida en la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), que busca "garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad." [93]

Dentro de un elenco variopinto de tecnologías, la expansión universal de Internet ha significado –junto con sus beneficios- un paralelo avance invasivo sobre la privacidad de las personas, por múltiples vías. Una descripción amena y no exenta de profundidad sobre las variadas formas en que se vulnera la privacidad de las personas en Internet, puede encontrarse en el análisis que practica el profesor español Suñé Llinás.[94]

4.2. Sujetos alcanzados por el régimen legal

El artículo 20 de la Ley uruguaya alcanza con su régimen a todas las modalidades expuestas, para lo cual establece quienes son los sujetos alcanzados como responsables frente al registro y tratamiento de datos personales a este nivel. Se trata de "los operadores que exploten redes públicas" y también de aquéllos "que presten servicios de comunicaciones electrónicas disponibles al público". Por ende, todo sujeto de derecho (persona física o jurídica, pública o privada) que actúe en el mercado de las

---

[92] J. Ltdo. Primera Instancia Civil 18º Turno, sentencia Nº 62 de 26 de octubre de 2007, suma en Anuario de Derecho Informático. Tomo VIII, 1era. Edición Año 2008. FCU, pág. 362. Un panorama doctrinario y jurisprudencial de la temática en el ámbito latinoamericano, aunque referido al tema sectorial de los datos de pacientes con VIH-SIDA, se encuentra en WIERZBA, Sandra M. "Protección de Datos de Salud en Procesos Judiciales. Transparencia judicial y confidencialidad de datos de litigantes con VIH-SIDA: ¿existe oposición entre tales principios?" consultable en www.ifai.org.mx/pdf/ciudadanos/sitios_de_interes/datos_personales/Protecci%C3%B3nDeDatosDeSaludEnPJ.pdf Página visitada el 14 de setiembre de 2010.

[93] Artículo 1.1. de la Directiva. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:NOT Página visitada el 14 de setiembre de 2010.

[94] SUÑÉ LLINÁS, Emilio. "La protección de datos personales en Internet", www.ieid.org/congreso/ponencias/Su%F1%E9%20Llin%E1s,Emilio.pdf Página visitada el 14 de setiembre de 2010.

telecomunicaciones, en cualquiera de sus segmentos, como titular o responsable de un servicio, estará alcanzado por esta norma.

Es del caso preguntarse qué es lo que se exige a estos operadores y prestadores en relación con la protección de los datos personales pertenecientes a sujetos con los que se vinculan. La respuesta pertinente a esta interrogante, con la correspondiente expectativa de parte del interesado o titular del dato, adopta una triple dimensión: seguridad, confidencialidad, consentimiento.[95]

4.3. Relevancia del principio de seguridad y el derecho de información

Estamos ante un precepto normativo especial, como todos los que vienen siendo objeto de examen en el presente capítulo, y que por ende asume ciertos particularismos.

Por tanto, una vez definidos quienes serán los responsables de la protección de datos personales en el sector, la norma pone el acento inmediatamente en otros aspectos.

Un primer elemento se relaciona con el factor o principio de seguridad, a partir del cual se establece el deber de ese responsable, en cuanto a adoptar las medidas técnicas y de gestión adecuadas, que garanticen la seguridad en la explotación de la red o en la prestación del servicio en su caso, conforme los niveles de protección exigidos por la reglamentación de la Ley. Corresponde advertir que esta regulación "por niveles" en materia de medidas de seguridad, no ha sido aún fijada, rigiendo por el momento los arts. 7º y 8º del Decreto Nº 414/009, de 31 de agosto de 2009, que no contemplan tal distinción.[96]

El legislador ha querido, asimismo, dar realce en este sector al deber de información como segundo elemento. Se aprecia que lo ha hecho previendo la posible existencia de algún riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, en cuyo caso, a través de las cláusulas contractuales o de advertencia correspondientes, ese operador deberá advertir a los abonados sobre el mencionado riesgo, y las medidas a adoptar.

Finalmente, la norma objeto de examen deja a salvo expresamente lo que surja de otras normativas especiales relativas a telecomunicaciones, vinculadas a la seguridad pública y la defensa nacional. La norma puede parecer sobreabundante, desde el momento que refiere a una materia expresamente excluida de la Ley y, por tanto, no afectada por ésta (artículo 3º literal B).

4.4. Casos de jurisprudencia

---

[95] DELPIAZZO, Carlos. "Derecho de las Telecomunicaciones". Universidad de Montevideo, Facultad de Derecho. Montevideo, 2005, pág. 94.

[96] El art. 80 del Real Decreto español 1720/2007 prescribe tres niveles de seguridad para las bases de datos y tratamientos: básico, medio y alto.

No hemos encontrado casos judiciales nacionales en este punto, si se exceptúa lo referido a la protección constitucional y penal de las telecomunicaciones, tema afín pero diferente del que venimos analizando. En tal sentido, se ha podido considerar la interceptación de correos electrónicos dentro de la figura tipificada en el artículo 296 del Código Penal.[97]

Un renglón temático que merece particular atención tanto para el presente ítem como para el siguiente, consiste en el envío de correo basura o spam, que en cierto modo representa, o se apoya, en un manejo ilegítimo de datos personales al ser utilizados en comunicaciones a distancia. En algunos países este tipo de asuntos han llegado a los tribunales. Es el caso de Argentina donde, "en una medida sin precedentes en el país, el juez Roberto Torti, a cargo del Juzgado Civil y Comercial Federal Nº 3, dictó una medida cautelar contra un emisor de correo electrónico no solicitado, quien deberá abstenerse de seguir enviando e-mails a los demandantes, al menos mientras dure el litigio." [98]

5. DATOS RELATIVOS A BASES DE DATOS CON FINES DE PUBLICIDAD

5.1. Publicidad y datos personales

La materia encuadra o aplica, tanto respecto del envío de comunicaciones comerciales tradicionales, como electrónicas. Como bien se ha podido expresar, "para llevar a cabo tales actividades es imprescindible que el anunciante, o su agencia de publicidad, dispongan de archivos o listados de datos personales, que les permitan seleccionar para el envío de su publicidad a aquellas personas que, de acuerdo con los datos incluidos en tales archivos, pueda estar interesados en sus productos o servicios".[99]

5.2. Actividades y perfiles admitidos

El régimen legal en este punto está contenido en el artículo 21 de la Ley. La norma señala diversas clases de actividades y finalidades en las que procede lícitamente el tratamiento de datos personales.

En cuanto a las actividades, el precepto señala varias situaciones (recopilación de domicilios, venta…), con la particularidad de que se trata de una reseña a vía de ejemplo.

La citada reseña incluye la "prospección comercial", que no estaba prevista a texto expreso en el texto legal original. Si bien se trataba a todas luces de una actividad comprendida en el ámbito del mismo artículo (...publicidad, ... otras

---

[97] Sentencia del Juzgado Letrado en lo Penal de 20º Turno Nº 225 de 26 de agosto de 2009, en Anuario de Derecho Informático. Tomo X, 1era. Edición Año 2010. FCU, págs. 234 y sgtes.

[98] "Primer caso judicial en el país contra el envío de correo basura por Internet" en http://edant.clarin.com/diario/2003/11/21/s-04501.htm Página visitada el 14 de setiembre de 2010.

[99] FERNANDO MARGARZO, Ma. del Rosario. "La protección de datos personales en el ámbito de la publicidad en la legislación española", en Revista Chilena de Derecho Informático Nº 7, dic. 2005, Universidad de Chile, Facultad de Derecho, Centro de Estudios en Derecho Informático, pág. 97 y sgtes.

actividades análogas...), su inclusión había sido objeto de debate por parte de algunos administrados, por lo que motivó la reforma[100]. Es del caso apreciar que el art. 30 de la Ley 15/1999 española incluye este término a partir ya de su nomen iuris: "tratamientos con fines de publicidad y prospección comercial", revelando con ello la natural inserción y esencialidad de dicha modalidad.

Por lo que refiere a las finalidades permitidas, la nomenclatura empleada ya no es enunciativa sino taxativa: "fines promocionales, comerciales o publicitarios, o permitan establecer hábitos de consumo". Aquí aparece una puntuación en el texto legal, que puede causar alguna duda interpretativa. La misma es superable aplicando un criterio racional y sistemático para la debida comprensión del precepto. Concluimos por ello que la frase "cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento", se aplica no sólo al caso de "hábitos de consumo" (tal lo que se desprende de la existencia de un punto y coma precedente), sino al conjunto completo de hipótesis que expresa la norma, que incluye, además del señalado, los casos de "fines promocionales, comerciales o publicitarios". De lo contrario no tendría sentido considerar a estas últimas categorías como "datos especialmente protegidos", puesto que habrían desparecido los requisitos o virtualidades que justamente le dan esta fisonomía.

Es lo que surge, por otra parte, de una lectura racional, conteste con las fuentes de inspiración en las que se basara el legislador patrio: el artículo 30 de la Ley 15/999 española, y el artículo 27 de la Ley 25.326 argentina.

En síntesis, entran en esta categoría especial de datos, las cuatro clases de finalidades señaladas en la norma, a saber: promoción, comercio, publicidad, establecimiento de hábitos de consumo. Por su parte son tres los requisitos o condiciones, alternativos, que pone el legislador, a efectos de legitimar el registro y tratamiento de este tipo de datos: figurar en documentos de acceso público, o bien que hayan sido facilitados por el titular, o bien obtenidos con el consentimiento de éste.

Como se anunciara en apartado precedente, ingresa en este capítulo lo relativo a las actividades de spamming o, en versión breve que significa lo mismo, el spam.

Se trata de un tema que carece de regulación especial en nuestro derecho, en cuyo tratamiento y elucidación intervienen –no obstante y de todos modos- normativas de última generación, como son la Ley Nº 17.250 sobre Relaciones de Consumo, y la Ley Nº 18.331 sobre Protección de Datos Personales y Acción de Habeas Data.

Del juego armónico de ambos cuerpos normativos, y a falta de una regulación más especial, se deduce que el spamming o spam es, cuando menos, una actividad controlable y pasible de enjuiciamiento en nuestro derecho.

---

[100] Art. 21 de la Ley Nº 18.331, en su redacción actual dada por el art. 152 de la Ley Nº 18.719, de 27 de diciembre de 2010.

En lo que corresponde a nuestro ámbito, la URCDP ha tenido oportunidad de expresarse sosteniendo que "para que el tratamiento de datos personales por parte del responsable de una Base de Datos sea lícito, aún cuando la finalidad sea la de enviar comunicaciones comerciales o publicitarias por vía electrónica, se requiere, como regla general, el consentimiento del titular de los datos, el que deberá ser previo, expreso e informado, el que deberá documentarse, conforme lo prevé el artículo 9º de la Ley de Protección de Datos y Acción de Habeas Data Nº 18.331 (LPDP), de 11 de agosto de 2008. Tal disposición establece excepciones, las que no resultan aplicables en la especie".[101]

5.3. Relevancia particular de los derechos de acceso y retiro o bloqueo

El legislador previó la gratuidad del derecho de acceso como ya lo había hecho a título general en el artículo 14 de la Ley. Con la diferencia que este caso no puso condiciones, como sí lo hizo en el régimen general, a su ejercicio. Por lo tanto, y en función del criterio interpretativo consistente en hacer predominar la norma especial por sobre la general, se debe entender que el titular de un dato personal, incluido en una base de datos con fines de publicidad, puede ejercitar el acceso sin las limitaciones contenidas en el citado artículo 14, es decir sin tener que respetar el intervalo de seis meses, ni esperar a que se suscite un nuevo interés legítimo.

Como segundo aspecto a considerar, está el hecho de que el titular de los datos queda facultado, en este caso, a solicitar el retiro o bloqueo de sus datos, lo que no es un tema de importancia menor (de hecho es el único caso en la ley donde el titular dispone de un derecho absoluto sobre sus datos, sin restricciones temporales ni de otro tipo).

5.4. Casos de jurisprudencia

En apartado anterior se aludió a jurisprudencia sobre spam por lo que no se insistirá en este punto. Mencionaremos, en cambio y como muestra de otro tipo de contenciosos igualmente calificables en la especie, la Sentencia española de 18 de mayo de 2006 de la Audiencia Nacional. (Sala de lo Contencioso-Administrativo, sección primera), sobre tratamiento de datos, consentimiento inequívoco, fuentes de acceso público, y tratamientos con fines de publicidad y prospección comercial.[102]

6. DATOS RELATIVOS A LA ACTIVIDAD COMERCIAL O CREDITICIA

6.1. El concepto de "informes objetivos de carácter comercial"

Se trata de una expresión que carece de antecedentes en el derecho comparado, y que fue empleada por primera vez en la Ley Nº 17.838, predecesora de la actualmente en vigor.

---

[101] Resolución Nº 024/2009, de 9 de setiembre de 2009 del Consejo Ejecutivo de la URCDP.

[102] www.agendaactiva.es/Archivos/Descargas/ConsentimientoInequivoco.pdf Página visitada el 14 de setiembre de 2010.

El sentido natural de la frase indica que se trata de reportes cuya particularidad consiste en traducir informaciones asépticas, sin carga valorativa, es decir que no contengan expresiones de ningún tipo que califiquen directamente al sujeto de derecho al que refiere el informe, dejando este juicio o calificación en manos de quien recibe y utiliza el informe.

Como quiera que sea, la expresión, si bien adecuada, se ha entendido insuficiente en orden a prescribir con la técnica y precisión requeridos el correcto encuadre y las limitaciones de este tipo de tratamientos. Por este motivo se reformó el primer inciso del texto legal original[103]. No debe perderse de vista la naturaleza excepcional y restrictiva que informa todo este segmento, verdadero sub-sistema del sistema mayor al que pertenece ("datos especialmente protegidos" reza nuestra ley), con particularidades proteccionistas propias. La ley argentina refiere a "prestación de servicios de información sobre solvencia patrimonial y crédito" lo que en la fórmula originaria del derecho patrio no quedaba evidente, o pasaba a segundo plano, y fue necesario rescatarlo mediante la enunciada reforma[104].

De aquí en más expondremos en forma ordenada y sistemática el régimen vigente en este sector, que comporta varios elementos lógicamente enlazables entre sí.

6.2. Tipos y requisitos especiales para la obtención de los datos

En un terreno donde existe siempre la tentación, o mayor proclividad, de olvidar o soslayar la presencia del principio protector (la Ley Nº 18.331 curiosamente no lo menciona en el elenco de principios generales, pero nadie puede osar discutir su existencia y preeminencia en todo el sistema legal, con mayores o menores niveles de exigencia), no parece mala cosa recordar que si las empresas y otras entidades tratan hoy día con datos personales a fines comerciales o crediticios, es porque existe una norma legal que les autoriza a ello. Para el caso esta norma es el art. 22 de la Ley Nº 18.331, en su redacción actual dada por el art. 152 de la Ley Nº 18.719, de 27 de diciembre de 2010.

Esta autorización no es incondicionada y, por el contrario, contiene una serie de requisitos. Resulta importante, así, desentrañar con precisión el contenido de esta norma, apreciando los requisitos y límites de este tipo de tratamientos.

Es claro que al tenor del texto legal actual, en este rubro no se pueden tratar datos personales que no sean aquéllos "destinados a informar sobre la solvencia patrimonial o crediticia". A partir de la citada reforma legal no pueden caber dudas al respecto, si es que antes las había. Por lo que el requisito de "brindar informes objetivos de carácter comercial" se mantiene pero pierde la centralidad de que gozaba en la fórmula legal originaria. Es claro también, que estas primeras precisiones son acompañadas de una serie de requisitos anexos o complementarios, que funcionan como otras tantas restricciones a las

[103] Art. 22 de la Ley Nº 18.331, en su redacción actual dada por el art. 152 de la Ley Nº 18.719, de 27 de diciembre de 2010.
[104] Art. 26 de la Ley Nº 25.326, de 30 de octubre de 2000.

posibilidades de tratamiento, aumentando así el marco proteccionista en favor de los titulares de los datos.

Pero con ser importantes y básicos los dos puntos de partida antedichos, es dable apreciar que el legislador no se queda ni se contenta con ello, exhibiendo una minucia reglamentaria como en ninguna otra parte de la Ley, tal la importancia que le concede a esta zona de tratamientos.

Es así que, por un lado, amplía la caracterización de los datos personales susceptibles de ser tratados, manteniendo el hilo conductor indicado en el nomen iuris de la norma, especificando que podrán ser "aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos".

Pero luego también acota el origen permitido de estos datos personales: fuentes de acceso público, informaciones facilitadas por un acreedor, y circunstancias previstas en la presente ley. Solamente en estos tres casos, y nada más que en estos tres casos, el registro y tratamiento de datos personales relativos a actividad comercial o crediticia, tendrán la nota de legitimidad.

Todo lo que acaba de expresarse funciona para las personas físicas. Tratándose de personas jurídicas el régimen se flexibiliza, permitiendo el tratamiento de toda información producto de las circunstancias de la presente ley, o bien autorizada por la normativa vigente.

6.3. Registro de los datos. Plazos y obligaciones

El régimen de plazos y obligaciones es otra muestra de la especial atención que dedica el legislador a esta clase de registros y tratamientos.

La regla inicial es la del registro de los datos por un plazo no superior a los cinco años contados a partir de su incorporación a dicho registro. Esta regla tiene dos tipos de prórroga. La primera por otros cinco años cuando al vencer el primer plazo la obligación permaneciera incumplida. La segunda por un plazo máximo y no renovable de cinco años, con anotación expresa del hecho y destinado a obligaciones canceladas o extinguidas, plazo que computa a partir de la fecha de la cancelación o extinción.

Estos plazos no operan automáticamente, salvo uno de ellos. Desde luego que el plazo inicial de regla rige si alguien (un acreedor) incorporó la obligación incumplida al registro. Pero también debe haber pedidos expresos en los otros casos. Así el nuevo registro por permanecer incumplida la obligación, requiere que sea solicitado por el acreedor dentro de los treinta días anteriores al vencimiento original. En cambio la permanencia del registro de una obligación cancelada o extinguida, no requiere excitación externa alguna.

Existen otros plazos dispuestos por la norma, que son los siguientes: cinco días hábiles para que el acreedor comunique al responsable de la base de datos o

tratamiento correspondiente, la cancelación de la obligación incumplida registrada. Tres días hábiles para proceder a actualizar los datos y asentar la nueva situación de éstos.

6.4. Casos de jurisprudencia

Al contrario de otros terrenos o sectores abordados en el presente capítulo, en materia de datos comerciales y crediticios se constata un contencioso bastante nutrido.

En Uruguay, incluso antes de la vigencia de la Ley Nº 17.838, existía jurisprudencia sobre el tema, posiblemente sin emplear expresamente la categoría o institución jurídica "protección de los datos personales", impensada por aquel entonces en los ámbitos jurídicos nacionales, pero de todas formas resolviendo asuntos o tópicos propios a la materia, aunque fuere acudiendo a otro tipo de encuadres jurídicos.[105]

Durante la vigencia de la Ley Nº 17.838 y bajo la actual Ley Nº 18.331, los pronunciamientos judiciales se fueron multiplicando. A vía de ejemplo:

- Sentencia del Tribunal de lo Contencioso Administrativo Nº 445, de 20 de agosto de 2009, anulando acto administrativo que denegó el acceso a determinados datos incorporados al Sistema Central de Riesgos del Banco Central del Uruguay.[106]

- Sentencia del Juzgado Departamental de la Capital de 26º Turno Nº 17, de 4 de agosto de 2009, que resuelve sobre daño moral producido por inclusión errónea en base de datos del Banco Central del Uruguay.[107]

- Sentencias del Juzgado Letrado de Primera Instancia en lo Contencioso Administrativo de 2º Turno Nº 38, de 13 de agosto de 2009, y del Tribunal de Apelaciones en lo Civil de 5º Turno Nº 120, de 16 de octubre de 2009, por las que se resuelve acción de habeas data contra el Banco Central del Uruguay.[108]

- Sentencia del Juzgado Letrado de Primera Instancia en lo Civil de 17º Turno Nº 55, de 20 de octubre de 2009, sobre acción de protección de datos personales en el marco de la nueva Ley Nº 18.331.[109]

- Sentencia del Tribunal de Apelaciones en lo Civil de 7º Turno Nº 76, de 30 de abril de 2008 revocatoria de la sentencia del Juzgado Letrado en lo Civil de 6º Turno Nº 5, de 28 de febrero de 2007, que resuelve sobre inclusión en

---

[105] BAUZÁ REILLY, Marcelo. "Régimen jurisdiccional de protección de datos personales" en Anuario de Derecho Informático. Tomo VI, 1era. Edición Año 2006. FCU, págs. 169 y sgtes. Ver Nota 14 del artículo, que trata el punto.
[106] Anuario de Derecho Informático. Tomo X, 1era. Edición Año 2010. FCU, págs. 301.
[107] Anuario de Derecho Informático. Tomo X, 1era. Edición Año 2010. FCU, págs. 299.
[108] Anuario de Derecho Informático. Tomo X, 1era. Edición Año 2010. FCU, págs. 244 y sgtes., con Nota de MESSANO, Fabrizio. "Conflictividad relativa al proceso de habeas data".
[109] Anuario de Derecho Informático. Tomo IX, 1era. Edición Año 2009. FCU, págs. 244 y sgtes.

clearing de informes.[110]

7. CONCLUSIONES

Los “datos especialmente protegidos” son una categoría especial de datos personales, distinguible porque el legislador les ha adjudicado diversas notas regulatorias, destinadas a darles un nivel mayor de protección.

Esas notas suponen en todos los casos la presencia de restricciones más fuertes a la posibilidad de su registro y tratamiento, en beneficio de una protección de los titulares aumentada en términos comparativos con respecto a otro tipo de datos personales, procedentes o contenidos en el régimen ordinario.

Las aludidas restricciones (requisitos, prohibiciones, sujetos habilitados para recolectar y tratar los datos, etc.) varían según los casos.

En algunas subcategorías se impondrá la exigencia ineludible del consentimiento expreso y escrito del titular, o bien la existencia de razones de interés general autorizadas por ley, o mandato legal en favor de un organismo solicitante (datos sensibles).

A su vez operará una flexibilización de tales restricciones cuando se trata de las bases de sus asociados o miembros que lleven los partidos políticos y otro tipo de asociaciones, cuya comunicación a terceros de todos modos requerirá el consentimiento de los titulares.

En otros casos las limitantes vendrán por el lado del tipo de sujetos que pueden recolectar y tratar los datos, así como la pertenencia de éstos a cierta clase de titulares (datos de salud y datos de telecomunicaciones). Se agregan, también, otros requisitos relativos al respeto de ciertas normas y principios (datos de salud) así como el cumplimiento de medidas técnico-gestionales, y una obligación de alertar eventuales riesgos de seguridad (datos de telecomunicaciones).

Finalmente están los casos o especies donde se acotan de modo plausible las posibilidades de origen de los datos y se prioriza al máximo la potestad del titular en cuanto a recuperar sus datos (datos de publicidad), para llegar a un régimen puntilloso de registro, donde también se prevén determinados orígenes de los datos a tratar, y se agregan plazos escalonados a diversos efectos y exigencias (datos comerciales o crediticios).

Estamos de esta suerte en presencia de normas de carácter excepcional, que por naturaleza propia hacen mayor énfasis aún que el resto del articulado legal, a favor del derecho de los titulares de los datos, limitando y poniendo restricciones de distinto tenor al registro y tratamiento de este tipo de datos personales. En tal sentido, se trata de un cuerpo o segmento dentro de la ley, que funciona como norma especial. Como tal, está destinado a actuar en

[110] Anuario de Derecho Informático. Tomo IX, 1era. Edición Año 2009. FCU, págs. 299.

armonía, pero en ciertos casos imponerse, respecto del cuerpo general u ordinario regulado en el resto del articulado legal. Es éste un aspecto que no cabe perder de vista, y que determina que todo lo que se interprete y resuelva en materia de “datos especialmente protegidos” deba practicarse a la luz no solamente de los principios generales consagrados en los artículos 5º a 12 de la Ley sino, además, bajo un criterio de mayor miramiento o predominio de los derechos de los titulares de los datos, en relación a derechos y facultades de quienes hacen la recolección y el tratamiento de tales datos.

CAPÍTULO VII – LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN LA LEY Nº 18.331

Dr. Federico Carnikian Brignoni

1. INTRODUCCIÓN

La realidad indica, que en la actualidad la transmisión y el entrecruzamiento de información por y entre los particulares, las empresas y Organismos estatales, es necesaria y fundamental para el cumplimiento de un sin fin de objetivos de muy variada índole.

En este sentido, se vuelve necesario regular de forma apropiada, la forma de proteger los datos personales que se transfieren y se re-transfieren a distintos países a efectos de salvaguardar los derechos que sobre estos datos tienen los titulares.

Es por ello, que los regímenes legales en materia de protección de datos, contemplan un conjunto de normas tendientes a regular las transferencias internacionales de datos personales -TIDP-.

El presente capítulo tiene como objeto fundamental, proporcionar una visión general del régimen de las TIDP desde la perspectiva del ordenamiento jurídico uruguayo.

Asimismo, se hará un breve análisis referente a la viabilidad de contar con un instrumento normativo de carácter regional en la materia.

2. ANÁLISIS DE LA SITUACIÓN URUGUAYA

El tema objeto de análisis ha sido bastamente estudiado por la doctrina internacional, fundamentalmente en el derecho continental, donde la normativa relativa a la protección de los datos personales ha tenido mayor desarrollo.

A continuación, se hará reseña a los aspectos teóricos que se consideran más relevantes de acuerdo con la actual situación de nuestro país, tomando algunas referencias de la experiencia comunitaria en el tema.

2.1. Concepto de TIDP y sus variantes

No todas las normativas que regulan el derecho a la protección de datos e instrumentos conexos, contienen una definición de transferencias internacionales. Por lo que, resulta acertado que el legislador uruguayo haya optado, no solo por definir este concepto de tanta importancia en un régimen legal y reglamentario que tiene vocación de extraterritorialidad, sino también de aportar otras definiciones que permiten interpretar la norma de acuerdo con los principios que imperan en la materia y los conceptos más importantes para su debida comprensión y análisis.

La normativa uruguaya define a las TIDP en el Decreto Nº 414/009 de 31 de agosto de 2009, que reglamenta con carácter general la Ley Nº 18.331, de 11 de agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data –en adelante Ley Nº 18.331-.

Asimismo, dicha normativa, define en sentido amplio los sujetos intervinientes en toda transferencia de datos, esto es el Exportador de datos o transmitente de la información y el Importador de datos o destinatario de los datos personales, siguiendo la tendencia internacional al respecto (art. 4º lit. E) y F) Decreto Nº 414/009 respectivamente).

La normativa señalada define al exportador de datos como: "la persona física o jurídica pública o privada, situada en territorio uruguayo que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a otro país" - literal E) del artículo 4º del Decreto Nº 414/009, de 31 de agosto de 2009 -.

Por su parte, el importador de datos es toda: "persona física o jurídica, pública o privada, receptora de los datos de otro país, en caso de transferencia internacional de éstos, ya sea responsable del tratamiento, encargada del tratamiento o tercero"-literal F) del artículo precitado-.

En cuanto a la definición de TIDP, el literal H) del artículo señalado la define como: "tratamientos de datos que supone una transmisión de éstos fuera del territorio nacional, constituyendo una cesión o comunicación, y teniendo por objeto la realización de un tratamiento por cuenta del responsable de la base de datos o tratamiento establecido en territorio uruguayo".

Por consiguiente, la circunstancia de transferir datos no siempre constituye una TIDP, sino que para ello es necesario que existan acumulativamente los siguientes elementos.

En primer lugar, debe haber una transferencia de datos personales. Tomando el criterio a mi juicio acertado de Miguel Ángel Davara Rodriguez[111] reseñado supra, no alcanza con que exista un flujo de información, sino que es necesario que exista una transferencia de información que contenga datos personales fuera del territorio uruguayo.

En segundo lugar, esa transferencia debe implicar necesariamente un tratamiento de datos personales por parte del responsable, pudiendo para ello realizar cualquiera de las acciones contempladas en el concepto de tratamiento de datos (literal M) del art. 4º de la Ley Nº 18.331).

En tercer lugar, y como veremos a continuación al señalar los distintos tipos de TIDP que recoge nuestro ordenamiento positivo, las transferencias no necesariamente significan una comunicación de datos, por lo que no sería acertado jurídicamente decir que las TIDP son comunicaciones de datos cuyo destinatario se encuentra en otro país.

[111] DAVARA RODRIGUEZ, Miguel Ángel. "La Transferencia Internacional de Datos". Revista Española de Protección de Datos. Julio – diciembre, 2006. Página. 23.

Haciendo referencia a los distintos tipos de TIDP que recoge la normativa uruguaya, se mantiene la posición sostenida[112] en cuanto a que existen dos tipos de transferencias claramente diferenciadas.

Pero antes de concentrarnos en las características que cada una de ellas posee, nos parece relevante realizar algunas precisiones que tienen que ver con las diferencias que tiene el régimen de TIDP con el establecido para las comunicaciones de datos y las características generales que posee el tratamiento de la información desde la visión del titular del dato.

Cuando estamos ante una típica cesión o comunicación de datos personales, existen dos partes involucradas, esto es, un emisor y un receptor o destinatario de la información.

Los distintos regímenes relativos a la protección de los datos personales, contienen preceptos dedicados exclusivamente a la protección de los derechos de los titulares de los datos en casos de cesiones o comunicaciones, constituyéndose en un derecho del titular del dato.

La razón de esta especial tutela, radica en que ante una eventual comunicación, y en el caso de no dar cumplimiento de ciertas condiciones legales, dichas cesiones estarán contrariando los principios generales de protección de datos personales.

En este sentido y siguiendo al autor reseñado, siempre que se trate de un tratamiento de información, se estará en presencia de al menos tres etapas o fases del procesamiento de datos[113].

Una primer etapa de recolección de los datos, donde el titular tiene total control de la información; una segunda fase de tratamiento de esa información y su utilización para los fines para los cuales fueron recogidos, donde si bien el control no es absoluto, el tratamiento se encuentra limitado por los principios reinantes en la materia, en especial los principios de legalidad, finalidad, veracidad de los datos, etc; y una tercera etapa constituida por una eventual comunicación o cesión de los datos.

Es en este último caso donde para dar cumplimiento a la normativa de protección de datos, el emisor de la información deberá: a) obtener el consentimiento del interesado; b) informar al titular la finalidad de la comunicación; c) proporcionar la información relacionada con él o los destinatarios de los datos a efectos de su identificación.

---

[112] CARNIKIAN BRIGNONI, Federico. “Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos. Seminario de la Red Iberoamericana de Protección de Datos (RIPD). Montevideo, 1-4 de junio de 2010. Página 5 y sgtes.

[113] DAVARA RODRIGUEZ, Miguel Ángel. Ob. Cit., pág. 24.

Asimismo, la comunicación de datos sólo será legítima cuando sea efectuada en virtud de un interés legítimo para el cumplimiento de los fines del emisor y receptor de los datos -artículo 17 de la LPDP-.

En este sentido, las previsiones concernientes a proteger a los interesados en este tipo de situaciones son en razón a que el titular es vulnerable de perder de forma casi total el control de su información, trayendo consigo un tratamiento desleal e ilegítimo.

Las mismas fases de tratamiento se dan en supuestos de transferencias internacionales realizadas por un Responsable a otro Responsable, recolección, tratamiento y posterior transmisión de los datos dentro los parámetros ya señalados.

a) TIDP de Responsable de la base de datos o tratamiento a Responsable (R1 a R2)

Para ejemplificar este tipo de TIDP, podemos dividir su análisis, en tres elementos sustanciales.

1) constituyen necesariamente una comunicación de datos: en estos casos el Responsable –exportador de datos- instalado en nuestro país, recolecta, trata y comunica los datos personales a otro Responsable –importador de datos- situado en el extranjero, para que este realice tratamiento sobre la información.

Por tanto, se deberá dar cumplimiento también a los mismos requisitos exigidos para que una cesión de datos sea con arreglo a derecho -principio del previo consentimiento informado del titular de los datos, informar al titular acerca de la finalidad y las consecuencias que tiene transferir esa información, identificación del destinatario, y que las cesiones tengan como objeto el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario de los datos-.

2) existencia de dos bases de datos personales: la información contenida en una base de datos sometida al tratamiento por parte de un Responsable situado en Uruguay, es transmitida a otra base de datos perteneciente a otro Responsable a efectos de su posterior o mejor dicho, nuevo tratamiento de información.

3) transferencia del riesgo en el tratamiento: al tratarse de una comunicación de datos, estamos en presencia de dos Responsables, que como tales, son propietarios de las bases de datos que poseen y deciden sobre el uso, contenido y finalidad para la cual tratan esos datos. Por lo que es lógico pensar, que cuando hay una transferencia de R1 a R2 y por tanto una comunicación de datos, el destinatario de la información (importador de datos), tiene la libertad de tratar la información recibida de acuerdo con los objetivos que éste persiga.

Conforme a ello, se podría afirmar que, el riesgo en el tratamiento se traslada, siendo cada uno responsable frente al titular del dato.

A modo de reflexión decimos que el concepto de transferencia subyace al de comunicación de datos, en virtud de que las transferencias pueden constituir o no una cesión de datos personales.

Por ejemplo, un Responsable del tratamiento trasmite los datos pertenecientes a los empleados de su empresa, a la empresa matriz que centraliza la gestión de recursos humanos, decidiendo este último sobre su finalidad contenido y uso del tratamiento[114]. En este caso, el receptor de los datos –como Responsable del tratamiento- realiza un posterior o nuevo tratamiento de los datos, decidiendo sobre la utilización y objeto que le dará a éstos.

b) TIDP de Responsable de la base de datos o del tratamiento a Encargado del tratamiento (R1 a E1)

En los supuestos donde un Responsable trasmite datos personales a un Encargado de tratamiento, situado en otro Estado con el objeto de que éste preste un servicio, no estamos ante una comunicación de datos propiamente dicha.

La Ley Nº 18.331, permite que un Responsable contrate con un sujeto para que éste realice determinadas tareas relacionadas con el tratamiento de la información que son establecidas previamente por el Responsable, tal como dice la Ley, el encargado trata los datos por cuenta de aquél.

Este tipo de TIDP se diferencia de las anteriores en los siguientes puntos.

1) no existe comunicación de datos: en estos supuestos el Encargado de tratamiento solamente accede a la base de datos perteneciente al Responsable y ejecuta las tareas encomendadas bajo la dirección e instrucciones de éste.

2) existencia de una sola base de datos: esto es debido a que existe acceso por parte del Encargado del tratamiento a la base de datos del Responsable, no existe otra base de datos. Además, el Encargado no tiene potestad alguna para decidir sobre la finalidad, contenido y uso del tratamiento, limitándose a ejecutar los servicios que fueron acordados previamente con el Responsable.

3) no existe traslado del riesgo en el tratamiento: al haber un acceso a la base de datos del Responsable, éste es quien toma las decisiones, siendo el único responsable frente a la autoridad de control y el titular del dato.

Existen varias normativas, que excluyen expresamente estas situaciones del concepto de comunicación de datos. A vía de ejemplo, tenemos el artículo 14 del Decreto Nº 414/009 de 31 de agosto de 2009.

Tomando como referencia el ejemplo planteado acerca de los datos de recursos humanos, puede suceder que exista un Encargado del tratamiento que trate los datos por cuenta del Responsable, siendo éste el que decide

[114] CEDDET. Ob. Cit. Módulo 3, pág. 81.

cuándo se pagan los salarios, se fijan las fechas de licencia, entre otros ejemplos.

Otra prestación típica de servicios por parte de un Encargado de tratamiento podría ser el servicio de telemarketing o atención al cliente, donde éste trata la información en virtud de las directivas acordadas con el Responsable.

Aquí podemos decir que el riesgo del tratamiento, es mantenida por el Responsable.

Es preciso señalar, que se debe tomar en consideración que la realidad empresaria demuestra que las empresas destinatarias de la información contratan otros Encargados de tratamiento para la prestación de un servicio determinado. Por tanto, se deberá estar ante el caso concreto para estar en condiciones de decidir qué modalidad de TIDP se ejecuta y la responsabilidad que le será imputable a los sujetos involucrados.

Por último es importante señalar, que el Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales (URCDP), se pronunció por Dictamen Nº 8 de 19 de marzo de 2010, resolviendo que: ”en virtud de lo establecido por los literales E), F) y H) del artículo 4º del Decreto reglamentario, se considera que las transferencias internacionales reguladas por la normativa nacional vigente de protección de datos personales, son las que constituyen una cesión o comunicación de datos strictu sensu, esto es, de Responsable a Responsable de la base de datos, como las que tengan por objeto la realización de un tratamiento por cuenta del responsable de la base de datos, esto es, de Responsable a Encargado del tratamiento”.

2.2. Regulación de las TIDP en el ámbito del MERCOSUR

Como punto de partida se expresa que la regulación europea relativa a la transferencia de datos personales entre los Estados, descansa en dos pilares fundamentales.

El primero de ellos, establece que la libre circulación de datos, -considerado como un presupuesto clave para el comercio entre Estados-, no debe estar sometida a la necesidad de autorización de éstos como forma de dotar de fluidez al sistema de intercambio de productos, bienes, servicios y el tránsito de personas.

En segundo lugar, las transmisiones de datos personales dentro del territorio comunitario, no son consideradas como transferencias de datos, sino como simples comunicaciones de datos personales y como tales, sometidas al régimen dispuesto en cada país al efecto.

Por su parte, el MERCOSUR, cuenta con una estructura orgánica compuesta por diversos organismos con sus competencias asignadas a través del Tratado de Asunción y el Protocolo de Ouro Preto.

Dado que existen diferencias sustanciales desde el punto de vista político y jurídico – positivo, con relación a la estructura comunitaria y la del MERCOSUR, se deja abierta la discusión jurídica en cuanto a la viabilidad de contar con un instrumento normativo de nivel regional, que contemple los principales aspectos relativos a la protección de datos personales. Para ello, se debería tomar en consideración que en la actualidad, dos de los países integrantes del Grupo no poseen una ley general en la materia.

Dentro de los aspectos generales a regular se podrían contemplar los relacionados con, los principios generales en la materia, los derechos del titular de los datos y los mecanismos administrativos y jurisdiccionales adecuados para efectivizar el ejercicio de éstos. Asimismo, se considera relevante regular un conjunto de normas relacionadas con las TIDP, que abarquen aspectos tales como, la procedencia del régimen de autorización, las obligaciones del Exportador e Importador de datos, la forma de ejercicio de los derechos cuando existe transferencia de los datos, las medidas de seguridad sobre estos datos, entre otros.

2.3. Cláusulas contractuales tipo y Reglas Corporativas Vinculantes en el sistema uruguayo

En la actualidad y como consecuencia de la sociedad de la información donde vivimos, el comercio electrónico se ha convertido, y así lo seguirá siendo, en uno de los ejes de la economía mundial.

En este sentido, es necesario brindar garantías adecuadas para los consumidores de productos y servicios en cuanto a la fiabilidad de éstos, la correcta identificación de las partes contratantes, y garantías que tutelen los intereses del titular del dato, a través de procedimientos garantistas y acordes con la normativa de protección de datos, fundamentalmente en lo relativo al intercambio de información personal entre los distintos involucrados en las relaciones contractuales situados en distintas partes del mundo.

Al igual que sucede en el sistema comunitario, la ley uruguaya previó que a efectos de realizar TIDP a países que a su juicio no cuenten con un nivel adecuado de protección, los Responsables de bases de datos o del tratamiento, podrán concertar cláusulas contractuales a efectos de someterlas a la autoridad de control para su posterior análisis y aprobación.

En principio, existe autonomía de las partes para determinar el contenido de las mencionadas cláusulas, sin embargo, podríamos decir que dicha autonomía de la voluntad no es ilimitada, sino que debe tomar en cuenta algunos aspectos.

Las cláusulas contractuales tipo o cláusulas contractuales apropiadas como las denomina la Ley Nº 18.331, deben ofrecer restrictivamente garantías suficientes para el respeto de la vida privada, los derechos y deberes fundamentales de las personas, y el respeto en el ejercicio de los derechos.

Asimismo y si bien las partes pueden incluir otras cláusulas relacionadas directa o indirectamente con la ejecución del servicio, éstas deben respetar y

estar en plena concordancia con las cláusulas contractuales apropiadas las cuales se refieren explícitamente al tratamiento de los datos personales [115].

En esta línea de razonamiento, las cláusulas contractuales tipo son una de las diversas posibilidades que cuentan los Responsables de bases de datos para poder realizar TIDP a países que no cuenten con una protección adecuada y se considera que aparecen de acuerdo con los usos y costumbres en nuestro derecho, como una solución acorde que resta complejidad y permite brindar garantías tanto a los titulares como a las propias partes concertantes a efectos de poder concretar sus negocios. En este sentido se ha pronunciado la URCDP[116].

En estos supuestos, los intereses comerciales entre las partes –que en alguna oportunidad podrían también comprender intereses de los propios titulares- pueden verse retazados por los derechos del titular del dato en cuanto al deber de cumplimiento de los presupuestos en materia de protección de su privacidad.

Es por ello, que las autoridades de control en la materia a la hora de analizar la procedencia de la autorización para transferir datos personales, así como también las cláusulas contractuales pactadas, deberán estar al caso concreto, tomando en consideración para su decisión en todas las situaciones, los criterios de ponderación y balance de origen doctrinario y jurisprudencial.

En consecuencia, el análisis de las cláusulas contractuales apropiadas por parte de las autoridades de control, no sólo consta de un procedimiento administrativo, sino se vuelve necesario un estudio caso a caso con el objetivo de lograr un equilibrio entre los derechos en juego.

Relacionado con el juego de los intereses comerciales y los que refieren al titular del dato, podríamos decir que la visión proteccionista del titular en las leyes de protección de datos personales, es acorde a la visión que se le da a las normas relacionadas con la protección del consumidor, en tanto, el consumidor es además titular de datos personales, y como tal, la parte más débil en la relación comercial o contractual con los proveedores de bienes y servicios.

Por lo que las cláusulas contractuales tipo a las que refiere la normativa de protección de datos, deberían estar en armonía con las disposiciones en temas de relaciones de consumo y tutela del consumidor, lo que coadyuvaría a la protección de los titulares de los datos, ante los intereses comerciales empresariales a la hora de desarrollar y promocionar sus productos.

Por otro lado y con referencia a las Reglas Corporativas vinculantes o Binding Corporate Rules, el Grupo del artículo 29 (creado por el artículo 29 de la

---

[115] CEDDET. Ob. Cit. Módulo 3, pág. 87.

[116] Dictamen Nº 8/009, de 19 de marzo de 2010. Disponible en http://www.datospersonales.gub.uy/sitio/dictamenes.aspx. Página visitada el 18 de setiembre de 2010.

Directiva Europea 95/46/CE), las define[117] como: “un cuerpo de reglas o normas vinculantes adoptadas en el seno de un grupo de empresas que operan a nivel internacional, para regir las transferencias de datos que se producen desde las sedes del grupo establecidas en el Espacio Económico Europeo hacia otras sedes del grupo establecidas en terceros Estados”.

Desde hace varios años las estructuras empresariales se han venido modificando y adecuando su funcionamiento a las nuevas tecnologías y formas negociales. En tal sentido, es cada vez más usual la existencia de empresas tercerizadas o subcontratadas para la prestación de servicios concertados específicamente para una finalidad determinada.

En efecto, las empresas multinacionales desempeñan a través de filiales, sucursales u otras estructuras societarias sus negocios. Conforme a ello, es necesario que el régimen de las TIDP se adecue a las características que estos grupos presentan tutelando los intereses de los titulares de los datos. Además, este tipo de reglas posee la ventaja de uniformizar los criterios en cuanto al tratamiento de datos, beneficiando a las empresas para que éstas no realicen acuerdos inter partes cada vez que necesiten transferir información.

En referencia a la ejecución de TIDP entre filiales o sucursales de distintos países, el marco normativo general para éstas se encuentra dado por el inciso segundo del artículo 35 del Decreto Nº 414/009 que establece que se podrán efectuar TIDP en empresas multinacionales siempre y cuando se posean códigos de conducta debidamente inscriptos.

En efecto, se interpreta que los códigos de conducta a los que refiere la norma, son códigos que contienen normas relativas expresamente a las TIDP entre las empresas, y que para su debida autorización deben cumplir con los mismos requisitos que las cláusulas contractuales tipo -Considerando Nº X, del dictamen Nº 8/009 referido-.

Se considera en definitiva, que de acuerdo con una interpretación sistemática de la normativa uruguaya, las reglas corporativas vinculantes son códigos de conducta, que contienen un conjunto de reglas adaptadas específicamente para facilitar la realización de TIDP, dentro de un grupo de empresas multinacionales, de acuerdo con su fisonomía y estructura.

En cuanto al ámbito de aplicación y sin entrar detalladamente en este aspecto, podemos decir que, sería necesario para que opere la normativa uruguaya de protección de datos personales que estos códigos de conducta se concerten entre empresas multinacionales o formatos empresariales de similar calibre, que su casa matriz o sucursal se encuentre situada en nuestro país y éstas transfieran datos personales a otros miembros del grupo empresarial, establecidos en países que la URCDP considera que no brindan un nivel adecuado de protección.

---

[117] WP 108 de 14 de abril de 2005; WP 107 de 14 de abril de 2005; WP 74 de 3 de junio de 2003; WP 102 de 25 de noviembre de 2004; WP 107 de 14 de abril de 2005; ; WP 108 de 14 de abril de 2005; WP 133 de 10 de enero de 2007. Disponibles en www.europa.eu.int/comm/privacy. Página visitada el 18 de setiembre de 2010.

Por último, y en relación con el contenido de las reglas corporativas vinculantes, sería muy similar al de las cláusulas contractuales apropiadas, con el agregado de contener cláusulas de obligatoriedad interna y externa a cumplir por las empresas integrantes del grupo multinacional[118].

2.4. Reflexiones acerca del procedimiento de autorización y sus excepciones

La normativa uruguaya de protección de datos, tomó como inspiración el sistema comunitario, fundamentalmente la normativa española, así como también la normativa Argentina.

Conforme a ello y de una primera reflexión al efecto, podemos decir que razones de uniformización normativa, garantías y protección efectiva a los titulares, así como sistemas de autorización de TIDP similares –entre otras- justifican tal medida.

Una regulación coherente y sistemática del procedimiento de autorización de TIDP, significa un análisis en profundidad, no sólo de la normativa de protección de datos, sino también del ordenamiento jurídico vigente, considerando las estructuras y características que las transferencias presentan en el comercio internacional en el cual nuestro país esta inserto.

De acuerdo con lo mencionado, el procedimiento de autorización aprobado por la URCDP[119], sienta las bases de los elementos señalados tomando en cuenta la realidad empresaria actual, tal como así lo dispone el Considerando Nº IX del dictamen Nº 8 ya referido.

En cuanto a los aspectos de procedimiento y procedencia, se destaca que el procedimiento de autorización opera cuando el país destinatario de la información es considerado por la URCDP[120] como un país que no brinda un nivel adecuado de protección, o cuando la TIDP no se encuentre comprendida dentro de las excepciones previstas en el artículo 23 de la Ley Nº 18.331.

En cuanto a las excepciones, se considera que éstas deben ser de interpretación y aplicación restrictiva, y sometidas al contralor de la URCDP, la que posee competencias legales adecuadas para verificar su cumplimiento.

Es en este punto, donde la normativa uruguaya, se apartó levemente de las fuentes legislativas de las cuales tomó referencia e inspiración, regulando un

---

[118] SANCHO VILLA, Diana. "Protección de Datos Personales y Transferencia Internacional: cuestiones de ley aplicable", en Revista Jurídica de Castilla y León Nº 16. España, 2006, página 57.

[119] Dictamen Nº 8/009, de 19 de marzo de 2010 (Considerando Nº VI) http://www.datospersonales.gub.uy/sitio/dictamenes.aspx. Página visitada el 19 de setiembre de 2010.

[120] Resolución Nº 17/009, de 12 de junio de 2009. http://www.datospersonales.gub.uy/sitio/resoluciones.aspx. Página visitada el 19 de setiembre de 2010.

cuerpo de excepciones no comprendidas en otros sistemas normativos de protección de datos.

Sin embargo, a título personal se expresa que el criterio del legislador fue acertado, debido a que la inclusión de dichas excepciones atiende a razones fundamentales derivadas de otros derechos existentes en nuestro ordenamiento jurídico.

La normativa de protección de datos -al igual que las restantes dictadas en un Estado de Derecho -debe guardar relación sistemática y armónica con todo el sistema normativo, considerando las características que éste posee, así como también su tradición en materia de suscripción de tratados internacionales.

Asimismo, las excepciones previstas en la Ley Nº 18.331 se encuentran reguladas de forma detallada y atendiendo a otros bienes jurídicos susceptibles de ser protegidos, tales como la salud de base también constitucional.

Por consiguiente, la regulación de las excepciones que realiza la Ley Nº 18.331, responde a la consideración de otros derechos en juego consagrados a nivel legal y constitucional.

Por otro lado, se agrega que la URCDP tiene potestades para en cualquier momento suspender la realización de una, o una serie de TIDP, cuando no se cumplan los requisitos evaluados para otorgar su autorización u exista incumplimiento de algunas de las disposiciones legales o reglamentarias aplicables.

3. CONCLUSIONES

El régimen jurídico de las TIDP, revista de una complejidad que condice con el carácter internacional que las concierne, por lo que su estudio debe contemplar una multiplicidad de aspectos que deben apuntar hacia la salvaguarda de los intereses en juego, atendiendo su análisis caso a caso tomando en cuenta para ello los criterios de balance y ponderación de derechos.

Asimismo, no se debería perder de vista que su adecuada regulación, es importante para evaluar el nivel de protección que un país posee, atento al control que las autoridades en la materia efectúan sobre los datos que trascienden desde sus fronteras hacia el resto del mundo.

CAPÍTULO VIII - PRINCIPIOS DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

Dra. Laura Nahabetián Brunet

1. INTRODUCCIÓN

La información implica la elaboración de un juicio de ser, esto es, el desarrollo de un hecho probable; ésta incluye de por sí tanto la emisión como la recepción.

A nivel doctrinal comparado se verifica la existencia de varias dimensiones del derecho de la información y se construyen a su vez, diversas teorías acerca de la información.

En este sentido, se ha establecido que el derecho de la información incluye el derecho a recibirla, la libertad de expresión, la libertad de recibir comunicaciones e incluso ubicarlas, el derecho de acceso a la información y la libertad de su difusión.

Se comprende entonces que se considere a la información en tanto bien jurídico autónomo, a partir de lo cual se verificarán regulaciones diferentes dependiendo de las dimensiones señalas en su vínculo, verificándose así la existencia de información de carácter social, de carácter privado o de carácter público, así como consideraciones diferentes de acuerdo con el contenido de ésta.

Asimismo, el derecho de la información no debe confundirse con el derecho a la información.

Esta última, parte de la consideración en aplicación de criterios de tipo politológico de la información en cuanto poder. A partir de esta afirmación es que se comprende que en muchos casos se proceda al retaceo de información a quienes deben tomar decisiones en mérito a su derecho y necesidad de participación. Sin embargo, éstas estarán viciadas por la manipulación del engaño, en muchas oportunidades.

Por lo tanto no debe confundirse con la opinión.

En efecto, la libertad de opinión implica la trasmisión de creencias y valores, el desarrollo de juicios subjetivos que no determinan de manera alguna la afirmación de datos de carácter objetivo o la afirmación de hechos, siendo tal vez, su límite, la relevancia pública que éstos pudieren tener, por lo que posee un margen de acción mayor que la libertad de información. Esta última tiene ínsita la obligación de verdad, que funciona a su vez como límite del derecho.

“La libertad de información comprende el derecho a investigar y acceder a las fuentes de información, a transmitir la información de cualquier forma y a través

de cualquier medio, sin censura ni restricciones preventivas y el derecho a recibir, seleccionar y rectificar las informaciones difundidas, debiendo el Estado, sus agentes y órganos respetar tales derechos, garantizarlos, como asimismo, promoverlos, contribuyendo al desarrollo del pluralismo informativo, previniendo la existencia de censuras directas o indirectas, administrando con transparencia, racionalidad y justicia el acceso a las frecuencias radioeléctricas, impidiendo la existencia de monopolios u oligopolios respecto de los medios o insumos necesarios para producir la información escrita, por cable o de cualquier otro modo o medio, como por último impidiendo la constitución de monopolios públicos o privados."[121]

La libertad de información tiene en su esencia la libertad de recibir, comunicar, difundir, publicar información así como acceso liberado a todas las fuentes de información, sin la cual no sería posible su ejercicio pleno.

"El derecho a la información, tiene por objeto la integridad moral del ser humano. Es una libertad democrática que tiene por destino permitir una participación adecuada, autónoma e igualitaria de los individuos en la esfera pública. El derecho a la información se encuentra fuertemente relacionado con la libertad de opinión y expresión, que por un lado implican una neutralidad por parte de los otros y por el otro, la libertad de expresión aparece como condición del uso público de la razón."[122]

En línea con lo establecido la Corte Europea de Derechos Humanos en una lenta evolución jurisprudencial ha avanzado en la consideración de este derecho y en la concreción de los principios y fundamentos que éste implica. Establece: "la libertad de expresión constituye uno de los cimientos esenciales de esa sociedad, una de las condiciones básicas para su progreso y para el desarrollo de todos los hombres. Sujeta a restricciones legítimas es aplicable no sólo a la "información" o a las "ideas" que son recibidas favorablemente o consideradas inofensivas o indiferentes, sino también a aquéllas que ofenden, chocan o perturban al Estado o a algún segmento de la población. Esas son las exigencias del pluralismo, la tolerancia, la apertura mental, sin lo cual no existe una "sociedad democrática". Ello significa, entre otras cosas, que toda "formalidad", "condición", "restricción" o "sanción" que se imponga en esta esfera debe estar en proporción al objetivo legítimo que se persigue."[123]

2. IMPORTANCIA DE LOS PRINCIPIOS EN MATERIA DE ACCESO A LA INFORMACIÓN PÚBLICA

Los principios en general no necesariamente deberán estar establecidos en forma expresa, en la medida que se trata de determinaciones jurídicas que son aceptadas e incorporadas de forma tal que se constituyen en verdaderos pilares de los ordenamientos jurídicos.

---

[121] NOGUEIRA ALCALA, Humberto.- El derecho a la libertad de opinión e información. Chile, 2008.
[122] FONDEVILLA, Gustavo.- El derecho a la información y los límites del derecho a la intimidad. Buenos Aires, 2005.
[123] CORTE EUROPEA DE DERECHOS HUMANOS.- Caso de Handyside vs Reino Unido. Sentencia de 7 de diciembre de 1976.

En esta línea, el Prof. Alberto Ramón Real, ha establecido que: “en todo sistema jurídico hay cantidad de reglas de gran generalidad, verdaderamente fundamentales, en el sentido de que a ellas pueden vincularse, de un modo directo o indirecto, una serie de soluciones expresas del Derecho positivo a la vez que pueden resolverse, mediante su aplicación, casos no previstos, que dichas normas regulan implícitamente”.[124]

En este sentido, el Prof. Carlos Delpiazzo ha señalado por su parte: “Se trata de verdaderos cimientos que cumplen la triple función de servir como criterio de interpretación de las normas escritas, de colmar las lagunas o vacíos normativos y de constituir el único medio de asegurar el mínimo de unidad al sistema normativo.”[125]

A mayor abundamiento, el Prof. Delpiazzo indica que: “Si en todos los campos del Derecho el papel de los principios generales de Derecho es trascendente, ello es especialmente cierto en el ámbito de un Derecho novedoso, con vocación de universalidad y en formación requerido de piezas arquitecturales del ordenamiento, cuya manifestación se verifica fundamentalmente a través de la práctica aplicativa del Derecho y del desarrollo de la ciencia jurídica, lo que conduce asimismo a revalorizar en la especie a la jurisprudencia y a la doctrina como fuentes relevantes del Derecho.”[126]

Dar garantía efectiva y concretar el ejercicio de este derecho fundamental, implica concretar en toda la normativa sobre acceso a la información pública, principios y criterios que vayan determinando los diferentes condicionamientos para su utilización.

Se trata de elementos que integran el contenido esencial del derecho de acceso a la información pública y por tanto su vulneración ocasionará la violación a estas normas. Por otra, es a su vez fundamental dejar establecido, que toda la secuencia de principios que informan a este derecho, no serían más que una declaración de intenciones si no fueran posibles de ser concretados a través del ejercicio de los derechos que todas las personas tienen posibilitado.

Así la Corte Interamericana de Derecho Humanos establecerá una serie de directrices fundamentales para la consolidación del derecho de acceso a la información pública, en aplicación de una interesante interpretación del artículo 13 de la Convención Americana:

- Que el artículo 13 de la Convención, al estipular expresamente los derechos a “buscar y a recibir informaciones,” protege el derecho de toda

[124] REAL, Alberto.- Los principios generales de Derecho en la Constitución uruguaya. Montevideo, 1965.
[125] DELPIAZZO, Carlos.- Regulación de Internet. Adecuación del Derecho uruguayo a los requerimientos de las nuevas tecnologías de la información en Anuario de Derecho Informático. Tomo I. 1era. Edición Año 2001. Montevideo, 2001.
[126] DELPIAZZO, Carlos.- “El derecho ante las telecomunicaciones, la informática e internet”, en Anuario de Derecho Informático Tomo III. 1era. Edición Año 2003. Montevideo, 2003.

persona a acceder a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención.

- Que el actuar del Estado se debe regir por los principios de publicidad y transparencia y el principio de máxima divulgación – este último que establece una presunción de que toda información es accesible, excepto cuando esté sujeta a un sistema restringido de excepciones.

- Que el silencio no puede ser una respuesta ante una solicitud de información.

- Que dicho derecho tiene como contrapartida obligaciones positivas por parte del Estado.

- Que el Estado debe suprimir tanto de las normas como de las prácticas de cualquier naturaleza que entrañen violaciones a las garantías previstas en la Convención, así como la expedición de normas y el desarrollo de prácticas conducentes a la efectiva observancia de dichas garantías.

- Que el Estado debe garantizar la efectividad de un procedimiento administrativo adecuado para la tramitación y resolución de las solicitudes de información, que fije plazos para resolver y entregar la información, y que se encuentre bajo la responsabilidad de funcionarios debidamente capacitados.

- Que el Estado debe garantizar el derecho a ser oído y otorgar un recurso rápido y sencillo para hacer efectivo este derecho.

- Que el Estado debe capacitar a los órganos, autoridades y agentes públicos en materia de acceso a información.[127]

La misma Corte Interamericana de Derechos Humanos ha establecido en forma por demás certera: “para el ciudadano promedio es tan importante conocer las opiniones de otros o el tener acceso a la información en general tanto como lo es su propio derecho a impartir su propia opinión”, concluyendo que “una sociedad que no está bien informada es una sociedad que no es verdaderamente libre”.[128]

Finalmente, ha indicado en sendas e importantes sentencias que “la libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática.

Es indispensable para la formación de la opinión pública. Es también conditio sine qua non para que los partidos políticos, los sindicatos, las sociedades científicas y culturales y en general, quienes deseen influir sobre la colectividad puedan desarrollarse plenamente.

---

[127] ORGANIZACIÓN DE ESTADOS AMERICANOS.- AG/RES. 2288 (XXXVII-O/07).- Acceso a la información: fortalecimiento de la democracia. Adoptada el 5 de junio de 2007.

[128] CORTE INTERAMERICANA DE DERECHOS HUMANOS.- Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism OC-5/85, 13 de noviembre de 1985.

Es, en fin, condición para que la comunidad, a la hora de ejercer sus opciones, esté suficientemente informada."[129]

3. PRINCIPIO DE MÁXIMA TRANSPARENCIA

El derecho de acceso a la información pública ha sido determinado como un derecho humano fundamental y en ese sentido, en un Estado democrático se entenderá que el poder otorgado a las autoridades públicas, no es en otro sentido que, en nombre y representación del pueblo.

Entonces, el principio de máxima transparencia se convierte en el núcleo central del funcionamiento y ejercicio efectivo por parte de las personas – ciudadanos o no de los diferentes estados – del derecho de acceso a la información pública.

En efecto, la información debe existir en forma asequible, apropiada y tempestiva, ya que se trata de un presupuesto esencial para el desarrollo de una relación efectiva entre las personas y las diferentes entidades públicas.

Este principio implicará, en consecuencia, que toda la información del Estado, debe estar disponible y sólo por excepción – siempre limitada – podrá negarse su accesibilidad.

Si no es posible que se cuente con información será muy difícil constituir un marco adecuado para favorecer la protección de los derechos; establecer un diálogo igualitario, es fundamental.

Se entiende, además, que éste colabora en el reconocimiento de contenido a otros derechos fundamentales, siendo que a su vez se encuentra incluido en aquél más amplio del derecho a la información y que tiene como parte esencial a la información en su consideración en tanto bien de carácter jurídico.[130]

Joseph Stiglitz establece desde el punto de vista económico las dificultades que trae aparejado para las sociedades las asimetrías en materia de información y determina que "la información acerca de lo que el gobierno está haciendo faculta a los ciudadanos a examinar como el dinero público es gastado"[131]. Asimismo, se pregunta: "¿Cómo los ciudadanos pueden significativamente expresarse acerca de lo que su gobierno está haciendo si ellos no saben lo que hace?"[132]

---

[129] CORTE INTERAMERICANA DE DERECHOS HUMANOS.- Caso Ricardo Canese. Sentencia de 31 de agosto de 2004. Caso Herrera Ulloa. Sentencia de 2 de julio de 2004.
[130] NAHABETIÁN BRUNET, Laura.- Acceso a la información pública: pilar fundamental del buen gobierno. Montevideo, 2010.
[131] STIGLITZ, Joseph.- The right to know. Transparency for an Open World. Columbia University Press. Estados Unidos de América, 2007.
[132] STIGLITZ, Joseph.- Obra citada.

Es obligación de las entidades públicas la máxima divulgación y a cada persona le corresponde el correlato del derecho a recibir la información, sólo acotado por un elenco de excepciones limitadas y muy concretas.[133]

No es dable olvidarse tal como lo establece la Declaración Africana de Derechos Humanos y de los Pueblos que: "las entidades públicas no tiene la información para sí mismas sino como custodios del bien público".[134]

En el mismo sentido se ha expedido la Corte Interamericana de Derechos Humanos, al determinar que: "el actuar del Estado debe encontrarse regido por los principios de publicidad y transparencia en la gestión pública, lo que hace posible que las personas que se encuentran bajo su jurisdicción ejerzan el control democrático de las gestiones estatales, de forma tal que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento de las funciones públicas."[135]

Los tres mandatos especiales sobre la libertad de expresión, el Relator Especial de la ONU para la Libertad de Opinión y Expresión, el Representante de la OSCE sobre la Libertad de los Medios de Comunicación Social y el Relator Especial de la OEA sobre la Libertad de Expresión – en su Declaración Conjunta del año 2004 –, manifestaron: "El derecho a acceder a la información que está en manos de autoridades públicas es un derecho humano fundamental que debe darse vigencia a nivel nacional mediante legislación integral (por ejemplo, leyes sobre la libertad de información) en base al principio de transparencia máxima, estableciendo la suposición de que toda información está accesible, con sujeción apenas a un sistema escueto de excepciones".[136]

4. PRINCIPIO DE OBLIGACIÓN DE PUBLICAR

Este principio implica la concreción efectiva de la obligación que tienen las diferentes entidades públicas de presentar en forma electrónica determinada información que en general las normas establecen como información mínima y que se denomina transparencia activa.

"La libertad de información implica que las entidades públicas publiquen y difundan ampliamente documentos de significativo interés público, por ejemplo,

---

[133] NAHABETIÁN BRUNET, Laura.- Obra citada.

[134] Declaración Africana de los Derechos Humanos y de los Pueblos, artículo IV Libertad de Información: "las entidades públicas no detentan la información para sí mismas sino como custodias del bien público, y toda persona tiene derecho de acceder a esta información, con sujeción tan sólo a las reglas claramente definidas en la ley."

[135] CORTE INTERAMERICANA DE DERECHOS HUMANOS.- Caso Claude Reyes y otros vs. Estado de Chile. Sentencia de 19 de setiembre de 2006.

[136] ORGANIZACIÓN DE LAS NACIONES UNIDAS.- Comunicado de Prensa de 15 de Diciembre de 2004. Experts on Freedom of Expression Call for Steps to Change or Repeal Laws Restricting Access to Information. Disponible en: http://www.unhchr.ch/huricane/huricane.nsf/0/9A56F80984C8BD5EC1256F6B005C47F0?opendocument página visitada el 27 de junio de 2010.

información operativa sobre cómo funciona la entidad pública y el contenido de cualquier decisión o política que afecte al público."[137]

Lo cierto es que al dar cumplimiento a estas obligaciones, en general al menos al principio no por voluntad propia sino en función de que se trata de obligaciones de índole legal y constitucional, las entidades públicas quedan expuestas y no pueden ocultar u ocultarse más. Esto es, se verifica una suerte de emplazamiento en la obtención por parte de los ciudadanos de las respuestas que interiormente se hacen, y éstas deben aparecer, lo que en definitiva termina por generar un nuevo tipo de vínculo mucho más democrático y por lo mismo mucho menos asimétrico.[138]

La transparencia activa implica, tal como se establecerá en el Capítulo XII, una acción proactiva del Estado de presentar información determinada como mínima sin que las personas deban solicitarlo.

Ésta es fundamental para el fortalecimiento democrático en la medida que coadyuva en la generación de participación y confianza entre gobernantes y gobernados.

Las obligaciones de transparencia activa se establecen entre otros motivos con finalidades muy claramente determinadas. "El objetivo a más largo plazo debe ser el hacer que la información esté disponible proactivamente, para minimizar la necesidad de que los individuos tengan que recurrir a solicitudes para acceder a la misma".[139]

La Declaración Conjunta de Mandatos Especiales de ONU y OEA ha afirmado que es necesaria la inclusión de mecanismos que colaboren en el aumento de la información que se publica en forma continua y rutinaria, por lo que un criterio inclusivo determinaría la incorporación de datos tales como la estructura funcional, funcionarial, organizativa, sustancial y presupuestaria de las diferentes entidades públicas.

En este sentido, la Declaración Conjunta de los Relatores para la Libertad de Expresión de Naciones Unidas, de la Organización para la Seguridad y Cooperación en Europa y de la Comisión Interamericana de Derechos Humanos, señala: "las autoridades públicas deberán tener la obligación de publicar de forma dinámica, incluso en la ausencia de una solicitud, toda una gama de información de interés público. Se establecerán sistemas para aumentar, con el tiempo, la cantidad de información sujeta a dicha rutina de divulgación." [140]

---

[137] ORGANIZACIÓN DE LAS NACIONES UNIDAS.- Doc. E/CN.4/2000/63. Informe del relator especial. Promoción y protección del derecho a la libertad de opinión y expresión, enero 2000.
[138] NAHABETIÁN BRUNET, Laura.- Obra citada.
[139] UGALDE, Carlos.- Rendición de cuentas y democracia. El caso de México. IFE. México, 2002.
[140] Declaración conjunta aprobada el 6 de diciembre de 2004 por Ambeyi Ligabo, Representante Especial de la Comisión de Derechos Humanos de Naciones Unidas sobre el derecho a la libertad de opinión y de expresión, Miklos Haraszti, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y Cooperación en

Las normas de la ONU han establecido que: “la libertad de información implica que las entidades públicas publiquen y difundan ampliamente documentos de significativo interés público, por ejemplo, información operativa sobre cómo funciona la entidad pública y el contenido de cualquier decisión o política que afecte al público.”[141]

5. PRINCIPIO DE PROMOCIÓN DEL GOBIERNO ABIERTO

“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.”[142]

Imprescindible para cambiar es tener muy claro la opacidad, secrecía y por tanto las enormes dificultades que deben afrontarse por parte de quienes en ejercicio de un derecho fundamental pretenden relacionarse con el gobierno obteniendo los datos de que son dueños legítimos.

Es en mérito al principio de gobierno abierto, que debe tenerse presente que los actos y resoluciones, su fundamentación, la documentación que haya sido utilizada para sustentar las bases de los mismos así como los procedimientos que se hubieren seguido para su elaboración, sea que provengan de los poderes del Estado, las diferentes entidades de éste tienen por esencia carácter público, con la única salvedad de las excepciones que se establezcan en legal forma.

Las características de un gobierno abierto debe señalarse son:
- Acceso por parte de los ciudadanos y la prensa a los documentos de gobierno.
- Apertura de las reuniones – parlamentarias, actas de las entidades públicas, reuniones de las autoridades departamentales y locales - al público.
- Comunicación por parte del propio gobierno de la información acerca de sus políticas en instrumentación o a instrumentar.
- Consulta sistemática a quienes están interesados en la determinación de políticas públicas específicas, así como los avances de ejecución y la publicación de informes y opiniones sobre las mismas.

Así es posible afirmar también que es a partir de la concreción de la transparencia que se habilita una suerte de desinfección de las múltiples

---

Europa (OSCE), y Eduardo Bertoni, Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.

[141] ORGANIZACIÓN DE LAS NACIONES UNIDAS.- Documento citado.

[142] BEETHAM, David y BOYLE, Kevin.- Cuestiones sobre la democracia: Conceptos, elementos y principios básicos. UNESCO. París, 1996.

relaciones de tipo clientelar que el secreto construye en su entorno desde siempre. De esta forma se permite que cada una de las decisiones sea conocida, facilitando el pasaje desde el oscurantismo de la secrecía institucionalizada, donde el miedo a mostrar su actividad estaba en la primera línea de respuesta, a una cultura de apertura y accesibilidad donde se facilita la consolidación democrática a través del conocimiento, la facilitación del compromiso y el incentivo a la participación, para finalmente comprometer la legitimidad de un sistema que apueste a la calidad gubernamental.

6. PRINCIPIO DE LIMITACIÓN DE EXCEPCIONES

En la medida que el principio base y sustento del acceso a la información pública es – tal se expresara - aquél de transparencia máxima, las excepciones a la entrega y obtención de información por parte de las entidades públicas y las personas interesadas, sólo debe efectuarse mediante una legislación estricta que así lo establezca.

En efecto, las excepciones deben ser limitadas y sólo en la medida que refieran a cuestiones que sean fundamentales y que resguarden elementos tales como la dignidad de las personas, la defensa y seguridad públicas y el interés público. Sin embargo, estos conceptos son por demás amplios y esta amplitud lejos de favorecer el acceso que es lo que se pretende, lo controla y hasta la coarta.

Así es que las normas de ONU disponen: “La negativa de divulgar información no podrá fundamentarse en la finalidad de proteger a los gobiernos de una situación embarazosa o la revelación de sus actos incorrectos, una lista completa de las finalidades legítimas que podrían justificar no divulgar deberá disponerse en la ley y las excepciones deben ser formuladas en términos estrechos para evitar la inclusión de material que no afecte el interés legítimo.”[143]

Es evidente que las excepciones se limitarán a situaciones en las que de entregarse la información podrían plantearse perjuicios de carácter real o potencial. Sin embargo, debe considerarse que aún elaborando muy específicamente el elenco de excepciones, es posible que existan casos en los que de todas formas el interés público estará calificado de una manera que la divulgación de la información puede resultar de más importancia que el perjuicio que pudiere causarse al interés protegido y por el que se hubieren determinado las excepciones.

La Suprema Corte de Justicia de los Estados Unidos Mexicanos ha establecido en este sentido que “al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un

[143] ORGANIZACIÓN DE LAS NACIONES UNIDAS.- Doc. E/CN.4/2000/63. Informe del relator especial. Promoción y protección del derecho a la libertad de opinión y expresión, enero 2000.

lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecto a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados."[144]

Finalmente, será entonces de fundamental consideración la ponderación, ya no sólo en materia de consideración de supremacía de derechos, sino para la consideración de la importancia de los intereses protegidos y vulnerables en cada caso. Por tanto, tener en cuenta los elementos de idoneidad, necesidad y proporcionalidad en sentido estricto[145], tienen aquí un sentido de aplicación por demás importante.

7. PRINCIPIO DE EXISTENCIA DE PROCESOS DE FACILITACIÓN DEL ACCESO

Este principio se vincula directamente con la denominada transparencia pasiva. En efecto, ésta implica la posibilidad que deben tener las personas de, mediante procedimientos de tipo administrativo y jurisdiccional, acceder a la información que es pretendida.

El Dr. Ferreiro ha establecido que: "Deben los ciudadanos tener la posibilidad de cuestionar judicialmente la denegación de acceso que la Administración fundamente en razón de alguna causal legal."[146]

La persona que solicita la información tiene un procedimiento específico para efectuar su solicitud; en general – salvo en la República Italiana - no debe expresar el motivo por el cual lo solicita, y existe un tiempo específico para concretar la respuesta por parte del sujeto obligado. Este procedimiento otorga garantías a la persona requirente, ya que en general es específico para el caso del acceso a la información y no depende del cumplimiento de ningún tipo de condición, sino simplemente de la verificación de la voluntad de facilitación del ejercicio del derecho por parte de la entidad de que se trate.

"El Estado tiene una doble obligación: abstenerse o no impedir, y brindar toda la información que contengan sus fuentes, salvo las excepciones mencionadas en la ley. Tiene también la obligación de impedir que cualquier particular o persona pública obstaculice el acceso a esa información. … Tiene obligación de abstenerse, obligación positiva de impedir y obligación de dar acceso a la información completa.

---

[144] SEMANARIO JUDICIAL DE LA FEDERACIÓN Y SU GACETA T XI abril de 2000. Tesis XLVII/2000.
[145] ALEXY, Robert.- Epílogo a la Teoría de los Derechos Fundamentales. Madrid, 2004.
[146] FERREIRO, Alejandro.- "Dinero, política y transparencia: el imperativo democrático de combatir la corrupción". Ponencia presentada en la 9th International Anti-Corruption Conference (IACC), Durban, 1999, Disponible en www.9iacc.org , página visitada el 27 de junio de 2010.

En una sociedad democrática el contenido del derecho a recibir información se ejerce fundamentalmente frente al Estado, el cual, está obligado a abstenerse y a remover todo obstáculo que impida el efectivo ejercicio de ese acceso. El acceso directo a los registros y archivos públicos es parte indispensable de este derecho y tiene que estar garantizado por las vías jurisdiccionales, llámese recurso de amparo o el específico hábeas data."[147]

Ahora bien, a los efectos que estos procedimientos se vean garantizados y las posibilidades de answerability - obligación de los representantes y los funcionarios de informar sobre las decisiones que adopten y otorgar justificación de las mismas – y de enforcement - capacidad de sanción a representantes y funcionarios en caso de que se verifique la violación de sus obligaciones públicas – cumplimentadas, es imprescindible la existencia de órganos de contralor.

Éstos tienen el desafío, la obligación y la responsabilidad de ser garantes nada menos que de la democracia. Si asumimos que el derecho fundamental al acceso a la información pública, es sustento de la libertad de expresión por un lado y de la posibilidad de elegir a los gobernantes por otro, se comprenderá la importancia que reviste el órgano que debe garantizarlo.

"...la política de transparencia... se refiere a las decisiones y los procesos asumidos por el Estado para darle contenido sustantivo a los principios democráticos de responsabilidad, publicidad e inclusión en la agenda gubernamental ... reclama una política definida capaz de responder a los problemas que se derivan de las asimetrías de la información en la acción pública y de vincular las decisiones tomadas por los distintos gobiernos con la mayor transparencia posible. Así, mientras el derecho de acceso a la información pública ha de ser universal para todos los ciudadanos, la política de transparencia ha de responder a las características propias de los gobiernos."[148]

8. PRINCIPIO DE GRATUIDAD

Se trata de un principio fundamental a los efectos de garantizar que la mayor cantidad de personas tengan facilitado el acceso a la información pública, constituyéndose entonces en una piedra angular para su concreción. Es a nivel del derecho comparado un principio sine qua non para la efectividad de este derecho fundamental, - al entenderse que el derecho de acceso a la información pública es un pilar fundamental del buen gobierno y un elemento de sustancia del desarrollo de la democracia y sustento del Estado de Derecho -, ya que las posibilidades económicas de los solicitantes no pueden tener injerencia de tipo alguno en la efectividad del mismo.

Sin embargo, sí se encuentra prevista la posibilidad de solicitar un reembolso a la entidad estatal que entrega la información con la única finalidad de resarcirse de los gastos del soporte de la información. En este sentido las normas de la

[147] URIOSTE, Fernando.- Derecho de la información. Buenos Aires, 2009.
[148] MERINO, Mauricio.- "Muchas políticas y un sólo derecho", en Democracia, Transparencia y Constitución: propuestas para un debate necesario. México, 2006.

ONU establecen en forma clara y enfática que los costos del acceso no pueden impedirlo, determinando: "El acceso público a la información es gratuito en tanto no se requiera la reproducción de la misma. Los costos de la reproducción de la información son a cargo del solicitante. En todo caso, las tarifas cobradas por la institución deberán ser razonables y calculadas tomando como base el costo del suministro de la información a fin de no causar una carga excesivamente onerosa a la entidad que entrega la información solicitada por el ciudadano. La información que se presta por medio de servicios de correo electrónico y de acceso público por vía de internet será entregada en forma gratuita al ciudadano."[149]

Finalmente en la recientemente aprobada Ley Modelo Interamericana sobre acceso a la información se establece en el artículo 28:
"(1) El solicitante sólo pagará el costo de reproducción de la información solicitada y, de ser el caso, el costo de envío, si así lo hubiese requerido. La información enviada de manera electrónica no podrá tener ningún cargo.

(2) El costo de reproducción y de envío no podrá exceder el valor del material en el que se soporta la reproducción; el costo del envío no deberá exceder el costo que este pudiera tener en el mercado. El costo del mercado, para este propósito, deberá ser establecido periódicamente por la Comisión de Información."[150]

9. PRINCIPIO DE REUNIONES ABIERTAS

"Si la función de la esfera pública es iluminar los asuntos humanos proporcionando un espacio de apariciones, donde los hombres puedan mostrar, a través de la palabra y de la acción, por lo mejor y por lo peor, quiénes son y qué pueden hacer, entonces, las sombras llegan cuando la luz de lo público se ve oscurecida por "fosos de credibilidad" y por "gobiernos invisibles"."[151]

Las Normas de ONU establecen la idea de la existencia de reuniones abiertas lo que implica que no sólo la información de las reuniones debe estar disponible sino que las propias reuniones de los sujetos obligados deberían ser también abiertas. Afirman: "La ley debe establecer la suposición de que toda reunión de las entidades del gobierno está abierta para el público"[152]. No hay acuerdo definitivo a nivel internacional sobre este principio pero se verifica una tendencia afirmativa en este sentido.

El hecho que las reuniones de los sujetos obligados que deliberan y adoptan decisiones que tienen incidencia directa sobre la actuación de la ciudadanía no sean públicas, está implicando una limitación en el derecho de acceso a la

---

[149] ORGANIZACIÓN DE ESTADOS AMERICANOS.- Herramientas de Cooperación Jurídica. Serie Legislaciones Modelo. Ley Modelo de acceso a la información administrativa, artículo 18. Esta Ley fue elaborada por el Jurista costarricense Alfredo Chirino Sánchez.
[150] ORGANIZACIÓN DE ESTADOS AMERICANOS.- XL Reunión de la Asamblea General y del Consejo Permanente. Junio 2010.
[151] ARENDT, Hannah.- Men in dark times. Nueva York. 1968.
[152] ORGANIZACIÓN DE LAS NACIONES UNIDAS.- Informe citado.

información pública, ya que impide que los asuntos públicos sean conocidos en todo su desarrollo por la ciudadanía. Si a esto se suma que es una costumbre bastante habitual el desarrollo de reuniones "informales" incluso privadas y fuera de los protocolos establecidos reglamentariamente para adoptar decisiones en relación con asuntos de consideración para las instituciones, es posible afirmar que de esta forma el derecho de acceso a la información pública podría verse menoscabado e incluso no es equivocado pensar que se podrían presentar supuestos de corrupción gubernamental.[153]

10. PRINCIPIO DE TRANSPARENCIA PRECEDENTE

Si se analiza el contenido del derecho de acceso a la información pública es posible determinar que éste servirá, para dar protección y sustentar el cumplimiento de otros derechos fundamentales. Esto puede considerarse así, en la medida que se entienda que éste colabora en el reconocimiento de contenido a otros derechos fundamentales, siendo que a su vez se encuentra incluido en aquél más amplio del derecho a la información y que tiene como parte esencial a la información en su consideración en tanto bien de carácter jurídico.

Del análisis de los elementos que se incluyen en el derecho de acceso a la información, es posible deducir que esta garantía está íntimamente vinculada con el respeto de la verdad. Se trata de un concepto básico para el mejoramiento de la conciencia colectiva que sin dudas contribuye al progreso social general. "Si las autoridades públicas, elegidas o designadas para servir y defender a la sociedad, asumen ante ésta actitudes que permitan atribuirles conductas faltas de ética, al entregar a la comunidad una información manipulada, incompleta, condicionada a intereses de grupos o personas, que le vede la posibilidad de conocer la verdad para poder participar libremente en la formación de la voluntad general, incurren en violación grave a las garantías individuales, pues su proceder conlleva a considerar que existe en ellas la propensión de incorporar a nuestra vida política, lo que podríamos llamar la cultura del engaño, de la maquinación y de la ocultación, en lugar de enfrentar la verdad y tomar acciones rápidas y eficaces para llegar a ésta y hacerla del conocimiento de los gobernados."[154]

Por tanto, el principio de la transparencia precedente implica en línea con lo establecido que deberá analizarse la legislación existente al momento del dictado de normas vinculadas con el acceso a la información y siempre éste será el que se mantendrá vigente, salvo excepciones muy limitadas. Toda la normativa que presente inconsistencias para con el ejercicio de este derecho deberán ser modificadas o derogadas a los efectos de privilegiar el acceso.

La Corte Interamericana de Derechos Humanos, por su parte estableció que: "considera necesario reiterar que, de conformidad con el deber dispuesto en el artículo 2 de la Convención, el Estado tiene que adoptar las medidas necesarias para garantizar los derechos protegidos en la Convención, lo cual

[153] NAHABETIÁN BRUNET, Laura.- Obra citada.
[154] SUPREMA CORTE DE JUSTICIA DE LOS ESTADOS UNIDOS MEXICANOS.- Tesis Nº LXXXIX/1996, de fecha 24 de junio de 1996.

implica la supresión tanto de las normas y prácticas que entrañen violaciones a tales derechos, así como la expedición de normas y el desarrollo de prácticas conducentes a la efectiva observancia de dichas garantías. En particular, ello implica que la normativa que regule restricciones al acceso a la información bajo el control del Estado debe cumplir con los parámetros convencionales y sólo pueden realizarse restricciones por las razones permitidas por la Convención, lo cual es también aplicable a las decisiones que adopten los órganos internos en dicha materia". [155]

11. PRINCIPIO DE PROTECCIÓN DE DENUNCIANTES

La organización internacional no gubernamental Article 19 en su Principio 9, establece: "Protección a denunciantes. La legislación debe incluir disposiciones que protejan a las personas de las sanciones legales, administrativas y de empleo por entregar información sobre errores/fechorías cometidas."

El principio de protección de denunciantes implica que la legislación nacional deberá proteger a aquellos funcionarios que en forma responsable y de buena fe, den a conocer información, sin estar sometidos a sanciones.

Así la opacidad y el secretismo característicos podrán iniciar el camino de su subsanación. De lo contrario los funcionarios continuarán prefiriendo el secreto antes que la exposición y la seguridad de problemas, dado el tradicional comportamiento de las administraciones y los administrados.

Si se garantiza protección a los denunciantes podrá comenzar el tan necesario camino del cambio cultural que implica avanzar en la concreción de la transparencia y claridad.

Es decir que se debe proteger la confidencialidad de los denunciantes de forma tal que todos quienes estén vinculados con un proceso de investigación tengan la obligatoriedad de mantener en forma confidencial la identidad de partes, testigos y terceros involucrados en el mismo. Asimismo, deben establecerse mecanismos mediante los cuales, quien comprometa tal confidencialidad esté sujeto a sanciones de tipo disciplinario, por lo menos.

Esto es fundamental si se pretende avanzar en forma cierta en este tema, que en muchas legislaciones, - fundamentalmente en la mayoría de las latinoamericanas - no está incluido.

12. CONCLUSIONES

"Una democracia requiere de un funcionamiento transparente y responsable por parte de los poderes públicos; esto significa que los ciudadanos deben tener la capacidad jurídica de conocer en todo momento la conducta de sus gobernantes. De otra manera, es imposible asignar responsabilidades a los malos funcionarios y recompensar a los buenos."[156]

---

[155] CORTE INTERAMERICANA DE DERECHOS HUMANOS.- Sentencia citada.
[156] LÓPEZ AYLLON, Sergio.- Democracia y acceso a la información. TRIFE. México, 2005.

Es preciso tener conciencia que el verdadero dueño de la información no es otro que el pueblo y las entidades públicas no tienen la información para sí mismas sino como custodias del bien público.

Como la mayoría de los gobiernos están acostumbrados a trabajar en secreto, la transparencia parece ser más una declaración de principios con muy buenas intenciones pero con escasa penetración en la mayoría de los burócratas con un compromiso cierto.

Éstos han desarrollado toda una situación de pertenencia en relación con los documentos sobre los que tienen responsabilidades y entienden que entregarlos al público es lo mismo que ceder el control, por tanto el poder.

Abdul Waheed Khan ha establecido que "un valor fundamental que sostiene el derecho a saber es el principio de la transparencia máxima, que establece la suposición de que toda información en poder de las entidades públicas debe estar sujeta a la divulgación a menos que exista una justificación más poderosa para no divulgarla en defensa del interés público. Este principio también implica la introducción de mecanismos eficaces mediante los cuales el pueblo pueda acceder a la información, incluyendo sistemas para responder a las solicitudes, así como publicación y difusión proactivas del material clave."[157]

Asimismo el Presidente Carter ha establecido que: "una ciudadanía informada podrá exigir responsabilidad a sus gobiernos por sus políticas y elegir sus dirigentes con mayor efectividad."[158]

Ahora bien, es fundamental establecer que al derecho del ciudadano a ser informado corresponde la obligación de la Administración de informar con absoluta veracidad. Si bien es cierto que no se trata de un principio novedoso, sí lo son ciertos avances legislativos en algunos países que han incluido normas claras y eficaces sobre la apertura de archivos y la atención de solicitudes de información efectuadas por cualquier ciudadano, con la única excepción de aquellos documentos que han sido expresamente reservados.

"Un sistema ágil y ligero de vigilancia política implica ciudadanos con poder para denunciar y detonar mecanismos legales de rendición de cuentas. Un sistema eficiente de rendición de cuentas requiere transparencia gubernamental. La responsabilidad de los votantes va más allá de emitir su voto cada tres o seis años. Su participación para exigir cuentas es indispensable para que nuestra democracia electoral sea a la vez una democracia gobernable y que resuelva los problemas cotidianos de la población."[159]

Modificar la mentalidad es prioritario en la medida que constituye uno de los mayores retos tanto para la sociedad civil involucrada en la militancia activa a

---

[157] ABDUL WAHEED, Khan.- "Presentación", en Libertad de Información: Comparación Jurídica.- UNESCO. París, 2003.
[158] CARTER, James.- Prefacio al libro "Acceso a la Información: la llave para la Democracia". Centro Carter. Atlanta, 2002.
[159] UGALDE, Carlos.- Obra citada.

favor del acceso a la información pública, cuanto para quienes están en la primera línea de la formulación de las políticas públicas en el tema. Las dificultades no son menores, sino importantes y crecientes en la medida que se inician las acciones, sin embargo, las recompensas son múltiples y de magnitudes considerables.

Ahora bien, la capacidad de aprender y aprehender en términos teóricos y prácticos de las buenas y malas prácticas que en materia de instrumentación es factible encontrar a lo largo y ancho del mundo, es sin dudas capital y base de trabajo sustancial para el éxito de la pretensión.

No cabe dudas que la aplicación correcta de las leyes de acceso a la información y transparencia pueden cambiar las reglas del juego no sólo para la sociedad civil sino también para el gobierno, además de contribuir al fortalecimiento del marco político democrático, la calidad institucional y la superación del déficit democrático, que en situación tan compleja coloca a América Latina en su conjunto.

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.

En esta línea, el acceso a la información pública se concreta en un elemento sustancial de los esfuerzos destinados a la reducción de la corrupción, el incremento de la responsabilidad gubernamental en la acción pública y a la construcción y fortalecimiento de confianzas en la particular relación ciudadano – gobierno.

Por tanto afirmar, que éste conjuntamente con la transparencia y la rendición de cuentas son las bases sustanciales del buen gobierno, implica que no son negociables. En el mismo sentido, buen gobierno debe asociarse a la idea de gobernanza y por tanto, a la pretensión de incremento de los niveles de democracia y con ella de verificación del Estado de Derecho. Para ello, los principios del acceso a la información pública, se presentan como sustanciales en la medida que se dirigen a la sustanciación de su consideración en calidad de derechos fundamentales.

De esta forma, y al considerar a los derechos fundamentales en tanto: "...triunfos políticos en manos de los individuos. Los individuos tienen derechos cuando, por alguna razón, una meta colectiva no es justificación suficiente para negarles lo que, en cuanto individuos, desean tener o hacer, o cuando no justifica suficientemente que se les imponga una pérdida o un perjuicio."[160]

Así es que es de sustancia no perder de vista que en el centro de estas afirmaciones está la consideración de la persona como ser individual y colectivo en torno a la cual se construye la visión democrática y social que se sustenta. En este sentido entonces y como bien se ha destacado, "Definir a la persona como centro de la acción pública significa no sólo, ni principalmente,

[160] DWORKIN, Ronald.- Los derechos en serio. Barcelona, 1993.

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."[161]

[161] 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.

CAPÍTULO IX – LA LEY N° 18.381 DE ACCESO A LA INFORMACIÓN PÚBLICA

Dra. Graciela Romero

1. INTRODUCCIÓN

La Ley N° 18.381 de Acceso a la Información Pública de 17 de octubre de 2008 tiene su origen en la sociedad civil ya que en el año 2004, -con la intención de impulsar el reconocimiento del Derecho de Acceso a la Información Pública-, un conjunto de asociaciones civiles u organizaciones de la sociedad civil, conformaron el Grupo de Acceso a la Información Pública (GAIP). Este grupo estaba integrado por organizaciones especializadas en Derechos Humanos como Amnistía Internacional-Sección Uruguay, IELSUR y SERPAJ, especializadas en la defensa de la libertad de expresión y de pensamiento como APU y AMARC, organizaciones que trabajan por la transparencia del Estado como Uruguay Transparente y Asociación Ciudadana por los Derechos Civiles, o que trabajan con el manejo y la organización de la información como el Archivo General de la Nación, Archiveros sin Fronteras- Sección Uruguay, Asociación Uruguaya de Archiveros y Escuela Universitaria de Bibliotecología y Ciencias afines.

La reseña de su origen constituye un dato importante a efectos de evaluar el consenso alcanzado por esta norma al ser aprobada por el Parlamento Nacional. En este caso podría afirmarse, que se ha cumplido con el "círculo virtuoso" de las políticas públicas, ya que ha existido en su elaboración, participación activa de la sociedad civil, así como del Estado a través del Parlamento Nacional y del Gobierno.

Es necesario enfatizar en la importancia que posee la consagración expresa del derecho de acceso a la información pública en nuestro derecho interno, así como la regulación y la protección de la información pública como un bien que nos pertenece a todos, y no únicamente a la administración pública y sus funcionarios.

Justamente, como la información pública debe considerarse como un “bien público común”[162], a partir de ahora la Ley determina de qué forma debe guardarse, conservarse, preservarse u ordenarse, así como también cuál es el procedimiento para brindar el acceso a todas las personas por igual, o para clasificar cierta información como reservada o confidencial, cuando así corresponda legalmente.

Actualmente, más de un centenar de países en el mundo cuentan con una ley de acceso a la información pública reconociéndose así, la importancia de este

[162] FUENMAYOR ESPINA, Alejandro. El Derecho de Acceso de los Ciudadanos a la Información Pública. Análisis Jurídico y recomendaciones para una propuesta de ley modelo sobre el derecho de acceso de los ciudadanos a la información pública. San José C.R.: Oficina de la UNESCO para América Central. 1 era. Edición Año 2004, pág. 6.

derecho que faculta a todas las personas a solicitar información en poder del Estado y que se erige como pilar de la denominada “accountability social” [163].

Las múltiples implicancias y la enorme incidencia que posee el Derecho de Acceso a la Información Pública en un sistema democrático, explican el hecho de que actualmente no se pueda hablar de gobernabilidad[164], sin asociarla a la existencia de mecanismos efectivos de participación y acceso a la información pública. En este sentido expresa el Programa de Naciones Unidas para el Desarrollo, que “El trabajar con menos recursos públicos para ayudar a más personas necesitadas significa que los gobiernos tienen que ser mejores a la hora de prestar servicios y asegurar igualdad e inclusión en los ámbitos económico, social y político. Al mismo tiempo, (...) requiere que las organizaciones de la sociedad civil y los ciudadanos tengan la capacidad de hacer que sus gobiernos rindan cuentas. Todos estos elementos juntos conforman el orden del día (…) en materia de gobernanza democrática"[165].

A su vez, en el documento “Información y Gobernabilidad” se reafirma este concepto cuando se expresa que: “El acceso a la información, su producción, difusión y buena gestión contribuyen a la gobernabilidad. ¿Cómo compartir el poder de manera honesta y responsable sin intercambio de información entre las instituciones, los órganos de control y todas las partes concernidas por dicha gestión? ¿Cómo luchar contra la violación de los derechos humanos si se desconocen los abusos cometidos? ¿Cómo proteger la naturaleza si no estamos informados de su estado de salud?"[166].

En definitiva, la aprobación de una ley que garantiza este derecho es fundamental, pues significa pasar “de un principio de provisión de la información gubernamental desde la base de una “necesidad de conocer” al principio de un “derecho por conocer”[167].

Ello a su vez favorece la participación ciudadana, ya que como señala la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, en el Informe del año 2002: "El derecho y respeto de la

---

[163] "El concepto de accountability hace referencia a la capacidad para asegurar que los funcionarios públicos rindan cuenta por sus conductas, es decir, que estén obligados a justificar y a informar sobre sus decisiones y a que eventualmente puedan ser castigados por ellas. Mediante una metáfora espacial, Guillermo O`Donnell ha clasificado los mecanismos de accountability en horizontales y verticales. La accountability horizontal se refiere a la operación de un sistema intraestatal de controles, mientras que los mecanismos verticales implican la existencia de controles externos sobre el Estado". FUENMAYOR ESPINA, Alejandro. Ob. Cit., pág. 22.

[164] Programa de Naciones Unidas para el desarrollo. http://www.undp.org/spanish/temas/gobernabilidad.shtml/ Página visitada 14 de julio de 2010.

[165] Programa de Naciones Unidas para el desarrollo. Obra Citada.

[166] Información y Gobernabilidad. Documento de Orientación. Agencia Suiza para el Desarrollo y la Cooperación (COSUDE). Ministerio Suizo de Asuntos Exteriores (DFAE). 2004. http://www.deza.admin.ch/es/Pagina_principal/Documentacion/Publicacion Página visitada el 14 de julio de 2010.

[167] ACKERMAN, John y SANDOVAL, Irma. Cuadernos IFAI. Leyes de Acceso a la Información en el Mundo. Capítulo 11. Cuaderno de Transparencia N° 7. 1era. Edición 2005. Página 20. http://cronopio.flacso.cl/fondo/pub/openaccess/2007/revista/028723.pdf. Página visitada 11 de octubre de 2011.

libertad de expresión se erige como un instrumento que permite el intercambio libre de ideas y funciona como ente fortalecedor de los procesos democráticos, a la vez que otorga a la ciudadanía una herramienta básica de participación (…)"[168].

Por otra parte, tal como expresa la UNESCO, "La Sociedad de la Información (...) incluye una noción de servicio universal de hacer accesible la información a todos. De ahí que la UNESCO la denomine "la sociedad de la información para todos", la cual nos compromete a defender y garantizar el derecho a la información y facilitar los medios de comunicación y de acceso, es decir, que exista un marco de libertad y democracia que permita que todo ciudadano, independientemente de su condición social, económica, étnica, religiosa, política y de idioma, pueda tener acceso a la información y existan los mecanismos que la faciliten (...)" [169].

Precisamente ante esta nueva realidad, uno de los principales desafíos que se presenta "(...) está en darle marco integral a las nuevas tecnologías de información y comunicación con leyes de acceso a la información pública gubernamental que formulen no solo procedimientos de entrega de información oficial, sino también obligaciones de transparencia a través de portales y medios electrónicos disponibles a todos los ciudadanos sin discriminación"[170].

En definitiva, lo anteriormente expuesto se subsume dentro de los principales objetivos planteados por la Ley N° 18.381, el fomento de la transparencia de la función administrativa y el ejercicio efectivo del derecho de acceso a la información pública reconocido como un derecho fundamental. Ambos constituyen metas que sin lugar a dudas, contribuirán significativamente al proceso de transformación hacia un Estado más cercano y abierto a los administrados, más eficiente y más democrático.

2. ÁMBITO DE APLICACIÓN

2.1 Sujetos obligados

La Ley N° 18.381 de Acceso a la Información Pública, en su art. 1º expresa que "(...) tiene por objeto establecer la transparencia de la función administrativa de todo organismo público, sea o no estatal (...)". y en el art. 2° establece el alcance en los siguientes términos: "Se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, (...)".

Por último, en el art. 5° vuelve a referirse a organismos públicos, sean o no estatales, como sujetos obligados a la difusión de la información a través de

---

[168] Informe del Relator Especial para la Libertad de Expresión de la OEA. Capítulo IV. Libertad de Expresión y Pobreza. "El acceso a la información pública como ejercicio de la libertad de expresión de los pobres". Puntos 12 y 17. 2002. http://www.cidh.org/relatoria/showarticle.asp?artID=329&IID=2 Página visitada el 15 de julio de 2010.
[169] FUENMAYOR ESPINA, Alejandro. Ob. Cit., pág. 21.
[170] FUENMAYOR ESPINA, Alejandro. Ob. Cit., pág. 64.

sus páginas Web. En el resto de su articulado la Ley alude a estos organismos sólo como "sujetos obligados".

Los sujetos obligados en definitiva, son los organismos públicos estatales y no estatales, pero no así aquellas sociedades, organismos o instituciones que se regulan por el derecho privado, aunque muchos de ellos gestionen fondos públicos o el Estado sea el principal accionista o posea una participación accionaria.

En este sentido, Sayagués Lazo propone un criterio para determinar cuándo nos encontramos ante una persona de derecho público y cuando nos encontramos ante una persona de derecho privado. Serían personas públicas estatales según Sayagués, cuando "(...) integran la organización jurídica de la nación. Su patrimonio pertenece a la colectividad y los fines que cumplen son fines propios de ésta. Su creación se explica por la imposibilidad de que las entidades públicas clásicas de base territorial, congestionadas por múltiples cometidos, puedan cumplir esos fines directamente, por sí mismas. Son los entes autónomos" y "servicios descentralizados" (...) que son personas públicas, no sólo por su calidad de estatales, sino porque actúan bajo normas de derecho público, lo cual (...) no excluye la aplicación del derecho privado dentro de ciertos límites"[171].

Según este autor, "los conceptos tradicionales han sido superados por las nuevas tendencias del derecho. (...) la distinción entre las personas públicas y privadas no puede hacerse sobre la base de su calidad de estatal o no, sino en razón del régimen jurídico en que se mueven: si se regulan por el derecho público, en todo o en parte, serán personas públicas; si exclusivamente por el derecho privado, serán personas privadas"[172].

En definitiva, cabe concluir que la Ley N° 18.381 sólo habilita legalmente a solicitar información de todas aquellas personas públicas estatales y no estatales que se desarrollan básicamente en el ámbito del Derecho Público.

Por su parte el art. 1° de la Ley también expresa que tiene por objeto promover la transparencia de la función administrativa. ¿A qué se refiere con "función administrativa"?.

Según Daniel Hugo Martins[173], para Linares la función administrativa consiste "en ejecutar -fuera de situaciones contenciosas- normas jurídicas de toda especie, en cuanto a su extensión lógica, mediante decisiones individuales normativas que particularizan, en casos concretos, cualesquiera de los contenidos de aquellas normas aplicadas y mediante hechos administrativos".

---

[171] SAYAGUÉS LASO, Enrique. Tratado de derecho Administrativo. Tomo II. 7ma. Edición puesta al día a 2002 por Daniel Hugo Martins. Montevideo. FCU, págs. 228 y sgtes.
[172] SAYAGUÉS LASO, Enrique. Ob. Cit., pág. 228 y sgtes.
[173] MARTINS, Daniel. "La esencia del derecho objeto y método de la ciencia del Derecho Administrativo (A propósito de una definición de Juan Francisco Linares)" en www.lajusticiauruguaya.com.uy. Página visitada el 21 de setiembre de 2009.

Aclara Martins que "la función de ejecutar, es conducta en interferencia intersubjetiva, que se da entre sujetos humanos que son órganos del Estado y particulares, o sólo entre órganos del Estado o sólo entre particulares. El orden jurídico se encarga de señalar "quiénes" son esos sujetos y "qué" pueden hacer legítimamente"[174].

En tanto, Sayagués Laso entiende por administración, a "los órganos públicos actuando en función administrativa" y por ésta, "a la actividad estatal que tiene por objeto la realización de los cometidos estatales en cuanto requieran ejecución práctica, mediante actos jurídicos -que pueden ser reglamentos, actos subjetivos o actos condición- y operaciones materiales".

Según el Prof. Carlos Delpiazzo[175], hay tres dimensiones a considerar dentro de la función administrativa, "que la distinguen y enmarcan: la jurídica, la operativa y la ética. En atención a ellas, puede decirse que la función administrativa consiste en el ejercicio de poderes jurídicos distintos a los de legislar y decir el Derecho (dimensión jurídica), que son necesarios para la concreción práctica de la diversidad de cometidos estatales (dimensión operativa) en servicio de la sociedad y de sus integrantes para el logro del bien común (dimensión ética)".

En definitiva según este autor, "desde el punto de vista jurídico, el ejercicio de la función administrativa se concreta en la organización y, especialmente, en la actividad de la administración. Bajo este enfoque, interesa destacar su sometimiento a la regla de Derecho (principio de juridicidad) y su carácter instrumental. (…) la función administrativa es medio y participa de la naturaleza instrumental de los sujetos que la cumplen: El Estado y los entes menores, que no son fines en sí mismos sino que existen para el bien común".

En cuanto a la dimensión ética, señala Delpiazzo que, "en la medida que "administrar" quiere decir etimológicamente "servir a" y que, por tanto, la función administrativa es función de servicio, la dimensión ética de la misma tiene su eje central en la idea de servicio a la sociedad en orden a la consecución del bien común."

Esta dimensión que destaca el Dr. Delpiazzo, a nuestro entender podría relacionarse a su vez con el concepto de información pública concebida ya no como propiedad de la administración y sus funcionarios, sino también como un bien que pertenece a todas las personas que sin distinción alguna y sin exponer motivo, tienen derecho a acceder a la misma en los términos que fija la norma.

En definitiva, "el Estado actúa en la información a través de todas sus potestades: legislativa, reglamentaria, judicial, de policía, sancionadora, pues cualquier acto administrativo puede originar una noticia, una respuesta social o

[174] MARTINS, Daniel. Ob. Cit.
[175] DELPIAZZO, Carlos. Derecho Administrativo Uruguayo. Editorial Porrúa. México 2005, pág.25.

una opinión. Tiene unas actuaciones que, participando de una o varias de las potestades anteriores, le convierten específicamente en informador"[176].

2.2 Concepto de información pública

Como ya se ha expresado supra, la Ley en el art. 2° se establece que "se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, (...)".

El Código de Buenas Prácticas y Alternativas para el Diseño de Leyes de Transparencia y Acceso a la Información Pública de México[177] define como información pública a: "toda información en posesión de los sujetos obligados que no tenga el carácter de confidencial", y reconoce que los principios que rigen para la información pública no rigen para la información confidencial, pues hay cierta "(…) información a la que no se le aplica el principio de máxima publicidad, pues la información confidencial, es decir aquélla referida a la protección de la vida privada y los datos personales, se rige por otros principios. Esto no quiere decir que la información confidencial se mantenga siempre alejada del conocimiento público. El propio Código de Buenas Prácticas establece las excepciones que permiten la divulgación de información confidencial cuando existe un interés público que así lo justifica".

Este Código también aclara que los datos referidos a las personas jurídicas, -que se equiparan a datos personales-, también se protegen (personas morales se denominan en este Código y así lo establece el art. 503 del mismo). Nuestra Ley también hace referencia a cierta información confidencial que pueden entregar en tal carácter las personas jurídicas, en el art. 10, numeral I.

Por ende, la información pública y la información confidencial tienen diferencias sustanciales entre sí, pero la principal diferencia está constituida por el hecho de que la información pública es la que emana o está en poder de los sujetos obligados, que puede estar disponible y ser accesible por cualquier persona.

También cabe señalar, que en el caso de la información pública, incluso aunque ésta esté clasificada como información reservada, sigue siendo información pública sólo que se reserva al conocimiento o al acceso de las personas durante determinado período de tiempo. En cambio, la información confidencial es información generalmente perteneciente a personas físicas o jurídicas, que por diferentes motivos posee el Estado según lo establecido en el artículo 10.

Esta diferencia es importante ya que no es lo mismo una información reservada, sujeta a determinado plazo por razones de interés público que justifican su reserva, que una información confidencial, mantenida en esa situación por tiempo indefinido.

---

[176] BASTONS, Jorge Luis y ELIADES, Analía. El Derecho de Acceso a la Información Pública en el Ámbito Iberoamericano. Marzo 2007. Noticias Jurídicas. http://noticias.juridicas.com/articulos/00-Generalidades/200703-5102003278491354578.html. Página visitada el 20 de julio de 2010.

[177] Elaborado con el apoyo del Instituto de Federal de Acceso a la Información de México. IFAI. Año 2007.

En definitiva la información pública es aquélla que le pertenece a todas las personas que por ende tienen derecho a conocerla, y es la que se encuentra en poder de las organismos públicas, estatales o no, independientemente del formato en que se guarde (papel, soporte digital, etc.), del organismo que la elaboró, obtuvo o posee y de la fecha de su elaboración.

3. DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

3.1 Legitimación activa

El derecho de acceso a la información pública, es un derecho humano derivado del derecho a la información en cuyas vertientes se encuentran la libertad de expresión y de pensamiento. Es un derecho reconocido por el Derecho Internacional tanto en la Declaración Universal de Derechos Humanos, como en el Pacto de Derechos Civiles y Políticos y en la Convención Interamericana de Derechos Humanos[178], entre otros instrumentos jurídicos. También es considerado como tal en nuestro derecho en la Constitución de la República, arts. 7°, 29 y 72, así como en el art. 1° de Ley N° 18.381 que se analiza.

El derecho de acceso a la información que se garantiza en esta Ley, refiere a la libre circulación y conocimiento por parte de todas las personas, de aquella información pública generada tanto en el ámbito de la administración pública estatal, como en organismos públicos no estatales, que no se encuentre sujeta a alguna restricción legal prevista en la Ley.

Debido a ello, la Ley en el art. 3° establece que es "un derecho de todas las personas, sin discriminación por razón de nacionalidad o carácter del solicitante, y que se ejerce sin necesidad de justificar las razones por las que se solicita la información".

¿Qué significa esto?

a) Que atendiendo al principio de no discriminación que expresamente recoge la norma, cualquier interesado o cualquier persona, ya sea física o jurídica, puede formular una petición de acceso a información pública ante un sujeto obligado.

b) Que tampoco se distingue en razón de la nacionalidad o carácter del solicitante, o sea entre ser ciudadano o ser extranjero y ello es así porque estamos ante un derecho fundamental inherente a la personalidad humana.

---

[178] "Todo individuo tiene derecho a...investigar y recibir informaciones y opiniones, y el de difundirlas...".(Artículo 19 de la Declaración Universal de los Derechos Humanos). "Toda persona tiene derecho a la libertad de expresión; ... la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, ...". (Artículo 19 del Pacto de Derechos Civiles y Políticos). "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ...". (Artículo 13 de la Convención Americana de Derechos Humanos). "Es enteramente libre en toda materia la comunicación de pensamientos por palabras, escritos privados o publicados en la prensa, o por cualquier otra forma de divulgación...". (Artículo 29 de la Constitución Nacional).

c) Que no es necesario explicitar el motivo por el cual se pretende el acceso, ni exponer acerca de cuál es el interés que se posee en esa información, así como tampoco explicar para qué se va a utilizar la misma. Esto básicamente es así porque se trata de acceder a información pública, o sea que si es pública es de acceso libre lo que en definitiva significa que no hay que acreditar interés alguno.

Por ende, "(...) las facultades jurídicas que se integran en el derecho a la información son básicamente tres: la facultad de investigar, la facultad de difundir y la facultad de recibir información. Y (...) toda persona es titular de "todo el derecho a la información, comprendidas sus tres facultades" (Desantes; 1986)"[179].

La regulación de este aspecto, también se relaciona con uno de los caracteres que posee el derecho de acceso a la información pública, que es considerado un derecho humano con una doble dimensión jurídica: como derecho individual que poseen todas las personas y como derecho colectivo que posee la sociedad en su conjunto.

En definitiva, "el derecho de acceso a la información pública implica la concreción del derecho a la libertad de expresión, entendido éste en toda su amplitud y extendido a lo que hoy llamamos Derecho a la Información, que comprende tanto la facultad de dar como de recibir información, y cuyo ejercicio corresponde a toda persona: al "sujeto universal", a todos y cada uno de nosotros"[180].

3.2. La solicitud y sus requisitos

Para ejercer este derecho el interesado deberá presentar una solicitud escrita ante el organismo que posee la información a la que desea acceder.

Al respecto, el art. 13 de la Ley establece que toda persona física o jurídica interesada en acceder a la información pública en poder de los sujetos obligados, deberá hacerlo mediante solicitud escrita ante el titular del organismo.

Dicha solicitud deberá contener:

a) la identificación del solicitante, su domicilio y una forma de comunicación (teléfono, correo electrónico),

b) la descripción clara de la información que se está solicitando y cualquier otro dato que el interesado conozca y que desee proporcionar para contribuir a su ubicación.

El artículo agrega además que, en forma opcional se puede establecer en la solicitud, en que soporte se desea recibir la información (papel, CD, etc.), pero

[179] FUENMAYOR ESPINA, Alejandro. Ob. Cit., pág.15
[180] BASTONS, Jorge Luis y ELIADES, Analía. Obra. Citada.

ello no obligará al organismo requerido ya que en definitiva podrá entregar la información en el soporte que desee o en el que le sea más conveniente.

En definitiva la Ley no exige mayores formalidades, pues el objetivo es que este primer paso, no se constituya en un obstáculo para el ejercicio del derecho, sino que sólo se trata de identificar al interesado, de mantener un canal de comunicación, así como de dejar constancia de la información que se solicita y de cuándo se ha solicitado, pues a partir de la fecha de recepción de la petición comienzan a correr los plazos que establece la Ley para brindar la respuesta.

4. OBLIGACIONES ATRIBUIDAS A LOS SUJETOS OBLIGADOS

4.1. Relacionadas con el derecho de acceso

Una vez recibida la solicitud por escrito, el organismo requerido deberá darle el trámite correspondiente. La obligación más importante que deriva de este derecho es justamente, brindar el acceso a la información que se ha solicitado en los términos y condiciones que establece la Ley, por ello es que se considera falta grave la negativa de cualquier funcionario a proveer la misma según lo establecido en el artículo 18 in fine.

Para satisfacer adecuadamente este derecho, también deberán respetarse los plazos y formalidades que establece la Ley. Al respecto el art. 15 de la Ley establece que “ante la petición formulada por el interesado, el organismo requerido está obligado a permitir el acceso o, si es posible, contestar la consulta en el momento en que se ha solicitado. En caso contrario tendrá un plazo máximo de veinte días hábiles para permitir o negar el acceso o contestar la consulta. El plazo podrá prorrogarse, con razones fundadas y por escrito por otros veinte días hábiles si median circunstancias excepcionales”.

Es de destacar que la norma, recoge la posibilidad de que la respuesta se brinde en el mismo momento en que se formula la petición. Ello puede ser posible en aquellos casos en que la información está disponible y es de muy fácil ubicación, de tal forma que hace posible que el funcionario la entregue en el momento.

Lo anterior se vincula a lo expresado en el art. 17 que expresa que: “en caso que los sujetos obligados resuelvan favorablemente las peticiones formuladas, autorizarán la consulta de los documentos pertinentes en las oficinas que determinen o, en su caso, expedirán copia auténtica de los antecedentes que posean relativos a la solicitud”.

La realidad indica que en la mayoría de los casos lo anterior no es posible debido a que no es tan sencillo ubicar y preparar la información a efectos de brindar el acceso. Generalmente entonces, se recibe la solicitud por escrito, luego se ubica la información, se hace copia de la misma a efectos de entregarla y posteriormente se notifica al interesado para que se presente a retirarla, dentro del plazo de veinte días hábiles.

En definitiva, el funcionario debe recepcionar la solicitud de acceso, explicar el trámite al interesado, dejar constancia de la fecha de recepción y brindar el acceso dentro del plazo previsto en la norma, entregando la información en forma completa y en un formato claro y comprensible para el solicitante.

Al respecto también, hay que tener presente el art. 15 de la Ley que hace mención expresa a las obligaciones que se le imponen al "organismo requerido", o sea a los organismos públicos, estatales o no. Entre esas obligaciones, está la de responder en plazo una solicitud de acceso, o de lo contrario establecer una prórroga de 20 días fundando la decisión.

Esta prórroga es viable en aquellos casos en que no es posible brindar el acceso dentro del plazo de veinte días, debido a que no se ubica fácilmente la información solicitada, o a que la misma debe ser recopilada o compilada. El organismo, mediante resolución fundada deberá determinar que se acoge a la prórroga de 20 días y esta resolución deberá ser notificada al interesado.

Si se resuelve no brindar acceso a la información solicitada, ya sea porque la misma es información secreta, reservada o confidencial, de acuerdo a lo expresado en los arts. 8°, 9° y 10 de la Ley, también se deberá informar por escrito al interesado, notificándole la resolución que indica el fundamento legal que se esgrime.

A su vez, el art. 16 establece respecto a la competencia para decidir, que "El acto que resuelva sobre la petición deberá emanar del jerarca máximo del organismo o quien ejerza facultades delegadas (...)"

El art. 18 por su parte, establece que: "El organismo requerido sólo podrá negar la expedición de la información solicitada mediante resolución motivada del jerarca del organismo (…)".

Armonizando el contenido de los mencionados artículos se infiere que:

a) Es competencia del sujeto obligado decidir sobre la petición y sobre la eventual prórroga de 20 días hábiles que permite duplicar el plazo para poder recabar la información y entregarla en forma debida a quien la solicite.

b) La prórroga debe fundarse y realizarse por escrito según el art. 15 in fine, debe estar firmada por el jerarca o por quien ejerza funciones delegadas según el art. 16, y luego ser notificada al solicitante según lo establecido en el art. 18.

Por su parte, el art. 17 establece también que, "el acceso a la información será siempre gratuito, pero su reproducción en cualquier soporte será a costa del interesado, quien reintegrará al organismo únicamente el precio de costo del soporte, sin ningún tipo de ganancia o arancel adicional".

Esto significa entonces que, los organismos obligados a brindar acceso a la información pública no pueden cobrar ya que el trámite es gratuito. La Ley sólo prevé que el solicitante cubra los gastos de reproducción de la información que

se solicita, sin ningún tipo de ganancia o arancel, en consonancia con el principio de gratuidad.

Otra obligación importante a tener en cuenta, es que los organismos obligados deben entregar la información que se les ha solicitado, en forma completa para satisfacer adecuadamente el derecho del solicitante y a su vez, la misma debe estar en un formato comprensible a efectos de que al interesado realmente le sea de utilidad.

Por su parte, el artículo 694 de la Ley N° 16.736, de 5 de enero de 1996, establece que "las administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administrados el pleno acceso a las informaciones de su interés". Esto habilita a que los organismos, progresivamente implementen mecanismos adecuados para recibir y responder solicitudes de acceso a la información online, además de las obligaciones que ya se prevén en el art. 5° de la Ley.

En definitiva, el derecho de acceso a la información pública, "debe ser satisfecho de la manera más rápida, sencilla y eficiente posible. Una forma de orientar al solicitante es difundir a través de su sitio Web el procedimiento mediante el cual puede realizar el trámite. Existen diferentes formas de instrumentar el procedimiento, una de ellas puede ser tener la solicitud en línea y otra por ejemplo podría ser publicar los formularios de solicitud para que cualquier usuario los pueda descargar y utilizar"[181].

A su vez, es importante tener presente que la Ley recoge otras formas para garantizar y favorecer el ejercicio del derecho de acceso a la información pública. De acuerdo con art. 5° los organismos públicos deben informar a través de sus páginas Web según lo dispone la norma. Esto es lo que se denomina transparencia activa, tema que es desarrollado específicamente en el Capítulo XII.

También los organismos, pueden brindar acceso a través de otros formatos físicos (folletos, CD, fotocopias) que pueden estar disponibles en forma permanente y actualizada en sus oficinas y ser accesibles al público en forma directa.

4.2. Relacionadas con los archivos

Como ya se había expresado supra, la información pública debe concebirse como un bien público común, por ende debe ser clasificada, ordenada, preservada y cuidada como tal y la Ley también impone específicamente obligaciones relacionadas con este tema.

---

[181] AGESIC. Guía para diseño e implementación de Portales Estatales. Capítulo IV. Normativa, pág. 247. http://www.agesic.gub.uy/innovaportal/file/549/1/Capitulo_4_Normativa_v1_0.pdf Página visitada el 15 de julio de 2010.

En este sentido, los organismos públicos deben tener la información que producen, crean o controlan, ordenada y organizada de manera profesional, independientemente del soporte en el que se encuentre. De esta forma además, se será más eficiente a la hora de garantizar el derecho porque será más fácil, ordenado y efectivo el trabajo que lleven adelante los funcionarios.

En el art. 6° inc. 1, la Ley establece que es responsabilidad de los sujetos obligados, crear y mantener registros de manera profesional, para que el derecho de acceso a la información pública se pueda ejercer en plenitud.

Por otra parte, es muy importante tener en cuenta que el art. 6° inc. 2 establece que "el personal que administre, manipule, archive o conserve información pública, será responsable, solidariamente con la autoridad de la dependencia a la que pertenece dicha información, por sus acciones u omisiones, en la ocultación, alteración, pérdida o desmembración de la información pública".

En resumen, la forma en que se organiza y preserva la información es un presupuesto fundamental para una gestión eficiente, así como para garantizar el ejercicio efectivo del derecho de acceso a la información.

Esto es así porque, "el gobierno es la principal fuente de información y la manera en que dispone de ella determina en gran medida los cambios sociales y económicos del país. Por esa razón, la gestión sistemática de documentos, sin ser un fin en sí, es un requisito indispensable para una auténtica democracia. Toda Administración sólida y documentada también debe poner esta información al alcance del público" [182].

Al respecto hay que tener presente que la Ley Nº 18.719,[183] de 27 de diciembre de 2010, en su artículo 151 amplió el plazo para que los organismos adecuen sus registros. Al respecto establece que dispondrán de un plazo de cuatro años desde la aprobación de la Ley Nº 18.381; se entiende que se les ha otorgado hasta el año 2012 para que adecuen sus archivos, plazo durante el cual no serán pasibles de sanción en caso de denegación de acceso fundados en la imposibilidad de ubicar la información.

4.3. Relacionadas con el Órgano de Control (UAIP)

La Ley ha previsto la creación de la Unidad de Acceso a la Información (UAIP) como órgano de control. Debido a ello, también prevé una serie de obligaciones a cargo de todos los sujetos obligados para con este nuevo organismo.

En el art.7° establece que deberán elaborar y presentar ante la UAIP, los siguientes informes:

- Un informe anual sobre el cumplimiento del derecho de acceso a la información pública, que deberá tener el siguiente contenido: Información del período anterior sobre el cumplimiento de las

[182] Información y Gobernabilidad. Documento de Orientación. Ob. Cit. http://www.deza.admin.ch/es/Pagina_principal/Documentacion/Publicacion

[183] Ley Nº 18.719,de 27 de diciembre de 2010, Presupuesto Nacional, Período 2010 – 2014

obligaciones previstas en la Ley y detalle de las solicitudes de acceso a la información y el trámite dado a cada una de ellas. Este informe deberá ser presentado hasta el último día hábil del mes de marzo de cada año.

- Un informe semestral actualizado con el listado de la información que el organismo ha clasificado como reservada.

Es de destacar que en la UAIP se han elaborado formularios para la presentación de ambos informes que se encuentran disponibles en su página web[184].

5. LÍMITES AL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

5.1. Breve reseña de las excepciones

El derecho de acceso a la información pública admite restricciones legítimas, adecuadas y proporcionales a la finalidad que se persigue.

Al respecto el art. 29 de la Declaración Universal de Derechos Humanos expresa que el ejercicio de los derechos y de las libertades de las personas, sólo podrán estar sujetos "(…) a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás y de satisfacer las justas exigencias de la moral, el orden público y el bienestar general en una sociedad democrática".

Actualmente se considera que, "en las relaciones del Estado con sus ciudadanos, se debe considerar superada la concepción del secreto de la Administración (...), y además por la naturaleza constitucional y universal del derecho a la información, la libertad es la regla y el secreto la excepción"[185].

Por ello, los límites al derecho de acceso a la información pública deben ser mínimos y de interpretación estricta, y entre ellos se encuentran las excepciones previstas en los arts. 8°, 9° y 10 de la Ley N° 18.381 las que serán objeto de un análisis más profundo en el Capítulo XIII.

Además, es importante tener presente que las mencionadas restricciones, -por constituirse en limitaciones que se imponen a un derecho fundamental-, deben estar establecidas en una Ley en sentido formal y material[186].

---

[184] http://www.informacionpublica.gub.uy/sitio/documentacion.html Página visitada el 15 de julio de 2010

[185] Información y Gobernabilidad. Documento de Orientación. http://www.deza.admin.ch/es/Pagina_principal/Documentacion/Publicacion Página visitada el 15 de julio de 2010.

[186] El artículo 30 de la Convención de Derechos Humanos de la OEA señala que "las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a las leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas". La Corte Interamericana agrega que "también es razonable sostener que la palabra "ley" incorpora asimismo el requisito de "generalidad", es decir, de ley en un sentido material. Cualquier otra interpretación de la palabra sería contraria al artículo 1.1 de la Convención, que establece un principio general de no discriminación."

El art. 8° de la Ley expresa que “las excepciones al acceso a la información pública serán de interpretación estricta y comprenderán aquéllas definidas como secretas por la ley y las que se definan como de carácter reservado y confidencial”.

Los titulares de los organismos obligados, serán responsables de clasificar la información de conformidad con lo establecido en la ley y deberán observar, tanto en la interpretación como en la aplicación de la ley el principio de máxima publicidad y transparencia que inspira a toda la norma.

Los organismos requeridos sólo pueden negar el acceso en aquellos casos que señala la Ley, mediante resolución fundada que debe indicar que la información solicitada es secreta, reservada o confidencial de acuerdo con las disposiciones legales que se deben explicitar (Arts. 8°, 9°, 10 y 18).

La motivación, - incluida en la resolución que debe emanar del jerarca máximo- , y la indicación del fundamento legal, son elementos imprescindibles para evaluar que dicha reserva obedece a criterios legales, objetivos y verificables, y no simplemente a motivos personales o arbitrarios pertenecientes al funcionario de turno.

Este concepto, es reforzado por lo establecido en el art. 16 de la ley, cuando se expresa que: "(...) deberá franquear o negar el acceso a la información que obrare en su poder relativa a la solicitud en forma fundada".

En este sentido, es claro que el Estado puede reservar temporalmente cierta información por razones de interés público, de acuerdo con las hipótesis mencionadas en el art. 9° de la Ley, pero esa clasificación debe ser hecha a través de una resolución fundada, en la que se pongan en consideración elementos objetivos y verificables, (procedimiento conocido en el derecho comparado como “prueba de daño”), que permitan evaluar el eventual daño que se causaría al interés público protegido.

La Ley además establece que el período máximo de reserva es de 15 años, según lo establecido en el art. 11, desde la fecha en que la información ha sido clasificada, pero que puede ser desclasificada antes de ese período si las causas que dieron origen a la reserva desaparecen. Si al cabo de 15 años las causas se mantienen, el plazo puede extenderse.

En cambio, tanto en lo que hace a la información secreta como a la confidencial, la Ley no señala plazos para ser desclasificadas.

Los sujetos obligados tampoco deben permitir el acceso a las secciones o documentos que contengan información secreta, reservada o confidencial, pero sí pueden permitir el acceso a las secciones o partes que no lo son, de acuerdo con el principio de divisibilidad. Esta posibilidad favorece en definitiva el ejercicio del derecho de acceso, ya que habilita a que los interesados puedan acceder a la información a pesar de que existan partes o secciones que se encuentran clasificadas.

Por otro lado hay que tener presente también, que hay casos donde la norma expresamente indica que no se pueden oponer excepciones al acceso. Estos casos refieren a violaciones a los derechos humanos o cuando la información sea relevante para prevenir o evitar violaciones a los mismos, según lo dispuesto en el art.12.

Creemos que la norma recoge la trascendencia que en la actualidad posee la protección integral de los derechos humanos, cuya tutela y garantía configura una cuestión de interés público en un Estado de Derecho.

En definitiva cuando se está ante las hipótesis que prevé la norma, el Estado, como principal garante de los derechos humanos, no puede negar el acceso fundamentándose en las excepciones previstas en la Ley.

5.2. Análisis del art.14

Otro límite que se presenta al derecho de acceso está previsto en el art. 14 de la norma.

Si bien el art. 2° de la Ley establece que es "información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal (...), el art. 14 delimita el alcance de lo anterior, en el sentido de que la solicitud de acceso no implica la obligación de los sujetos obligados de crear o producir información que no dispongan o no tengan obligación de poseer al momento de efectuarse el pedido.

Además, se establece que la Ley no faculta a los peticionarios a exigir a los organismos que efectúen evaluaciones o análisis de la información que poseen, salvo aquellos casos en que esto sea parte de sus cometidos institucionales.

Es pertinente tener en cuenta que, el silencio o el vencimiento de los plazos siempre perjudica al organismo, por ende corresponde que se comunique por escrito al interesado (dentro de los plazos legales), que la denegación obedece a la inexistencia en su poder de la información solicitada.

También hay que considerar lo expresado en la última parte del art. 14, respecto a que no se considera producción de información, a la recopilación o compilación de información que estuviese dispersa en las diversas áreas del organismo.

Esta previsión legal es muy importante y tiene como finalidad, evitar que los funcionarios utilicen este argumento para no brindar acceso cuando corresponde que se garantice el derecho, pues es claro que en este caso deben invertir tiempo y esfuerzo en buscar la información dispersa entre las diferentes dependencias del organismo para compilarla a efectos de brindar el acceso.

6. PLAZOS PARA ENTREGAR LA INFORMACIÓN SOLICITADA

6.1. Análisis del art. 15

Según este artículo los sujetos obligados disponen de 20 días hábiles a contar desde la recepción de la solicitud para brindar acceso a la información que le ha sido solicitada.

Si por motivos excepcionales, ya sea porque es un volumen importante de información, porque es difícil de ubicar, porque hay que compilarla, porque hay que elaborar una “versión pública” a efectos de proteger información confidencial, no se puede cumplir con el plazo anterior, el organismo puede decidir acogerse a la prórroga de 20 días hábiles que establece la Ley ya sea para negar o para brindar acceso. Esa decisión debe fundamentarse y establecerse mediante resolución fundada que será notificada al interesado.

Según lo expresado en este artículo, también el organismo puede entregarla en el momento mismo de la solicitud (en aquellos casos en que se dispone en forma inmediata de la información) de lo contrario, comienza a correr el plazo de 20 días para permitir o negar el acceso en el caso de que sea información secreta, reservada o confidencial, en consonancia con el principio de oportunidad.

6.2. La hipótesis de "silencio positivo" del art. 18

De lo anterior surge que, según las obligaciones establecidas en la Ley N° 18.381 el organismo dispone de 20 días hábiles para permitir el acceso ya sea en la propia oficina, o para entregar copia, de lo contrario deberá establecer una prórroga para contar con otros 20 días hábiles.

Respecto a la obligación de responder a las solicitudes de acceso a la información dentro del plazo de 20 días, también hay que tener en cuenta lo que establece el art. 18 inc. 2° de la Ley : "vencido el plazo de veinte días hábiles desde la presentación de la solicitud, si no ha mediado prórroga o vencida la misma sin que exista resolución expresa notificada al interesado, éste podrá acceder a la información respectiva, considerándose falta grave la negativa de cualquier funcionario a proveérsela (...)".

La Ley en definitiva establece un plazo para responder a la solicitud de acceso y la consecuencia del vencimiento de ese plazo, sin solicitud de prórroga, es lo que se denomina "silencio positivo". Ello significa según la misma norma, que ante el vencimiento de dicho plazo se "podrá acceder a la información" que se ha solicitado.

Esto tiene como consecuencia además, que la información, -que no estaba clasificada como reservada al momento de la solicitud-, ya no puede clasificarse como reservada pues el interesado tiene derecho a reclamar el acceso.

Este punto también nos indica la importancia que tiene para los organismos públicos, una correcta y oportuna clasificación de la información, tal como lo establece el art. 33 de la Ley[187]

7. LA ACCIÓN DE ACCESO A LA INFORMACIÓN PÚBLICA

7.1. Procedencia

El solicitante también tiene derecho a presentarse ante la justicia si su derecho de acceso a la información pública, no es satisfecho de acuerdo con las previsiones legales.

Al respecto es importante señalar que, esta acción también es conocida como Habeas Data Impropio y la diferencia con el Habeas Data propiamente dicho radica en que este último es una garantía procesal que permite ejercer el derecho que cada persona posee a conocer los datos que sobre si mismo se poseen tanto en el ámbito privado como en el público.

El Habeas Data Impropio en cambio, como señala Puccinelli "no está dirigido a la protección de datos de carácter personal asentados en bases o bancos de datos, sino a obtener información pública que le es indebidamente negada al legitimado activo"[188].

La Ley N° 18.381 en el art. 22 establece que "toda persona tendrá derecho a entablar una acción judicial efectiva que garantice el pleno acceso a las informaciones de su interés".

Esta acción por lo tanto, procede contra todo organismo público, estatal o no, que se niegue a expedir la información que se le ha solicitado o que permita acceder a la misma fuera de los plazos previstos en la Ley, según lo establecido en el art. 23).

7.2. Competencia y legitimación

En Montevideo son competentes para conocer en estas acciones los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo cuando la acción de acceso a la información pública se presenta contra una persona pública estatal, y son competentes los Juzgados Letrados de Primera Instancia en lo Civil cuando la acción se interpone contra organismos públicos no estatales. En el interior del país tienen competencia los Juzgados Letrados de Primera Instancia según se expresa en el art.23.

---

[187] El plazo previsto en el artículo mencionado ha sido modificado por el art. 150 de la Ley 18.719 de 27 de diciembre de 2010, que dispone que al 31 de julio de 2012 todos los sujetos obligados deberán elaborar la lista de la información que a la fecha se encuentre clasificada como reservada según los nuevos parámetros legales, así como desclasificar toda aquella que no se sujete a las excepciones previstas en la norma, o tenga más de quince años de clasificada como reservada.

[188] PUCCINELLI, Oscar. Tipos y subtipos de hábeas data en América Latina. Editorial Astrea, 2004. http://www.iprofesional.com/adjuntos/documentos/08/0000887.pdf. Página visitada el 21 de junio de 2010.

De acuerdo con el art. 24 en tanto, la acción podrá ser ejercida por cualquier interesado que haya solicitado acceder a determinada información y no haya recibido respuesta por parte del organismo, o éste se haya expedido fuera de plazo.

También puede ser ejercida por sus representantes, ya sean curadores o tutores y en caso de personas fallecidas, por los sucesores universales en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado.

En el caso de las personas jurídicas, esta acción deberá ser interpuesta por medio de los representantes legales o apoderados designados a tales efectos, según lo expresado por el art. 24.

7.3. Aspectos procesales

Los estándares internacionales en materia de acceso a la información pública, indican que para garantizar efectivamente este derecho, es necesario contar con un procedimiento judicial sencillo, rápido y efectivo.

En el mismo sentido nuestra Ley, ha establecido un procedimiento muy similar al amparo y con plazos muy breves. Al respecto el art. 25 dispone que, en todo lo pertinente serán aplicables los arts. 14 y 15 de la Ley N° 15.982 aprobatoria del Código General del Proceso.

Estos artículos del Código General del Proceso establecen que, "para interpretar la norma procesal, el tribunal deberá tener en cuenta que el fin del proceso es la efectividad de los derechos sustanciales. En caso de duda se deberá recurrir a las normas generales teniendo presente los principios generales de derecho y especiales del proceso y la necesidad de preservar las garantías constitucionales del debido proceso y de la defensa en el mismo".

A su vez, en "caso de vacío legal, se deberá recurrir a los fundamentos de las leyes que rigen situaciones análogas y a los principios constitucionales y generales de derecho y especiales del proceso y a las doctrinas más recibidas, atendidas las circunstancias del caso".

Debido a la sumariedad del proceso consagrado por la Ley N° 18.381 -que atiende a la efectividad del derecho sustancial tal como lo expresa el Código General del Proceso en el art. 14 que hemos analizado- no se podrán deducir cuestiones previas, reconvenciones o incidentes, quedando en manos del Juez la posibilidad de subsanar los vicios del procedimiento siempre que asegure el principio del contradictorio.

Por su parte, en el trámite específico previsto en los arts. 25 y siguientes, se establece que, salvo que la acción fuera manifiestamente improcedente en cuyo caso el Juez podrá rechazarla y disponer el archivo, se deberá convocar a una audiencia pública dentro del plazo de tres días a contar desde la fecha en que se presentó la demanda.

El Juez deberá presidir la audiencia so pena de nulidad, y durante la misma se escucharán las explicaciones del organismo denunciado y se recibirán las pruebas. El tribunal podrá rechazar aquéllas que sean manifiestamente impertinentes o innecesarias. También deberá interrogar a los testigos y a las partes, así como podrá diligenciar pruebas y adoptar medidas provisionales según lo previsto en el art. 27 y subsanar vicios de procedimiento según el art. 30, pues cuenta con amplias facultades y poderes para ello de acuerdo a lo establecido en el art. 26.

La sentencia deberá ser dictada en la audiencia, o a más tardar dentro de las veinticuatro horas de celebrada ésta, y sólo en casos excepcionales, la Ley habilita que la audiencia pueda prorrogarse por hasta tres días.

Según lo establecido en el art. 28, la sentencia que haga lugar a la acción deberá identificar a la autoridad o al particular a quien se dirige, debido a su acción, hecho u omisión, a efectos de garantizar el derecho que consagra la Ley.

También deberá determinarse en la misma, en forma precisa, qué es lo que debe o no hacerse, así como el plazo por el cual dicha resolución regirá,- si es que debe fijarse-, y por último, el Juez deberá establecer que plazo otorga, -según las circunstancias de cada caso-, para cumplir con lo dispuesto en la sentencia.

Es importante tener presente, que este plazo no deberá exceder los 15 días corridos e ininterrumpidos, a contar desde la notificación de la sentencia.

En cuanto a la posibilidad de apelar, el art. 29 establece que en el proceso sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente. Este recurso deberá interponerse por escrito y en forma fundada, dentro del plazo perentorio de 3 días.

La interposición de los recursos no suspende las medidas de amparo que hayan sido decretadas, las cuales deben ser cumplidas en forma inmediata después de notificada la sentencia, independientemente del resultado de los mismos.

Si el Juez ha desestimado la acción por manifiestamente improcedente, deberá elevar el recurso en forma inmediata al superior, o de lo contrario lo sustanciará dando traslado a la contraparte por otros tres días perentorios, cuando lo que se ha apelado es la sentencia definitiva.

Establece la Ley además, el plazo para que el Tribunal de Alzada resuelva. En este caso podrá disponer de cuatro días contados a partir de la recepción de los referidos autos.

8. RESPONSABILIDADES Y SANCIONES

El art. 31 enumera una serie de situaciones o hipótesis, que de verificarse, darían origen a la responsabilidad administrativa del funcionario o funcionarios

involucrados, sin perjuicio de las responsabilidades civiles y penales que también pudieran ser imputadas a los mismos.

En definitiva se incurre en responsabilidad cuando:

- Se deniegue la información que se ha solicitado y la misma no se encuentra clasificada como reservada o como confidencial, o sea cuando no hay fundamento legal para negar el acceso.
- Se omite entregar parte de la información o se suministra la misma en forma parcial, actuando con negligencia, dolo o mala fe. En este caso no se ha satisfecho adecuadamente el derecho de acceso.
- Se brinda acceso injustificado a información que se encuentra clasificada como reservada o confidencial y en definitiva se vulneran intereses del Estado o de los particulares.
- Y por último, también se incurre en responsabilidad si se sustrae, se oculta, se divulga o se altera total o parcialmente en forma indebida, la información que se encuentra bajo custodia, o aquélla a la que se accede por razones de la función que se cumple.

Como ya lo habíamos mencionado supra, estas responsabilidades se generan debido a que la Ley impone obligaciones relacionadas con el manejo de la información, con la conservación y organización profesional y responsable de los archivos del Estado, según lo establecido en el art. 6 porque en definitiva la información pública debe ser custodiada y protegido adecuadamente en beneficio de todos.

Por otra parte, toda la información en poder de los organismos públicos, sean estatales o no, se presume pública y como tal debe ser entregada a los solicitantes, salvo que se encuentre dentro de las excepciones previstas en la ley: información clasificada como secreta por Ley, reservada o confidencial. Pero para negar el acceso, la Ley también ha previsto un procedimiento que debe ser seguido por los funcionarios a efectos de actuar en forma responsable y adecuada. Por ello es que también es muy importante clasificar correctamente la información, tal como se explica en el Capítulo VIII.

Por último, hay que recordar que en el art. 18 se considera falta grave, de acuerdo con lo previsto por la Ley N° 17.060, la negativa de cualquier funcionario a proveer la información cuando el organismo no ha contestado dentro de los plazos establecidos, y por ende se ha configurado lo que se denomina “silencio positivo”.

En definitiva, los sujetos obligados deben brindar acceso a la información pública a todas las personas por igual, de la manera más completa, adecuada, oportuna y veraz que sea posible, salvo que se establezca en forma fundada, que la información solicitada cae dentro del régimen de las excepciones establecidas en la Ley.

9. CONCLUSIONES

La Ley N° 18.381 de Acceso a la Información Pública en general, recoge los principales estándares internacionales en la materia y su aprobación debe considerarse un paso trascendente para nuestro país.

Este avance debe ser visto como parte de un proceso más amplio de cambios, que deben producirse tanto a nivel de la sociedad en su conjunto como a nivel del funcionamiento del Estado, y para ello es necesario e imprescindible que exista voluntad política por parte de las autoridades y de los sujetos obligados de garantizar los derechos previstos en la ley.

La experiencia internacional también indica, que es beneficioso para este tipo de proceso, que los ciudadanos se informen y adquieran conciencia acerca de la potencialidad que posee el ejercicio responsable de este derecho, así como que los funcionarios y la administración en general, se capacite y se prepare adecuadamente para asegurar el éxito de una política pública de transparencia y acceso a la información.

CAPÍTULO X- EL DECRETO N° 232/010

Dra. Rosario Ierardo

1. INTRODUCCIÓN

Con fecha 17 de octubre de 2008 se promulgó en Uruguay la Ley de Acceso a la Información Pública cuyo artículo 35 establece como debe realizarse su reglamentación.

Para la redacción del Anteproyecto fue consultado el Instituto de Derecho Informático de la Facultad de Derecho de la Universidad Mayor de la República Oriental de Uruguay, y el Centro de Archivo y Acceso a la Información Pública (CAinfo), que actuó como contraparte representando a la sociedad civil.

Respecto a la participación de la sociedad civil como interesado, la Asamblea General de la OEA en el plenario "Acceso a la Información Pública: Fortalecimiento de la Democracia", del 3 de junio de 2008, resolvió: "Alentar, asimismo, a los Estados miembros a que, cuando elaboren o adapten, de ser el caso, los respectivos marcos jurídicos normativos, brinden a la sociedad civil la posibilidad de participar en dicho proceso e instar a los estados miembros a que, cuando elaboren y adapten su legislación nacional, tengan en cuenta criterios de excepción claros y transparentes."[189]

En la reglamentación de la Ley Nº 18.381, se destaca la importancia de garantizar el ejercicio del derecho de acceso a la información pública estableciendo claramente las excepciones. Asimismo reconoce al derecho de acceso a la información pública como herramienta para el desarrollo y fortalecimiento de la democracia.

Con fecha 2 de agosto del 2010 el Proyecto de Decreto que Reglamenta la Ley N° 18.381 es aprobado y publicado con el N° 232/2010.

2. ÁMBITO DE APLICACIÓN

2.1 Ámbito objetivo

El Decreto Reglamentario se aplica a todas las personas públicas sean o no estatales, que son los sujetos obligados a efectos de la Ley de Acceso a la Información Pública. Las personas estatales son: Poder Ejecutivo, Poder Judicial, Poder Legislativo, Entes Autónomos, Servicios Descentralizados, Órganos de Contralor y Gobiernos Departamentales.
Las personas públicas no estatales son: Caja de Jubilaciones y Pensiones Bancarias, Cooperativa Nacional de Productores de Leche (CONAPROLE), Caja Notarial de Jubilaciones y Pensiones, Caja de Jubilaciones y Pensiones de Profesionales Universitarios, Fondo para la Erradicación de la Vivienda Rural Insalubre (MEVIR), Laboratorio Tecnológico del Uruguay (LATU),Consejo

[189] Tomado de http://www.oas.org/dil/esp/AG-RES_2418_XXXVIII-O-08_esp.pdf, página visitada el 17 de agosto de 2011.

de Capacitación Profesional (COCAP), Instituto Nacional de Carnes (INAC), Fondo Nacional de Recursos (Comisión Honoraria Administradora), Corporación Nacional para el Desarrollo (CND), Comisión Honoraria para la Lucha Antituberculosa y Enfermedades Prevalentes, Instituto Nacional de Vitivinicultura (INAVI), Instituto Nacional de Investigación Agropecuaria (INIA), Comisión Honoraria de Lucha contra el Cáncer, Comisión Honoraria para la Salud Cardiovascular, Instituto de Promoción de la Inversión y las Exportaciones de Bienes y Servicios, Instituto Plan Agropecuario, Dirección Nacional de Impresiones y Publicaciones Oficiales(IMPO), Comisión Honoraria Administradora del Fondo de Solidaridad, Comisión del Fondo Nacional de Música, Instituto Nacional de Semillas (INASE), Administración del Mercado Eléctrico (ADME), Fondo de Solidaridad, Servicio de Retiros y Pensiones de las Fuerzas Armadas, Agencia Nacional de Desarrollo, Instituto Nacional de Calidad INACAL), Instituto Nacional de la Leche, Fondo de Cesantía y Retiro de la Construcción, Fondo de Seguro de Salud de Funcionarios y Ex Funcionarios de OSE, Colegio Médico del Uruguay.

2.2 Ámbito subjetivo

El artículo 3° del Decreto Reglamentario establece el ámbito subjetivo, indicando que todas las personas físicas y jurídicas tienen derecho de acceso a la información pública. El citado artículo reconoce la raigambre Constitucional del derecho, ya que no se admite discriminación de tipo alguno. Esta amplitud queda de manifiesto en el artículo 9º del Decreto Reglamentario, que consagra el principio de no discriminación del solicitante ya sea por su carácter o nacionalidad. También se puede ver reflejada en el artículo 6º donde se establece el principio de máxima publicidad de la información. Cuanto mayor sea la información que las entidades publiciten por sí a través de sus páginas web (transparencia activa), menor será la posibilidad de discriminación.

De hecho las entidades deben publicitar obligatoriamente cierta información actualizada a través de sus páginas web. El artículo 38 detalla la información, que debe publicarse, lo que será desarrollado en el Capítulo referente a la transparencia activa.

3. PRINCIPIOS GENERALES

El Decreto Reglamentario, en sus artículos 2º y 3º enumera los principios generales, nucleándolos como principios de la información y de los archivos.

Es fundamental el papel que juegan los principios generales, en un derecho humano como lo es el derecho de acceso a la información pública; que a su vez se convierte en herramienta para el ejercicio de otros derechos. La información pública es el insumo para la defensa y el ejercicio de los demás derechos humanos.

Según indica la Dra. Cristina Vázquez: “La transparencia absoluta es un bien público puro de importancia central en el sector público, donde no actúan los filtros naturales a los comportamientos contrarios a la ética que puede imponer la condición de mercado. Implica apertura, comunicación y rendición de

cuentas, y el acceso a la información pública constituye instrumento fundamental para su realización". Respecto al concepto de "bienes públicos puros", los define como "aquellos respecto de los cuales no es viable ni deseable racionar el uso".[190]

3.1 Principios referidos a la información

1-El principio de libertad de información indica que todas las personas tienen derecho a acceder a la información en poder de las entidades públicas salvo aquélla que encuadre dentro de las excepciones establecidas por la Ley Nº 18.381.

Como indicara la Dra. Laura Nahabetián en el capítulo VIII: "En efecto, la información debe existir en forma asequible, apropiada y tempestiva, ya que se trata de un presupuesto esencial para el desarrollo de una relación efectiva entre las personas y las diferentes entidades públicas. Este principio implicará, en consecuencia, que toda la información del Estado, debe estar disponible y sólo por excepción – siempre limitada – podrá negarse su accesibilidad".

2-El principio de transparencia entiende pública a toda la información en poder de los sujetos obligados, con las excepciones legales. Este principio reconoce el derecho de las personas de conocer la gestión de las entidades públicas. En las palabras del Dr. Carlos Delpiazzo: "Es que la transparencia se asocia a lo que es visible y accesible, a lo que puede ser conocido y comprendido, por contraposición a lo cerrado, misterioso, inaccesible o inexplicable. Igualmente, la transparencia se asocia a una carga afectiva ligada a la tranquilidad y serenidad provocada por todo aquello que se domina y racionaliza, por oposición a la angustia y perturbación de lo misterioso y desconocido. Además, del contraste entre las sombras y la luz, entre opacidad y transparencia, nacen nuevos métodos que tratan de referir el principio de legalidad, como límite y fundamento de la acción administrativa, al principio de consecución del interés público y del respeto por los derechos de los ciudadanos en el marco del bien común, métodos que tratan de promover los principios de colaboración ciudadana, de participación y de promoción de una nueva y diferente forma de concebir el poder administrativo más próximo a los ciudadanos".[191]
3-El principio de máxima publicidad obliga a las entidades a difundir la información pública de la manera más amplia posible. Este principio está ligado a la obligación de transparencia activa, que implica el publicitar determinada información sin la necesidad que ésta sea solicitada.

4-El principio de divisibilidad establece que si dentro de un documento existe información pública e información no pública, se debe permitir el acceso a la primera. Esto se logra creando lo que se conoce como "versión pública del documento". La versión pública elimina los párrafos donde se encuentra la información clasificada o confidencial haciendo referencia a la resolución de

---

[190] VÁZQUEZ, Cristina, "Saludable brecha en el secretismo administrativo", en www.ferrere.com. Página visitada 19 de agosto de 2011.
[191] DELPIAZZO, Carlos. La transparencia como antídoto para la corrupción, en www.periodicogobierna.com Número 8- Agosto de 2007. Página visitada el 10 de agosto de 2010.

clasificación. En caso de que el documento únicamente se posea en versión impresa y como criterio general, deberá fotocopiarse y sobre éste deberán testarse las palabras, párrafos o renglones que sean clasificados, y no entregar aquellas partes o secciones que tengan el mismo carácter. En caso de documento electrónico, deberá insertarse la palabra "Eliminado".

Las versiones públicas, además estarían incluidas dentro del principio de limitación de las excepciones, que es uno de los principios del derecho de acceso a la información pública. Es así que las excepciones deben tener como fundamento una Ley, y la consideración de las mismas es tan estricta, que dentro del mismo documento pueden existir partes no excepcionadas.

5-Se regula también por principio la falta de ritualismo a la hora de permitir el acceso a la información, sin que esto se contradiga con los requerimientos formales que debe tener una solicitud de acceso a la información, según el artículo 13 de la Ley Nº 18.381. Es natural que se haya optado por incluir este principio, si se tiene en cuenta que la información es un bien del público y no de los sujetos obligados.

Los sujetos obligados desempeñan el papel de depositarios de la información, pero no son sus dueños.

6-El artículo 9º establece el ya referido principio de no discriminación. En este punto se indica que la solicitud no es motivada, y tiene pocas formalidades, lo cual también evita posibles situaciones de discriminación. La información pública ya no se considera propiedad de cada organismo, sino "un bien común al que todos tenemos derecho", "y quienes trabajamos en la administración pública manejamos bienes, recursos e información pública en nombre de los ciudadanos o administrados".[192]

7-El principio de oportunidad indica el apego de la respuesta a lo solicitado y el acatamiento a los plazos de respuesta consignados en la precitada Ley. La solicitud se debe responder dentro de los 20 días hábiles siguientes a la formulación, o haciendo uso de la prórroga de 20 días hábiles. La prórroga debe ser fundada, y comunicada al solicitante.
8-El principio de responsabilidad hace pasibles de sanción a los sujetos obligados ante violaciones a la Ley. El incumplir la Ley conlleva sanciones. Las mismas son referidas en el artículo 58 del Decreto Reglamentario, y serán objeto de estudio en el punto 10.

9-Por último se reafirma el carácter gratuito del acceso a la información. Sólo se pueden trasladar al solicitante el costo de reproducción de la misma. Este principio se encuentra fuertemente enlazado con el de no discriminación, ya que supone que la situación económica de la persona no se convierta en una traba a la hora de ejercer su derecho.

3.2 Principios vinculados con los archivos

[192] ROMERO, Graciela. "Análisis del Decreto Nº 232/010 reglamentario de la Ley Nº 18.381 de Acceso a la Información Pública" en Anuario de Derecho Informático. Tomo XI. FCU, 2011.

El Decreto Reglamentario compila también principios sobre la gestión de archivos como un presupuesto para la accesibilidad de la información. La Ley Nº 18.220 de fecha 20 de diciembre de 2007, crea el Sistema Nacional de Archivo cuyo ámbito objetivo coincide con el del presente Decreto Reglamentario: todas las personas públicas estatales y no estatales. En la comparecencia ante el Parlamento de fecha 6 de junio de 2007, con motivo de la Ley N° 18.220, la Directora del Archivo General de la Nación, Alicia Casas expone: "Por último, hay un ítem que es muy importante, que es el referido al acceso a la información. Aquí se dice que toda persona tiene derecho al acceso a la consulta de documentos de los archivos públicos. Sin embargo, es imposible acceder a ellos, porque no están organizados, por lo que muchas veces vamos a pedir una información y nos contestan que no la tienen, cuando generalmente no es que no exista, sino que no está a mano; está, pero no se sabe dónde. Esto ocurre muy frecuentemente. Entonces, el acceso está limitado, en los hechos, por la organización de los documentos".[193]

El principio de disponibilidad establece que la información de los archivos debe ser entregada al solicitante con las excepciones legales. Este principio referido a los archivos es una arista del principio de libertad de la información.

Los principios de eficiencia, integridad y conservación fijan las pautas para que los documentos sean fácilmente localizables, se puedan conservar y sean eficientes económicamente. Los archivos constituyen la memoria de los sujetos obligados.

Mediante la organización profesional de esa memoria es que los sujetos obligados se vuelven verdaderos custodios de la información que es un bien público.

4. DEFINICIONES INCLUIDAS EN EL DECRETO REGLAMENTARIO

El Decreto Reglamentario incluye definiciones de expresiones que aparecen en la Ley Nº 18.381.

Se define como información a cualquier archivo, registro o dato contenido en cualquier medio, documento o registro impreso, óptico, electrónico, magnético, químico, físico o biológico que se encuentre en poder de los sujetos obligados.

Una de las definiciones clave para entender la Ley es la de clasificación.

Clasificar un documento como confidencial o reservado es fundamental para determinar si el mismo es o no entregable al solicitante. La clasificación es un acto administrativo motivado y fundado, responsabilidad del jerarca de cada entidades, según lo indica el Decreto Reglamentario en sus artículos 21 y 31.
Una vez clasificado el documento o parte del documento (en virtud del principio de divisibilidad de la información), se debe indicar, mediante una leyenda si la información es reservada o confidencial. De la misma manera se debe indicar

[193] CASAS, Alicia. Comparecencia ante la Cámara de Senadores. Disponible en: www.parlamento.gub.uy/distribuidos/AccesoDistribuidos.asp?Url=/distribuidos/caratulas/senado/s20071702.html Página visitada el 14 de agosto de 2011.

la fecha de la resolución de clasificación, la base legal para la misma y finalmente se estampa la firma del jerarca.

Los criterios de clasificación deben ser iguales para todos los sujetos obligados, dado que se trata de restringir el ejercicio de un derecho humano.

Asimismo se incluye la definición de los informes que deben presentar los sujetos obligados, que son detallados en el Título IV del Decreto Reglamentario.

Se define publicación como la reproducción en medios electrónicos o impresos de información contenida en documentos para su conocimiento público.

Es fundamental definir documento y expediente, dado que en varias normas se ofrecen distintas definiciones. Según el Decreto se entiende por documentos los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus funcionarios, sin importar su fuente o fecha de elaboración. Éstos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico. Se entiende por expediente el conjunto de documentos que tratan de un mismo asunto y que se forma siguiendo el ordenamiento regular de los documentos que lo integran, en forma sucesiva y por orden de fechas.

5. TIPOS DE INFORMACIÓN

El título II, capítulo II del Decreto Reglamentario refiere a la información reservada y el capítulo III a la información confidencial, como excepciones a la publicidad de la información.

Dichas excepciones serán analizadas en detalle en el capítulo correspondiente a la Clasificación de la Información.

6. REGULACIÓN DE LOS ARCHIVOS

Los artículos 33 y 34 refieren a pautas para el funcionamiento de los archivos, en el entendido que la profesionalización de los mismos es garantía del acceso a la información pública.

La falta de organización en los archivos no puede ser un impedimento para la transparencia, dado que éstos son básicamente la memoria de las entidades públicas.

Según la Dra. Laura Nahabetián: La importancia de los archivos radica en principio, en tres razones fundamentales: “Facilitan la gestión de la Administración Pública e Instituciones, proporcionando acceso a los documentos en el curso de las actividades administrativas cotidianas. Permiten al ciudadano el ejercicio del derecho de acceso a la información, poniendo a su

disposición los documentos administrativos, técnicos y jurídicos que le conciernen o que son de interés para el conjunto de la sociedad. La transparencia es esencial en todo estado democrático. Preservan la memoria colectiva de las naciones, las regiones, las comunidades, las organizaciones y las personas.

Sin embargo, a éstas deben adicionarse dos absolutamente fundamentales:

Para que exista rendición de cuentas y transparencia, la sociedad necesita de información sólida y datos irrefutables, porque de otra manera la denuncia se convierte en prédica política sin ningún tipo de sustento y pierden por tanto valor y eficacia. En los archivos existe multiplicidad de información que permite la verificación de claves fundamentales para la comprensión y solución de problemas nacionales acuciantes."[194]

El artículo 33 establece la obligación de las entidades públicas de mantener archivos organizados y actualizados.

El responsable debe garantizar ciertas condiciones para el buen funcionamiento de los archivos. Estas condiciones son edilicias, ambientales, de seguridad respecto a la entrada y salida de documentos. La referencia a mantener una organización sistemática de los archivos implicaría que estas tareas deberían ser coordinadas o supervisadas por personas que tengan título habilitante.
Por su parte el artículo 34 permite a los miembros de la Unidad de Acceso a la Información Pública el acceso a los documentos y expedientes clasificados, en tanto se trata del órgano de control.

Dentro de las disposiciones transitorias, el artículo 60 indica que mientras no se publique el Decreto Reglamentario de la Ley Nº 18.220 del Sistema Nacional de Archivo, el archivo de la documentación deberá elaborarse de acuerdo con las normas archivísticas internacionalmente reconocidas.

7. INFORMES QUE DEBEN PRESENTAR LOS SUJETOS OBLIGADOS

Como parte de las obligaciones impuestas por la Ley Nº 18.381, se establece la presentación de informes ante el órgano de control para que éste fiscalice el grado de cumplimiento.

Mediante esta información, la Unidad tiene la posibilidad de evaluar la puesta en práctica de la transparencia por parte de las entidades públicas. "El nuevo paradigma basado en la información se expande rápidamente, lo que hace cada vez más difícil, costoso e inconveniente continuar sosteniendo modelos institucionales cerrados o con márgenes de opacidad que le restan confiabilidad y pérdida de credibilidad pública (…) La transparencia ha dejado de ser solo un imperativo ético para convertirse en una práctica necesaria para

[194] NAHABETIÁN BRUNET, Laura. "El valor de los archivos en el proceso de transparencia y Democracia", pág. 10, 1er. Foro Internacional: La Ley de Acceso a la Información Pública y los Archivos Gubernamentales. Guatemala, 2010.

el crecimiento, consolidación y sostenibilidad de cualquier organismo público o privado".[195]

Todos estos formularios se pueden descargar de la página web de la Unidad, en cualquiera de sus dominios: www.informacionpublica.gub.uy o www.uaip.gub.uy.

7.1 Informe anual

Se encuentra detallado en el artículo 36 del Decreto Reglamentario. El último día hábil del mes de marzo de cada año, los sujetos obligados deben presentar ante la UAIP un formulario que da cuenta del estado de cumplimiento de las solicitudes de acceso recibidas. En caso de no haber recibido ninguna solicitud de acceso, el formulario debe igualmente ser presentado, indicando que no se produjeron solicitudes.

En el formulario se encuentran los siguientes campos:
-La identificación del sujeto obligado.
-El período que comprende el informe.
-Detalles del trámite que siguieron las solicitudes de acceso a la información pública. En este ítem se consulta acerca de cuál fue el trámite seguido, dentro de qué plazo fueron contestadas las solicitudes. Si las solicitudes fueron denegadas, cuáles fueron los motivos, así como cuál fue el soporte que se utilizó principalmente para entregar la información a los solicitantes (ej. papel, magnético).

7.2 informe semestral

Detallado en el artículo 37 del Decreto Reglamentario se encuentra lo atinente al informe semestral. La primera quincena de febrero y de agosto los sujetos obligados deberán presentar ante la UAIP un informe con la lista de la información reservada que haya sido clasificada en el período considerado.

-En el frente del formulario, se deben colocar los datos que identifican al sujeto obligado.

-Al dorso, en los renglones existentes, deberá describirse uno a uno cada expediente o documento reservado. En cada renglón se coloca la descripción temática por la cual se reservó la información y los datos de la resolución que así lo determinó - número y fecha-.

Además el sujeto obligado debe completar por cada expediente o documento reservado un formulario para la presentación de información reservada individual. El mismo contiene los siguientes datos:

-Identificación del sujeto obligado.

---

[195] CAINFO. "Transparencia y acceso en la información pública en el Poder Judicial". 1ª Edición. Letraeñe Ediciones. Montevideo, 2009, pág.30.

-Individualización de los documentos o expedientes reservados. En estos campos se detalla la ubicación, el tema que motiva la reserva, la denominación del documento y demás datos identificatorios del mismo, asimismo deberá indicarse si se hizo lugar a la prórroga del plazo de reserva y en qué fecha.

8. REGULACIÓN DE LAS OBLIGACIONES DE LOS RESPONSABLES

El artículo 38 establece la obligación de transparencia activa referida con anterioridad. Se indica qué información debe ser difundida de oficio por los sujetos obligados a través de su página web. La finalidad es crear una red de confianza entre los sujetos obligados y la ciudadanía. Además cuanto mayor sea la cantidad de información publicitada por los sujetos obligados, menor será la cantidad de solicitudes de acceso que se tramiten ante ellos.

Un problema que plantea la Ley Nº18.381, y que no resuelve el Decreto Reglamentario, es que no se establece con precisión la extensión de la obligación de transparencia activa. En el caso de una unidad ejecutora, no queda claro si la obligación de transparencia activa alcanza a las páginas web de las unidades, de las direcciones y de las demás reparticiones.

En el caso del Poder Ejecutivo, hay información extra que se debe publicitar:

-Expropiaciones por razones de utilidad pública.

-La coordinación de proyectos con personas públicas estatales y no estatales, sectores empresariales y sociales.

-El presupuesto aprobado y las adecuaciones presupuestales que se sucedan en las diferentes rendiciones de cuentas.

-Información útil para el conocimiento y evaluación de las funciones y políticas públicas.

Asimismo cada sujeto obligado tiene que designar a un responsable por la publicación de información en el sitio web.

9. ÓRGANO DE CONTROL

El título VI del Decreto Reglamentario regula todo lo referente al órgano de Control. En el mismo se detalla el funcionamiento del Consejo Ejecutivo y Consejo Consultivo de la Unidad de Acceso a la Información Pública.

El capítulo referente al órgano de Control detalla estas disposiciones.

10. RESPONSABILIDAD DE LOS FUNCIONARIOS

El Decreto Reglamentario establece, en su artículo 58, que puede constituir una falta grave, las hipótesis de obstrucción al derecho de acceso que se plantean en el artículo 31 de la Ley Nº 18.381. Estas conductas obstructivas son: negar el acceso a información no clasificada; suministro parcial de

información si existe dolo, mala fe o negligencia; permitir el acceso injustificado a la información clasificada y utilizar, sustraer, ocultar, divulgar o alterar información a la que tuviere acceso. Asimismo el artículo 6º de la citada Ley, establece responsabilidad solidaria de los funcionarios y el jerarca del sujeto obligado ante las conductas descriptas.

El artículo 55 del Decreto Reglamentario regula las responsabilidades de los jerarcas de los sujetos obligados:

-Designar funcionarios responsables de gestionar las solicitudes de acceso. En el artículo 57, se establece que dicho funcionario debe acatar los plazos de respuesta, solicitar la información a la dependencia correspondiente y entregarla al solicitante.

-Adoptar medidas que garanticen el derecho de acceso a la información pública, así como crear y mantener registros.

-Clasificar la información.

-Enviar al órgano de control los informes anuales y semestrales.

-Proveer medidas de seguridad para la información.

-Disponer en el presupuesto recursos para capacitar a los funcionarios en el acceso a la información pública.

11. CONCLUSIONES

Tanto la Ley de Acceso a la Información pública como su Decreto Reglamentario, conciben el acceso a la información pública como un Derecho Humano, y un Derecho ciudadano, cuyo ejercicio debe estar libre de trabas formalistas, y debe garantizarse a todas las personas.

El acceso a la información pública está ligado indisolublemente con la organización y profesionalización de los archivos, así como con el uso de las tecnologías de la información para logar llegar a todos los ciudadanos.

En una posterior etapa, debe considerarse el determinar con mayor precisión elementos que no se consideraron en el presente Decreto Reglamentario, como el alcance de las obligaciones de transparencia activa y la determinación concreta de las excepciones al acceso a la información pública, hasta ahora referidos de forma genérica como: la dignidad de las personas, la defensa y seguridad públicas y el interés público.

CAPÍTULO XI - AUTORIDADES DE CONTROL EN ACCESO A LA INFORMACIÓN PÚBLICA

Dra. Jimena Hernández

1. INTRODUCCIÓN

El derecho a la información es ampliamente reconocido como un derecho fundamental, y es así que se encuentra consagrado como tal en numerosos textos internacionales y regionales referidos a los derechos humanos.

A pesar de ello, debemos reconocer que el éxito del derecho de acceso a la información pública, no recae únicamente en la existencia de una ley que lo consagre expresamente y se encuentre orientada a aumentar la transparencia de la función administrativa, sino que se requiere de un órgano de control que pueda llevar a cabo los cometidos en ella previstos. Es necesario el establecimiento de sistemas de control, supervisión y vigilancia del cumplimiento de la ley, órganos que velen por el respeto del derecho a la información pública como derecho de todas las personas.

Ésta es la única manera de que las disposiciones legales que consagran derechos no permanezcan inmóviles o como “letra muerta”, sino que tengan una incidencia real en la protección de los derechos que buscan garantizar; esto es que logren una protección efectiva de esos derechos.

En el caso del derecho de acceso, esta necesidad aparece reforzada en virtud de que implica la posibilidad que tenemos todas las personas de participar del poder político, estando debidamente informados, dentro de un Estado Democrático de Derecho. Implica la posibilidad de acceder a información que se encuentra dentro del Estado y sus organismos, de asuntos públicos o que afectan el interés público. La transparencia y acceso a la información pública son de vital importancia para los ciudadanos ya que permiten monitorear los actos del gobierno y de forma general controlar el accionar de la gestión pública, mediante la exigencia de una permanente rendición de cuentas respecto a las decisiones que se toman dentro del Estado.

Por otra parte, no debemos perder de vista que el Gobierno Electrónico afianza la trasparencia en la gestión del Estado respecto de los ciudadanos, a través del fácil acceso de éstos a la información pública.

La base para la supervisión de una ley de acceso a la información pública es la existencia de un sistema institucional favorable que contribuya a facilitar el acceso a la información que se encuentra dentro del ámbito del estado.

La necesidad de controlar la correcta ejecución de las disposiciones contenidas en las leyes de acceso a la información pública es de vital importancia. Los estados deben establecer sistemas que permitan que se respete el derecho de acceso a la información, oportunamente, a fin de que el usuario pueda usarla en el momento en que la necesita.

Para ello, podríamos pensar en el establecimiento de un organismo autónomo que funcione como receptor y canalizador de las posibles contingencias que puedan suscitarse en la aplicación de la norma de acceso a la información pública, de acuerdo a las competencias que ésta le asigne.

2. DERECHO COMPARADO

2.1. Leyes de acceso a la Información en el mundo y modelos de control

Respecto a las leyes de acceso a la información en el mundo y a los órganos de control por ellas creados, Roberts[196] ha reseñado tres posibles modelos para el seguimiento de las leyes de acceso a la información pública. Estos son:

a. A los individuos se les otorga el derecho de someter una apelación administrativa ante otro funcionario de la misma institución a la cual la solicitud de la información fue sometida en primer lugar. Si esta apelación administrativa falla, el individuo puede apelar ante una corte o tribunal que pueda ordenar la entrega de la información.
b. A los individuos se les otorga el derecho a entablar una apelación ante un Ombudsman independiente o ante un Comisionado de la información quien debe enviar una recomendación acerca de la entrega de la información solicitada. Si la institución ignora la recomendación, se procederá a apelar ante la corte.
c. A los individuos se les otorga la posibilidad de someter una apelación ante un Comisionado de la Información que tenga el poder de obligar a la apertura de la información requerida. Aquí no proceden mayores apelaciones legales, aunque en casos extremos las acciones del Comisionado quedan sujetas a revisión judicial.

Por último destaca que frente a cualquiera de estos escenarios es necesaria la existencia de un Poder Judicial independiente.

Respecto a los modelos de autoridades de control, resultan interesantes las ideas expresadas por la Dra. Laura Nahabetián en ponencia elaborada en ocasión del 1º Foro Internacional denominado “La ley de transparencia y acceso a la información pública y los archivos gubernamentales”.[197] En ésta destaca que en materia de autoridades de control y el papel que éstas juegan para el fortalecimiento de la democracia, podemos encontrarnos frente a varios escenarios: la ausencia de órgano de control, entidad no creada por la legislación pero forjada en la práctica por su aplicación, creación de un órgano de control con competencias específicas.

De los diversos países que cuentan hoy en día con leyes de acceso a la información pública, solo algunos cuentan con órganos independientes encargados de las tareas de control de la aplicación de la norma y el respeto del derecho de acceso a la información pública. El análisis de diversos casos y modelos de control, establecidos en el derecho comparado, nos permite

[196] ROBERT citado por ACKERMAN, John M y SANDOVAL, Irma E. “Leyes de Acceso a la información en el Mundo”. Cuadernos de transparencia 07. IFAI. México. 2007.
[197] El mencionado evento se llevo a cabo el 21 y 22 de Junio de 2010, en Guatemala.

profundizar aún más en el papel determinante que juegan estos órganos como garantes de la efectividad de las leyes de acceso a la información pública en los países que los consagran.

2.2. Unión Europea

2.2.1. Suecia es el primer país del mundo en consagrar el derecho fundamental de acceso a la información pública en el año 1766. "The Freedom of the Press Act" es una ley constitucional donde se establecen las normas fundamentales sobre el acceso a los documentos oficiales[198]. Esta norma no incluye la existencia de un órgano de control independiente sino que deposita la supervisión de la ley en manos del Canciller de Justicia. El 30 de junio de 2009 entró en vigor otra disposición "Public Acces To Information and Secrecy Act", el acceso del público a la información y la Ley de secreto. Contiene disposiciones que complementan las disposiciones contenidas en la Ley de libertad de la prensa. En materia de control establece que si una autoridad ha rechazado una solicitud para obtener un documento el solicitante tiene derecho a apelar contra la decisión ante un tribunal administrativo de apelación. A su vez, una decisión de estos Tribunales podrá ser recurrida ante el Tribunal Supremo Administrativo.

2.2.2. Francia es un caso muy interesante en virtud de que cuenta con la Ley de Acceso a Documentos Administrativos de 1978 "*Loi relative ou droit d´accès aux documents administratifs*" (Ley Nº 78-753 del 17 de Julio de 1978). Esta ley prevé la existencia de una Comisión de Acceso a Documentos Administrativos como autoridad encargada de asegurar el respeto de la libertad de acceso a los documentos administrativos y los registros públicos. Es una autoridad que posee absoluta independencia de criterio. Ella aconseja frente a la negativa de un documento administrativo, una negativa de acceso o la divulgación de los registros públicos. La remisión del dictamen de la comisión es un requisito previo para el ejercicio de un recurso judicial.

El Comité está integrado por once miembros: tres magistrados (un consejero de Estado, un consejero de la Corte de Cuentas y un consejero de la Corte de Casación), tres funcionarios electos por sufragio popular (un Diputado, un Senador designados por el Presidente de la Asamblea Nacional y el Presidente del Senado y un funcionario electo de una autoridad local designada por el Presidente del Senado), un profesor de educación superior, una persona cualificada en los archivos, impartida por el Director de los Archivos de Francia, una persona calificada en materia de protección de datos personales, propuesta por el Presidente de la Comisión Nacional de la Informática y las Libertades, una persona calificada en términos de competencia y fijación de precios, propuesta por el Presidente de la Autoridad de la Competencia, y una persona calificada en la difusión de información pública.

---

[198] El texto de la norma se encuentra disponible en: http://www.riksdagen.se/templates/R_Page____6313.aspx. Página web consultada el 15 de febrero de 2011.

Estos miembros son designados por decreto del Primer Ministro y duran en sus cargos por un período de tres años con la posibilidad de ser renovados.[199]

2.2.3. Portugal[200] por su parte cuenta con la Ley Nº 65/93 del 26 de agosto de 1993 de acceso a documentos administrativos "Lei de Acceso aos Documentos Administrativos". En su art. 18 establece la creación de una entidad pública independiente, dotada de autonomía técnica y administrativa denominada Comité de Acceso a Documentos Administrativos (CADA), con el objetivo de velar por la aplicación de las disposiciones de la ley. Dentro de sus facultades más importantes se encuentran la posibilidad de aprobar su reglamento interno, examinar toda queja que se le presente, emitir dictámenes sobre el acceso a los documentos con nombre, decidir sobre el sistema de clasificación de documentos, resolver sobre la aplicación de esta ley, así como la preparación y aplicación de la legislación en asuntos relacionados a petición del gobierno, la Asamblea de la República o de la administración, preparar un informe anual sobre la aplicación de esta ley y su actividad que se remitirá tanto a la Asamblea de la República, para su publicación y examen, como al Primer Ministro.

El Comité se encuentra integrado por un juez, miembro del Tribunal Administrativo Supremo, nombrado por el Consejo Supremo de los Tribunales Administrativos y Fiscales que actuará como Presidente, dos miembros de la Asamblea de la República elegidos por esta última, uno nombrado por el grupo parlamentario del partido de gobierno, y el otro designado por el grupo parlamentario del partido mayoritario en la oposición, un profesor de derecho designados por el Presidente de la Asamblea de la República, dos personas de reconocido prestigio designados por el gobierno, un representante de cada una de las Comunidades Autónomas, respectivamente, designados por los Gobiernos de las Comunidades Autónomas, una persona designada por la Asociación Nacional de Municipios Portugueses, un abogado designado por el Colegio de Abogados, un miembro del Comité Nacional para la Protección de Datos de Carácter Personal designado por este último. Tienen una duración de dos años en sus cargos, pudiendo ser renovados en ellos.

2.2.4. Inglaterra[201] cuenta con la "Freedom of Information Act", la Ley de Libertad de Información que se encuentra vigente desde el año 2005 y crea el Comisionado para la Información. Este Comisionado es la autoridad encargada de supervisar el cumplimiento de la Ley; está facultado para tramitar las peticiones que se le presenten sobre el acceso a la información. En el artículo 47 de la Ley se establecen las funciones del Comisionado entre las cuales podemos destacar la promoción de su observancia por parte de las autoridades públicas y sus potestades para evaluar su cumplimiento por parte de dichas

---

[199] Ley disponible en: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=924A5F00C900B5DA2B2EE5C84DADED8D.tpdjo07v_2?cidTexte=LEGITEXT000006068643&dateTexte=20090607. Página web consultada el 15 de febrero de 2011.

[200] Ley disponible en: http://www.gddc.pt/legislacao-lingua-estrangeira/english/law-65-93.html. Página web consultada el 17 de febrero de 2011.

[201] Ley disponible en: http://www.legislation.gov.uk/ukpga/2000/36/contents. Página web consultada el 17 de febrero de 2011.

autoridades. Se encarga también de difundir el funcionamiento de la ley y las buenas prácticas en torno a ésta.

El Comisionado está facultado para tramitar las peticiones que sean realizadas ante él en materia de acceso a la información pública. Luego de recibida y evaluada la solicitud puede enviar a la autoridad en cuestión un aviso de decisión. En éste se indican los pasos que debe seguir la autoridad para adecuarse a la Ley. Por otra parte, en el caso en que el Comisionado entienda que la autoridad no ha cumplido con algunos de los requisitos de la Ley, puede enviar un aviso de ejecución a efectos de que la autoridad adopte las medidas por ésta requeridas.

En el marco del ejercicio de estas actividades, el Comisionado debe brindar un informe anual al Parlamento que refleje cómo se han cumplido las obligaciones establecidas por la Ley.

2.3. América Latina

Actualmente, en América Latina existen 11 países que cuentan con Leyes de Acceso a la Información Pública, son: Chile, Colombia, Ecuador, Guatemala, Honduras, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay. Es interesante analizar algunas de ellas para ilustrarnos acerca de los modelos de órganos de control que han establecido, sobre todo aquéllas que han creado órganos de control independientes.[202]

2.3.1. México[203] fue uno de los primeros países latinoamericanos en adoptar una Ley de acceso a la información pública en junio de 2002, la Ley Federal de Transparencia y Acceso a la Información Pública. En sus artículos 33 y siguientes crea un órgano de vigilancia y control independiente denominado Instituto Federal de Acceso a la Información Pública (IFAI). El IFAI es un órgano dotado de autonomía operativa, presupuestaria y de decisión. Se encarga de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades públicas. Se integra por cinco comisionados que durarán siete años en sus cargos sin posibilidad de renovación y en régimen de dedicación exclusiva.

La Ley destaca la absoluta independencia y autonomía del IFAI en la adopción de sus resoluciones.

Dentro de sus cometidos esenciales podemos destacar: conocer y resolver los recursos de revisión interpuestos por los solicitantes, establecer y revisar los criterios de clasificación, desclasificación y custodia de la información reservada y confidencial, vigilar y, en caso de incumplimiento, hacer las recomendaciones a las dependencias y entidades para que se de cumplimiento a la obligación de transparencia, orientar y asesorar a los particulares acerca

---

[202] Información acerca de la regulación del Acceso a la Información Pública en América latina: MENDEL, Toby. “El Derecho a la Información en América Latina”. UNESCO. 2009. Ecuador.

[203] Ley disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf. Página web consultada el 19 de febrero de 2011.

de las solicitudes de acceso a la información, proporcionar apoyo técnico a las dependencias y entidades en la elaboración y ejecución de sus programas de información, elaborar los formatos de solicitudes de acceso a la información, así como los de acceso y corrección de datos personales, promover y, en su caso, ejecutar la capacitación de los servidores públicos en materia de acceso a la información y protección de datos personales, elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de esta Ley, elaborar su Reglamento Interior y demás normas de operación, preparar su proyecto de presupuesto anual, entre otros.

Es interesante destacar que la labor del IFAI, no solo tiene gran relevancia dentro de su país, sino que cuenta con gran proyección internacional, en virtud de que se ha encargado de la difusión del derecho de acceso a la información pública a nivel internacional. Una de las maneras en que se ha producido dicha difusión es a través de los numerosos informes y textos que ha elaborado publicados a través de los Cuadernos de Transparencia del IFAI, además de la gran cantidad de información que puede consultarse a través de su página web.[204]

2.3.2. Honduras[205] es otro de los países americanos que posee una Ley de Transparencia y Acceso a la Información Pública sancionada en el año 2006, pero con entrada en vigencia en enero del año 2008. Esta Ley crea el Instituto para el Acceso a la Información Pública (IAIP). El IAIP es un órgano desconcentrado de la administración pública, con independencia operativa, decisión y presupuestaria. Su objetivo principal consiste en promover y facilitar el acceso de los ciudadanos a la información pública.

Se integra por tres comisionados electos por el Congreso Nacional que duran cinco años en sus cargos.

Sus principales funciones y atribuciones consisten en: conocer y resolver los recursos de revisión interpuestos por solicitantes en el marco de la Ley, establecer los manuales e instructivos de procedimiento para la clasificación, archivo, custodia y protección de la información pública que deban aplicar las instituciones públicas conforme las disposiciones de la Ley, apoyar las acciones del Archivo Nacional en cuanto a la formación y protección de los fondos documentales de la Nación, establecer los criterios y recomendaciones para el funcionamiento del Sistema Nacional de Información Pública, aplicar el marco sancionatorio de la Ley, reglamentar, planificar, organizar y llevar a cabo su funcionamiento interno, presentar un informe de actividades en forma semestral a la Presidencia de la República y al Congreso Nacional, y realizar actividades de promoción y divulgación en cuanto al ejercicio del derecho de acceso a la información pública, entre otras.

---

[204] http://www.ifai.org.mx/. Página web consultada el 20 de febrero de 2011.
[205] Ley disponible en: http://www.redipd.org/documentacion/legislacion/common/legislacion/honduras/ley_transparencia_honduras.pdf
Web IAIP: www.iaip.gob.hn. Página web consultada el 20 de febrero de 2011.

2.3.3. Chile ha sancionado en agosto de 2008 la Ley Nº 20.285 sobre el Acceso a la Información Pública[206]. En su artículo 31 crea el Consejo para la Transparencia como una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio. Entre sus funciones más importantes se destacan: fiscalizar el cumplimiento de las disposiciones de la Ley y aplicar las sanciones en caso de infracción a ellas, resolver fundadamente los reclamos por denegación de acceso a la información, promover la transparencia de la función pública, la publicidad de la información de los órganos de la Administración del Estado, y el derecho de acceso a la información, por cualquier medio de publicación, dictar instrucciones generales para el cumplimiento de la legislación sobre transparencia y acceso a la información por parte de los órganos de la Administración del Estado, y requerir a éstos para que ajusten sus procedimientos y sistemas de atención al público a dicha legislación, proponer al Presidente de la República y al Congreso Nacional, las normas, instructivos y demás perfeccionamientos normativos para asegurar la transparencia y el acceso a la información, realizar actividades de difusión e información al público, entre otras.

La dirección y administración del Consejo está en manos de un Consejo Directivo integrado por cuatro consejeros designados por el Presidente de la República, previo acuerdo del Senado. Los consejeros durarán seis años en sus cargos pudiendo ser renovados por parcialidades de tres años.

2.4. Estados Unidos de Norteamérica

Con fecha 4 de julio de 1966 se promulga en Estados Unidos la ley denominada "Freedom of Information Act (FOIA)", entrando en vigor al año siguiente. Se trata de una Ley Federal que permite el acceso parcial o completo a la información y a los documentos que se encuentren en poder del gobierno, partiendo de la base de que los individuos tienen derecho a conocer aquello en lo que el gobierno está trabajando. Permite a cualquier persona solicitar el acceso a la información o registros de una agencia federal, la cual tiene que divulgarla tras la recepción de la solicitud por escrito, excepto para los registros que estén protegidos contra la divulgación por las nueve exenciones o las tres exclusiones que se prevén en la Ley. Las personas también pueden solicitar documentos en formato electrónico a partir de 1996 cuando se dicta la Ley de libertad de información electrónica "The Electronic Freedom of Information Amendments of 1996 (E-FOIA)".

La FOIA fue objeto de numerosas modificaciones posteriores que buscaron fortalecer el derecho por ella consagrado. La ley original no contempló por ejemplo plazos para el cumplimiento, sanciones por incumplimiento, ni la posibilidad de la revisión judicial posterior frente a la negativa de la entrega de la información por parte de la autoridad en cuestión. En virtud de esta situación, se dictaron en 1974 una serie de enmiendas a la ley a través de las cuales se buscó fortalecerla por ejemplo estableciendo plazos de cumplimiento y habilitando la posibilidad de la revisión judicial de las negativas al acceso a la información.

---

[206] Ley disponible en: http://www.leychile.cl/Navegar?idNorma=276363. Página web consultada el 20 de febrero de 2011.

Dentro del Departamento de Justicia de los Estados Unidos funciona la Oficina de Políticas de Información "Office of Information Policy"[207]. Esta Oficina se encarga de controlar el cumplimiento de la FOIA, y de asesorar tanto a los particulares como a los organismos estatales en cuanto a la aplicación y cumplimiento de la norma. Los organismos deben presentarle informes anuales acerca del cumplimiento de la ley y de la cantidad de solicitudes recibidas y procesadas. Por otra parte, contiene la información necesaria acerca de cómo se deben presentar las solicitudes de información, qué se puede solicitar, y qué se puede hacer si la misma no resulta satisfecha.

3. ÓRGANO DE CONTROL URUGUAYO

3.1. Creación de la Unidad de Acceso a la Información Pública

La Unidad de Acceso a la Información Pública, (UAIP), fue creada el 17 de octubre de 2008 por el art. 19 de la Ley Nº 18.331 de Acceso a la Información Pública.

La UAIP se creó como un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento, dotado de la más amplia autonomía técnica. Está integrada por un Consejo Ejecutivo y un Consejo Consultivo.

Funciona como un órgano técnico que tiene por objetivo garantizar la transparencia de la función administrativa y el derecho fundamental de las personas al acceso a la información pública, lo cual constituye el objeto fundamental de la Ley. En el artículo 21 de la Ley, se establece que el órgano de control tiene como cometido esencial realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la Ley de acceso a la información pública.

Además de los objetivos señalados en la Ley, debemos tener presente las normas contenidas en el Decreto Nº 232/010, de 2 de agosto de 2010, que en cumplimiento del mandato legal establecido en el art. 35 de la Ley 18.381, se encargó de reglamentar las disposiciones legales en ella contenidas, entre otras, aquellas normas referidas al órgano de control.

3.2. Consejo Ejecutivo

3.2.1. Integración

El Consejo Ejecutivo es el órgano de Dirección de la UAIP. El artículo 19 de la Ley dispone que se integra por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de idoneidad en la materia, aseguren la independencia de criterio, eficiencia, objetividad, e imparcialidad en el desempeño de sus cargos.

---

[207] Página web de la Oficina de Políticas de la Información de Estados Unidos: http://www.justice.gov/oip/. Página web consultada con fecha 2 de abril de 2011.

Los miembros del Consejo Ejecutivo duran cuatro años en sus cargos, a excepción del Director de AGESIC, pudiendo ser designados nuevamente. La Ley indica que solo cesarán por la expiración de su mandato y la designación de sus sucesores. Pueden también ser removidos por disposición del Poder Ejecutivo en casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso.

La Presidencia del Consejo es de carácter rotativo, anualmente, entre los dos miembros designados por el Poder Ejecutivo. El Presidente tiene a cargo la representación del Consejo y las actividades necesarias para garantizar el cumplimiento de sus resoluciones.

3.2.2. Cometidos

El Consejo Ejecutivo cuenta con una amplia gama de funciones y atribuciones que se enumeran en el artículo 21 de la Ley Nº 18.381:

A) Asesorar al Poder Ejecutivo en el cumplimiento de la normativa constitucional, legal o reglamentaria vigente y de los instrumentos internacionales ratificados por la República referidos al acceso a la información pública.

B) Controlar la implementación de la Ley Nº 18.381 por los sujetos obligados. En el cumplimiento del presente objetivo la UAIP cuenta con algunos recursos que le permiten a los sujetos obligados cumplir con las disposiciones legales. La página web de la Unidad proporciona documentos útiles a estos efectos, como los formularios para el Informe sobre cumplimiento de las obligaciones establecidas en el artículo 7º literales a y b, referidos a los informes anuales sobre el cumplimiento del derecho de acceso los cuales deben contener la información del período anterior sobre el cumplimiento de las obligaciones que le asigna la Ley, y el detalle de las solicitudes de acceso a la información y el trámite dado a cada una de ellas. Por otra parte, contiene los formularios para los informes semestrales relativos a la información reservada general e individual previstos en los artículos 7 y 9 de la Ley.

Estos informes son uno de los mecanismos que le permiten a la UAIP controlar a los sujetos obligados.

Dentro de sus cometidos de control la UAIP debe encargarse del cumplimiento de los plazos, que la ley ha dispuesto, para el cumplimiento de algunas de las obligaciones previstas como la implementación de sitio web por parte de los sujetos obligados o de los organismos, indicando un plazo de 1 año desde la publicación de la ley con vencimiento el 7 de noviembre de 2009 (art. 32). También se determinó el vencimiento del plazo de 1 año desde la vigencia de la ley para la clasificación de la información, el 27 de octubre de 2009; y para la desclasificación de la información en 6 meses desde el cumplimiento del plazo anterior con vencimiento el 27 de abril de 2010 (art. 33). Por otra parte, la ley

dispuso el plazo para la adecuación de registros de los sujetos obligados de 2 años, disponiendo su vencimiento el 27 de Octubre de 2010.[208]

En materia de plazos debemos tener presente las modificaciones que fueron introducidas a través del artículo 150 de la Ley N° 18.719 (Ley de Presupuesto Nacional período 2010-2014) del 27 de Diciembre de 2010. El mencionado artículo sustituyó el artículo 33 de la Ley N° 18.381 disponiendo respecto a la clasificación de información que: *"Al 31 de julio de 2012, todos los sujetos obligados deberán elaborar una lista de toda la información que a la fecha se encuentre clasificada como reservada, siempre y cuando esté comprendida en alguna de las excepciones contempladas en el artículo 9° de la presente ley. En la misma fecha, la información que no se sujete a estas excepciones, deberá ser desclasificada. A partir de la fecha señalada, toda la información clasificada como reservada, que tenga más de 15 años, deberá ser desclasificada y abierta libremente al público."*

Por otra parte, el artículo 151 de la Ley N°18.719 sustituye el artículo 34 de la Ley N° 18.381, respecto al plazo de adecuación de los registros por parte de los sujetos obligados, disponiendo que: *"Los sujetos obligados por la presente ley dispondrán de un plazo de cuatro años para adecuar sus registros, durante el cual no serán pasibles de sanción en caso de denegación de acceso fundada en la imposibilidad de ubicar la información."*
C) Coordinar con autoridades nacionales la implementación de políticas.

D) Orientar y asesorar a los particulares respecto al derecho de acceso a la información pública. En este marco la UAIP cuenta con mecanismos de contacto directo con los ciudadanos, telefónicamente o por correo electrónico. Además se ha elaborado un documento conteniendo las preguntas más frecuentes en cuando al derecho de acceso y el funcionamiento de la Unidad, contando también con el formulario a los efectos de cualquier denuncia que pueda presentarse frente a la denegación de acceso a la información pública.

E) Capacitar a los funcionarios de los sujetos que están obligados a brindar el acceso a la información. En cumplimiento de este cometido la Unidad ha brindado numerosas charlas en varios departamentos del país.

F) Promover y coordinar con todos los sujetos obligados las políticas tendientes a facilitar el acceso informativo y la transparencia.

G) Ser órgano de consulta para todo lo relativo a la puesta en práctica de la Ley Nº 18.381 por parte de todos los sujetos obligados.

En cumplimiento de estos objetivos la UAIP ha desarrollado numerosas tareas como recibir consultas por parte de los sujetos obligados, en cuanto a la correcta aplicación de las disposiciones legales, así como implantando charlas en los organismos públicos, informando sobre la aplicación de la Ley.

---

[208] La información proporcionada en el presente capítulo referida a plazos y documentos elaborados por la Unidad, se encuentra disponible en la página web de la UAIP www.informaciónpública.gub.uy. Página web consultada con fecha 26 de febrero de 2011.

H) Promover campañas educativas y publicitarias donde se reafirme el derecho al acceso a la información como un derecho fundamental.

I) Realizar un informe de carácter anual relativo al estado de situación de este derecho al Poder Ejecutivo.

J) Denunciar ante las autoridades competentes cualquier conducta violatoria a la ley que se comenta y aportar las pruebas que consideren pertinentes.

En cumplimiento de los objetivos que la norma le ha encargado, la Unidad, conjuntamente con AGESIC, ha participado durante su puesta en funcionamiento a la fecha, en numerosos eventos y talleres en la materia.

3.2.3. Normas introducidas por el Decreto Nº 232/010

El Decreto Nº 232/010, de 2 de agosto de 2010, introduce algunas disposiciones que reglamentan la labor del Presidente del Consejo Ejecutivo indicando las funciones con las que debe cumplir. Al Presidente le corresponde: la representación de la UAIP por sí o por apoderado, cumplir y hacer cumplir las normas constitucionales, legales y reglamentarias, así como ejecutar y hacer ejecutar las resoluciones del Consejo Ejecutivo, presidir las sesiones del Consejo y dirigir sus deliberaciones, tomar medidas en caso de urgencia, estructurar el orden del día, convocar sesiones ordinarias y extraordinarias, someter a aprobación del Consejo la planificación y el proyecto de memoria anual de la Unidad, firmar las actas del Consejo, resoluciones y correspondencia oficial, firmar contratos y documentos autorizados por el Consejo Ejecutivo, fiscalizar la administración ejecutiva y el desempeño de los funcionarios que presten funciones para la UAIP.

Por otra parte, el artículo 44 del Decreto reafirma los cometidos y funciones que le han sido atribuidos a la Unidad por la Ley Nº 18.381.

Por otra parte, también encontramos importantes disposiciones que se encargan de reglamentar el funcionamiento del Consejo Ejecutivo de la UAIP. En el artículo 45 se indica que el Consejo fijará día y hora para sus sesiones ordinarias. Puede reunirse en forma extraordinaria por disposición del Presidente o a solicitud de dos de sus miembros. El Consejo se encuentra habilitado para sesionar con la presencia de dos de sus miembros. El artículo 48 establece que para las votaciones se requiere la asistencia de todos los miembros y se tomarán por mayoría, en caso de empate, el asunto se pasa para la próxima sesión y en caso de persistir se computará doble el voto del Presidente.

En cuanto al desarrollo de las sesiones del Consejo, se indica que el Presidente abrirá la sesión y procederá a la lectura de las actas, y una vez aprobadas, se pasará a considerar los asuntos a tratar según el orden del día establecido.

El Decreto, en su artículo 46, prevé la posibilidad de realizar mociones ya sean

con carácter de cuestión de orden o previa, las cuales serán inmediatamente resueltas. La norma se encarga de definir como cuestiones de orden: "*las que se refieren al orden del día, observancia del presente Decreto, suspensión o aplazamiento de la discusión, consideración de un asunto, reconsideración de un proyecto antes de su sanción definitiva y declaración de urgencia*". Por otra parte, define a las cuestiones previas indicando que: "*son las consultas al Consejo Ejecutivo sobre el contenido o el espíritu de una disposición legal o reglamentaria que tenga relación con el asunto que se discuta*".

Otra de las innovaciones importantes que incluye el Decreto Nº 232/010, es la posibilidad de que el Consejo Ejecutivo se constituya en el Comisión General para conferenciar sobre algún asunto que exija explicaciones preliminares. La Comisión no adoptará decisiones.

Establece también, en el artículo 49, la posibilidad de que se formen Comisiones Especiales. Dicha formación debe ser resuelta por el Consejo Ejecutivo. Pueden tener carácter permanente o extraordinario y se forman a los efectos de asesorar, realizar trabajos o estudios que se dispongan. Rendirán informes por escrito, salvo que se acepte verbal, dentro de los plazos que sean establecidos a dichos efectos por el Consejo Ejecutivo. Sus dictámenes no son obligatorios para el Consejo Ejecutivo.

Por último es interesante destacar que el Decreto establece un principio de publicidad indicando en su artículo 51 que: "*La UAIP hará públicas las resoluciones que adopte incluyéndolas en su sitio web, en forma posterior a la notificación. La publicación se realizará aplicando los criterios de disociación de datos de carácter personal que a tal efecto se establezcan*". Esta disposición es importante en virtud de que determina la transparencia de todas las decisiones que tome el órgano encargado de garantizarla.

3.3. CONSEJO CONSULTIVO

3.3.1. Integración y funcionamiento

En el artículo 20 de la Ley Nº 18.381 se crea el Consejo Consultivo de la UAIP como un órgano que se encarga de asistir al Consejo Ejecutivo, y funciona a instancias de éste.

Su integración se compone de cinco miembros: una persona de reconocida trayectoria en la promoción y defensa de los derechos humanos, designada 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. Sus integrantes durarán cuatro años en sus cargos.

El Consejo sesionará convocado por el Presidente de la UAIP, o por la mayoría de sus miembros. Sesionará presidido por el Presidente del Consejo Ejecutivo.
La competencia del Consejo Consultivo es, como lo determina su nombre, de asesoría. Puede ser consultado por el Consejo Ejecutivo sobre cualquier

aspecto de su competencia.

En cuanto al funcionamiento del Consejo Consultivo, éste ya se encuentra integrado y sesiona cuando le es requerido según lo dispone la Ley.

3.3.2. Normas introducidas por el Decreto 232/010

El Decreto Reglamentario también contiene algunas disposiciones referidas al Consejo Consultivo de la UAIP.

Se indica que la convocatoria del Consejo debe realizarse con una antelación mínima de 5 días y podrá sesionar con la presencia de la mayoría simple de sus integrantes.

Regula también el desarrollo de las sesiones del Consejo indicando que el Presidente declarará abierta la sesión, y procederá a la lectura de las actas. Las decisiones se tomarán por mayoría de los miembros. Todo lo actuado en el Consejo se documenta en actas que serán debidamente firmadas.

Por último, el Decreto establece algunas pautas para la designación de algunos integrantes del Consejo Consultivo indicando que el representante del área académica debe ser designado por acuerdo de las Facultades de Derecho de las Universidades reconocidas del país. El representante del sector privado será designado por el Centro de Archivos y Acceso a la Información Pública (CAInfo).

4. CONCLUSIONES

A lo largo de estas páginas hemos tratado de visualizar la importancia del derecho al acceso a la información pública como derecho humano fundamental, ampliamente reconocido y protegido a nivel internacional y a nivel nacional por los Estados. Éstos han reconocido la necesidad de que los ciudadanos puedan acceder a las informaciones públicas como elemento esencial para la transparencia del Estado, dentro de un sistema democrático, y como medio de fortalecer el relacionamiento entre el Estado y los ciudadanos.

Las denominadas leyes de acceso a la información pública o de transparencia del Estado son la piedra angular para el derecho de acceso a la información pública. Pero deben estar acompañadas de sistemas de control y fiscalización que se encarguen de proporcionar un sistema de garantías eficientes para el respeto de este derecho. Dicho sistema debe encarnarse en un órgano de control de naturaleza independiente y que funcione de manera autónoma respecto a los Poderes del Estado cuya transparencia busca garantizar.

CAPÍTULO XIII – CLASIFICACIÓN DE LA INFORMACIÓN

Dra. Bárbara Muracciole

1. INTRODUCCIÓN

"Cuando la transparencia reemplaza los secretos y el poder se expone al escrutinio público, los abusos se pueden frenar, la opinión pública se puede incorporar y el Estado puede rendirle cuentas al interés público"[209]

El derecho a la información y en especial el derecho de acceder a la información, es un derecho fundamental con repercusión directa en la transparencia de los Estados y democracias modernas. Al decir de Toby Mendel "el derecho a la información está en el corazón de la democracia. Sólo una ciudadanía bien informada sobre las intenciones y acciones de sus líderes electos, puede contribuir de forma efectiva al proceso de toma de decisiones que afecta su futuro".[210]

La conciencia parlamentaria en este sentido, ha caracterizado las últimas décadas por una proliferación normativa en la materia, tendiente a garantizar y regular este derecho y sus excepciones. Punto, neurálgico de su ejercicio.

Nos proponemos revisar los criterios que deben imperar para establecer excepciones al derecho de acceso, abordando por tanto el concepto de clasificación de la información, objeto del presente trabajo.

2. INFORMACIÓN PÚBLICA

Dispone el artículo 2º de la Ley N° 18.381, de 7 de Octubre de 2008 *"Se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales".*

Por su parte el artículo 4°del Decreto reglamentario N° 232/010 de 2 de Agosto de 2010, bajo el *nomen iuris* "*Principio de libertad de información*", nos dice que *"toda persona tiene derecho de acceder a la información que obre en posesión de los sujetos obligados con la única excepción que aquélla clasificada como información reservada, confidencial y secreta de acuerdo a lo establecido en las leyes especiales a tales efectos"*.

La regla entonces, es que la información en manos de los organismos del Estado es pública y por tanto accesible a cualquier interesado. La excepción a su acceso, es que la información sea secreta por ley, o se encuentre clasificada como reservada o confidencial.

---

[209] MENDEL, Toby. El Derecho a la Información en América Latina, pág. 1. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, Oficina de Quito. 2009.
[210] MENDEL, Toby. Ob. Cit., pág. 1.

Dos consideraciones se imponen. Las excepciones a la información pública y la clasificación de la información.

3. EXCEPCIONES

El derecho de acceso a la información pública es un derecho fundamental, presente desde siempre en nuestro ordenamiento jurídico como una de las manifestaciones del derecho de información y de reciente reconocimiento legal por la Ley N° 18.381, de Acceso a la Información Pública.

"Puede definirse como la prerrogativa de la persona para acceder a datos, registros y todo tipo de información en poder de entidades públicas y empresas privadas que ejercen gasto público y/o cumplen funciones de autoridad, con las excepciones taxativas que establezca la ley en una sociedad democrática"[211]

Tratándose de un derecho fundamental, su goce solo podrá ser limitado por ley formal fundada en razones de interés general y será de interpretación estricta.

Siguiendo a Risso Ferrand, cabe recordar que "las normas que establecen excepciones a los derechos fundamentales o que autorizan su limitación, serán siempre de interpretación estricta, y nunca será válida una interpretación analógica o a *contrario sensu* de una norma que establece una excepción a la normativa de derechos humanos[212]"

En este sentido, las excepciones al acceso son uno de los temas más discutidos por la comunidad internacional, desde que de su correcta redacción dependerá el éxito o fracaso de una Ley de Acceso a la Información ¿Por qué? Por un lado, porque una apertura excesiva que implique un elenco amplio y vago de excepciones, permitiría retener información discrecionalmente, vaciando el acceso, y por otro lado, porque su falta vulneraría otros derechos (privacidad, seguridad) que también es necesario tutelar .

3.1 Principio de Limitación de Excepciones

Recogido como cuarto principio por la organización no gubernamental ARTICULO 19[213], el principio de limitación de excepciones implica que las excepciones al derecho de acceso habrán de ser establecidas por ley, serán limitadas, deberán definirse claramente y estarán sujetas a pruebas estrictas de daño e interés público.

Esta organización ha formulado y propone "una prueba de interés público" en tres partes, para valorar si las excepciones al acceso cumplen los referidos requisitos solicitados por la comunidad internacional:

- la información (restringida) debe relacionarse con un fin legítimo definido

[211] VILLANUEVA, Ernesto. El derecho a la información, pág. XXIV.
[212] RISSO FERRAND, Martín. Algunas Garantías Básicas de los Derechos Humanos, Segunda Edición actualizada y ampliada, Fundación de Cultura Universitaria, pág. 34
[213] El derecho de saber del público: Principios sobre la Legislación en materia de la Libertad de Información (los Principios de Artículo 19)

en la misma ley,
- la divulgación de la información debe plantear la amenaza de un daño o perjuicio sustancial a ese fin legítimo; y
- el perjuicio o daño para el fin legítimo debe ser mayor al interés público en acceder a la información restringida.[214]

Si se cumplen estas tres condiciones, entonces se justifica la no revelación de la información al público.

Vemos claramente la referencia a un daño o perjuicio causado por la difusión de la información. En efecto, consensuado es el hecho que el acceso a la información pública admite dos grandes tipos de excepciones:

El primero, refiere a las hipótesis de revelación que causen daño a un interés público jurídicamente protegido, como son la seguridad pública o la seguridad nacional.

El segundo, responde a la necesidad de proteger la vida privada y el patrimonio de las personas.

Cada tipo habrá de ser valorado en función de su aplicación al caso concreto, ponderándose los valores en conflicto.

En el primer grupo, la ponderación se hará entre publicidad y seguridad, a fin de determinar si la primera pone en riesgo la segunda y amerita la reserva temporal de la información. Es lo que se conoce como "prueba de daño".

En el segundo grupo, la ponderación se hará confrontando la publicidad con la privacidad o el patrimonio de las personas. Es lo que se conoce como "prueba de interés público".

Ambas pruebas, han sido utilizadas en vía administrativa y judicial, para revisar la aplicación de las excepciones al principio de publicidad. Algunos países han resuelto incluir estos criterios o estándares en sus legislaciones en la materia.

A continuación analizaremos la normativa de acceso a la información pública y sus excepciones, en seis países latinoamericanos.

3.2 Derecho Comparado

3.2.1 Chile

Chile aprobó la Ley N° 20.285[215] sobre Acceso a la Información Pública, publicada en el Diario Oficial el 20 de Agosto de 2008.

En su artículo 10, reconoce el derecho de toda persona *"a solicitar y recibir*

[214] Leyes de Acceso a la Información en el Mundo, pág. 27. Cuadernos de transparencia N° 07. Instituto Federal de Acceso a la Información Pública, México 2007.
[215] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html Página visitada el 5 de Enero de 2012.

información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece la ley". Disponiendo, que dicho acceso comprende el derecho de *"acceder a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como a toda información elaborada con presupuesto público, cualquiera sea el formato o soporte en que se contenga, salvo las excepciones legales".*

Respecto de las excepciones, el artículo 21 establece las causales de secreto o reserva en virtud de las cuales se podrá denegar total o parcialmente el acceso a la información, divididas en cinco numerales que refieren al caso que la publicidad afecte el debido cumplimiento de las funciones del órgano requerido, los derechos de las personas, la seguridad de la Nación, la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país, o cuando se trate de documentos, datos o informaciones que una ley de *quorum* calificado haya declarados reservados o secretos.

3.2.2 Colombia

La Ley N° 57[216] de Acceso a la Información Pública, fue publicada en el Diario Oficial el 12 de Julio de 1985.

Su artículo 12, reconoce el derecho de acceso de toda persona "*a consultar los documentos que reposen en las oficinas públicas y a que se le expida copia de los mismos, siempre que dichos documentos no tengan carácter de reservado conforme la Constitución o la ley, o no hagan relación a la defensa o seguridad nacional".*

En cuanto a las excepciones, esta Ley no cuenta con un artículo que las enuncie, lo que torna dificultosa la tarea de limitación, por lo que debemos acudir a artículos dispersos.

La primera limitante surge del propio artículo 12 al referirse a los documentos reservados, o que guarden relación a la defensa o seguridad nacional. Por su parte, el artículo 19 dispone que las investigaciones de carácter administrativo o disciplinario no estarán sometidas a reserva. Del mismo modo, el artículo 20, enuncia que el carácter reservado de un documento, no será oponible a las autoridades que lo soliciten para el debido ejercicio de sus funciones. Finalmente, corresponde tener presente el artículo 13 (modificado por el artículo 28 de la Ley N° 594 de 2000), que dispone que la reserva legal dura únicamente 30 años.

3.2.3 Ecuador

Este país cuenta con La Ley Orgánica de Transparencia y Acceso a la Información N° 2004-34[217], publicada el 18 de Mayo de 2004.

---

[216] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html Página visitada el 5 de Enero de 2012.

[217] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html Página visitada el 5 de Enero de 2012.

Su artículo 1, enuncia el acceso a la información pública como un derecho de las personas garantizado por el Estado. Por su parte el artículo 2 al establecer el objeto, erige a la ley como garante del derecho fundamental de las personas a la información, conforme a las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes para Ecuador.

En relación a las excepciones, el artículo 17 dispone que no procede el derecho de acceso cuando se trate de documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional, y cuando sean informaciones expresamente reservadas por leyes vigentes.

3.2.4 Guatemala

En el año 2008, este país aprobó su Ley de Acceso a la información Pública[218], según Decreto N° 57-2008 de 23 de Setiembre de 2008.

En su artículo 1.1, al definir sus objetos, dispone *"garantizar a toda persona, sin discriminación alguna, el derecho a solicitar y a tener acceso a la información pública en posesión de las autoridades y sujetos obligados por la presente ley"*. Según el artículo 5, dicho acceso es un derecho reconocido a *"toda persona individual o jurídica, pública o privada, que tiene derecho a solicitar, tener acceso y obtener la información pública que hubiere solicitado conforme lo establecido en esta ley"*.

El artículo 21 enuncia como excepciones al acceso, el que se trate de información confidencial por ley, reservada por ley, y las que de acuerdo a tratados o convenios internacionales ratificados tengan cláusula de reserva. Por su parte el artículo 22 define lo que se considera para la ley como información confidencial, y el artículo 23 lo que se considera como secreta.

Es de destacar, que esta ley exige que la clasificación de la información se fundamente en prueba de daño, demostrada en el cumplimiento de tres requisitos enunciados en su artículo 26.

3.2.5 Honduras

La Ley de Transparencia y Acceso a la Información[219] de Honduras, según Decreto N° 170-2006, fue publicada en el Diario Oficial La Gaceta el 30 de Diciembre de 2006.

Su artículo 4º in fine, establece que *"toda persona, natural o jurídica, tiene derecho a solicitar y a recibir de las Instituciones Obligadas, información completa, veraz, adecuada y oportuna en los límites y condiciones establecidas*

---

[218] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html .Página visitada el 5 de Enero de 2012.

[219] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html Página visitada el 5 de Enero de 2012.

en esta Ley".

Sobre las excepciones, el artículo 16 previene como restricción de acceso a la información, el estar establecido por la Constitución, las leyes, los tratados o ser declarada como reservada o confidencial conforme la propia ley; así como todo lo que corresponda a instituciones y empresas del sector privado que no esté comprendido en la obligaciones que señala esta ley y leyes especiales; como también las fuentes periodísticas dentro de los órganos del sector público y la información a periodística que haya sido debidamente publicada y obre en los archivos de las empresas de medios de comunicación. Por su parte, los artículos 17 y 18 enuncian la forma de clasificación de la información como reservada.

Además, se formulan las siguientes excepciones específicas:
- Información confidencial (artículo 3.7)
- Información proporcionada por terceros que la ley considera confidencial (artículo 3.9)
- Información que pudiere arriesgar la seguridad del Estado (17.1), la vida o salud de cualquier persona o la ayuda humanitaria; los intereses jurídicamente tutelados a favor de la niñez y de otras personas o por la garantía de Habeas Data(17.2); la investigación, prevención o prosecución de de delitos o la impartición de justicia (17.3); el interés protegido por la Constitución y la ley (17.4); la conducción de negociaciones o relaciones internacionales (17.5); la estabilidad económica, financiera o monetaria del país o su gobernabilidad (17.6).

3.2.6 México

Pionero y ejemplo en la materia, cuenta con una Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[220], publicada en el Diario Oficial de la Federación el 11 de Junio de 2002.

Su artículo 2º, expresa la regla *"Toda la información gubernamental a que se refiere esta Ley es pública y los particulares tendrán acceso a la misma en los términos que ésta señala".*

En cuanto a las excepciones, el artículo 7º erige como excepciones la información reservada o confidencial prevista en la ley, conforme los artículos 13 y 14 definirán.

Entre las causales de clasificación de la información como reservada, encontramos aquella cuya difusión pudiere comprometer la seguridad nacional, pública o la defensa nacional; menoscabar la conducción de las negociaciones o relaciones internacionales; dañar la estabilidad financiera, económica o monetaria del país; poner en riesgo la vida, la seguridad o la salud o causar serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, impartición de justicia y operaciones de control migratorio, entre otros.

---

[220] Disponible en: http://www.informacionpublica.gub.uy/sitio/normativas-internacionales-legislacion.html Página visitada el 5 de Enero de 2012.

4. CLASIFICACIÓN DE LA INFORMACIÓN

Clasificar, del latín *classificāre*, significa ordenar por clases. Clasificación: acción y efecto de clasificar[221].

Según el artículo 17 del Decreto N° 232/010, clasificación es el *"procedimiento por el cual se determina que la información de un sujeto obligado es información confidencial o reservada".*

De acuerdo a lo dispuesto por el artículo 8º de la Ley N° 18.381, las excepciones a la información pública serán de interpretación estricta y *"comprenderán aquellas definidas como secretas por la ley y las que se definan seguidamente como de carácter reservado o confidencial".*

Significa que para nuestro ordenamiento jurídico, existen tres excepciones a la la información pública y por ende a su acceso: la secreta, que será establecida por ley, la reservada y la confidencial, que serán las así clasificadas de acuerdo a la propia Ley y su Decreto reglamentario.

4.1 Información secreta

Esta excepción, salvaguarda el deber de secreto dispuesto en otras leyes.

Nuestro ordenamiento jurídico cuenta con copiosa legislación que impone secreto. La Unidad de Acceso a la Información Pública ha realizado la valiosa tarea de relevamiento de dichas normas[222], que se transcriben a continuación:

4.1.1 Secretos comerciales-industriales

- Código de Comercio, art. 101 por el que se establece dentro de las obligaciones de los corredores la de guardar secreto de las negociaciones que se les encargan.
- Código Civil, art. 2256, establece la obligación del depositario respecto a no violar el secreto de un depósito de confianza, asimismo tampoco puede obligarlo a revelarlo.
- Ley N°4.294, de 7 de enero de 1913, art. 4° por el que se establece que la oficina de estadísticas y publicaciones del Ministerio de Industria no debe comprometer el secreto de industria.
- Ley N° 10.089, de 12 de diciembre de 1941, art. 47 el que determina que las solicitudes de patentes de invención denegadas, desistidas y abandonadas se deben conservar en un archivo secreto.
- Ley N° 11.923, de 27 de marzo de 1953, art. 66 que establece la obligación que tienen los residentes en el país de presentar datos estadísticos requeridos por la Dirección General de Estadística y Censos. Dichos datos no deben comprometer el secreto del giro

[221] Disponible en: www.rae.es. Página visitada el 4 de Enero de 2012.
[222] Disponible en http://www.informacionpublica.gub.uy/Sitio/normativa.html. Página visitada el 5 de Enero de 2012.

comercial.

- Ley N° 13.669, de 1 de julio de 1968, por la que se ratifica el Tratado para la proscripción de armas nucleares en América Latina crea un órgano que tiene como obligación la no revelación de secretos de fabricación.
- Ley N° 14.541, de 20 de julio de 1976, art. 5° por el que se establece la protección de los secretos comerciales en el ámbito de la Organización Internacional de Energía Atómica.
- Ley N° 17.102, de 16 de mayo de 1999, art. 1° por el que se incluye dentro de la propiedad intelectual al secreto comercial.
- Ley N° 17.164, de 2 de setiembre de 1999, art. 109 por el que se determina que la solicitud de patente es secreta hasta su publicación.

4.1.2 Secretos que deben guardar los funcionarios

- Ley N° 15.098, de 23 de diciembre de 1980, art. 3° por el que se establece el deber que tienen los policías de no divulgar hechos o documentos que deban permanecer secretos.
- Ley N° 15.524, de 9 de enero de 1984, art. 65 por el que se determina que los miembros del Tribual de lo Contencioso Administrativo al dictar sentencia no pueden tomar en cuenta afirmaciones del actor que estén comprendidas dentro del secreto administrativo.
- Ley N° 15.605, de 27 de julio de 1984, art. 15 por el cual el presidente de la Junta Directiva del Instituto Nacional de Carnes proporcionará a los demás miembros de la Junta las informaciones reservadas pudiendo establecer la obligatoriedad de la preservación del secreto.
- Ley N° 15.709, de 28 de enero de 1985, art. 27 por el que se establece el secreto que deben guardar los funcionarios de ANTEL sobre ciertos asuntos teniendo en cuenta su naturaleza o instrucciones especiales.
- Ley N° 16.736, de 5 de enero de 1996, art. 26 por el que se estatuye el secreto que deben guardar los funcionarios del MGAP en cumplimiento de funciones inspectivas.
- Ley N° 18.401, de 24 de octubre de 2008, art. 27 el que determina que los empleados de la Corporación de Protección del Ahorro Bancario deben guardar secreto profesional.

4.1.3 Secreto de las comunicaciones

- Ley N° 14.705, de 23 de setiembre de 1977, art. 22, Ley N° 15.604, de 27 de julio de 1984, art. 22 y Ley N° 16.303, de 14 de setiembre de 1992, art. 23 aseguran el secreto de las telecomunicaciones en el ámbito del Convenio Internacional de Telecomunicaciones.
- Ley N° 16.967, de 10 de junio de 1998, art. 26 por el que se asegura el secreto de la correspondencia internacional.
- Ley N°17.930, de 19 de diciembre de 2005, art. 77 por el que se establece que la política postal debe asegurar secreto de la correspondencia.

4.1.4 Secreto bancario – tributario

- Ley N° 14.306, de 29 de noviembre de 1974, art. 47 por el que se establece el secreto que debe guardar la Administración Tributaria en relación con todas las actuaciones administrativas o judiciales.
- Ley N° 15.322, de 17 de setiembre de 1982, art. 25 determinante del secreto que deben guardar las personas dedicadas a la intermediación financiera.
- Ley N° 16.696, de 30 de marzo de 2002, art. 22 por el que se señala el secreto que debe guardar el B.C.U. cuando ejerce actividad financiera.
- Ley N° 17.292, de 25 de enero de 2001, art. 57 por el que se excluye del secreto bancario todo lo relativo al R.A.V.E. inclusive la información contenida en las declaraciones juradas.
- Ley N° 17.704, de 27 de octubre de 2003, art. 12 por el que se establece que en caso de represión de la financiación del terrorismo no procede el secreto bancario.
- Ley N° 17.861, de 28 de diciembre de 2004, art. 12 que establece que en caso de represión de la delincuencia organizada no procede el secreto bancario.
- Ley N° 18.241, de 27 de diciembre de 2007, art. 6° que releva del secreto bancario al BPS respecto al Mides.
- Ley N° 18.485, de 11 de mayo de 2009, art. 50 que releva el secreto bancario de los partidos políticos respecto a la Corte Electoral.

4.1.5 Secreto estadístico

- Ley N° 15.664, de 30 de octubre de 1984, art. 4° por el que se establece el secreto estadístico para registros del B.R.O.U.
- Ley N° 16.616, de 20 de octubre de 1994, por la que se regula el Sistema Estadístico Nacional, regido por el secreto estadístico.

4.1.6 Secreto profesional

- Ley N° 14.005, de 17 de agosto de 1971, art. 2º por el que se determina que es secreta la información en poder del Registro Nacional de Órganos y Tejidos.
- Ley N° 16.099, de 3 de noviembre de 1989, art. 1° por el que se establece el secreto profesional de los periodistas respecto a sus fuentes.
- Ley N° 16.774, de 27 de setiembre de 1996, por la que se consagra el secreto profesional sobre los fondos de inversión.
- Ley N° 17.202, de 24 de setiembre de 1999, cap. V, art. 5°, extiende las disposiciones del secreto profesional de la Ley N° 15.322 a las sociedades administradoras de fondos de inversión.
- Ley N° 17.613, de 27 de diciembre de 2002, art. 30 por el que se establece el secreto profesional de las actuaciones de la comisión auditora del B.C.U.
- Ley N° 17.823, de 7 de setiembre de 2004, art. 22 por el que se resguarda con el secreto profesional los indicadores de desarrollo de niños y adolescentes.

- Ley N° 18.243, de 27 de diciembre de 2007, art. 19 por el que se determina que los expedientes e informaciones del B.S.E. están amparados por el secreto profesional.
- Ley N° 18.331, de 11 de agosto de 2008, art. 11 por el que se establece el secreto profesional que están obligados a guardar quienes acceden o intervienen en el tratamiento de datos personales.
- Ley N° 18.387, de 23 de octubre de 2008, art. 76 por el que se determina la inoponibilidad del secreto profesional de las entidades de intermediación financiera al síndico o interventor.
- Ley N° 18.494, de 5 de junio de 2009, art. 7º por el que se establece el secreto profesional para los funcionarios de la Unidad de Información y Análisis Financiero.

4.1.7 Secreto político y militar

- Código Penal en su art. 132, establece que es delito contra la patria la revelación de secretos políticos o militares.
- Ley N° 10.506, de 18 de setiembre de 1941, art. 424 por el que se determina como secreto el trámite referente a la organización y el material bélico de las instituciones armadas.
- Ley N° 13.737, de 9 de enero de 1969, art. 41 por el que se exime de explicitación a los programas del Ministerio de Defensa Nacional que refieran a planes militares secretos.
- Ley N° 14.157, de 21 de febrero de 1971, art. 61 por el que se establece el secreto profesional militar que debe guardar todo el personal militar.
- Ley N° 17.728, de 26 de diciembre de 2003, art. 4º que excluye los secretos de estado de la cooperación técnico-militar con Rusia.

4.1.8 Otras disposiciones

- Ley N° 9.515, de 28 de octubre de 1935, art. 11 por el que se establece que las Juntas Departamentales pueden declarar secretas las sesiones.
- Ley N° 13.711, de 6 de octubre de 1969, art. 4º por el que se garantiza el secreto del registro sobre menores con retardo mental que lleva el M.S.P.
- Ley N° 14.294, de 31 de octubre de 1974, art. 23 por el que se establece el carácter secreto del registro que lleva la Comisión Nacional de Lucha contra la Toxicomanía.
- Ley N° 16.698, de 25 de abril de 1995, art. 15 por el que el Poder Ejecutivo puede declarar secretos asuntos del Ministerio de Defensa Nacional, Ministerio de Economía y Finanzas, Ministerio del Interior y Ministerio de Relaciones Interiores.
- Ley N° 16.758, de 26 de junio de 1996, art. 2º por el que las comisiones investigadoras parlamentarias pueden declarar secretas algunas actuaciones.
- Ley N° 16.775, de 1 de octubre de 1996, art. 15 por el que se establece el carácter secreto de la información personal que se transmita dentro del marco del Convenio de seguridad Social con Grecia.
- Ley N° 17.613, de 27 de diciembre de 2002, art. 3º por el que se

garantiza el secreto de la identidad de los denunciantes ante el B.C.U.

- Ley N° 17.668, de 15 de julio de 2003, art. 2º por el que se garantiza el secreto de la información del Registro Nacional de Órganos y Tejidos.
- Ley N° 18.336, de 21 de agosto de 2008, art. 7° por el que se garantiza el secreto de las adopciones internacionales.

4.2 Información reservada

El artículo 9º de la Ley N° 18.381, establece que podrá clasificarse como información reservada la que pueda comprometer la seguridad pública o la defensa nacional; menoscabar la conducción de las negociaciones o relaciones internacionales; dañar la estabilidad financiera, económica o monetaria del país; poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona; suponer una pérdida de ventajas competitivas para el sujeto obligado o dañar su proceso de producción y desproteger descubrimientos científicos, tecnológicos o culturales.

Por su parte el Decreto N° 232/010 dispone en su artículo 20 que *"la documentación clasificada como reservada, de acuerdo con lo establecido en el artículo 9 de la ley que se reglamenta, deberá tener incluida una leyenda indicativa de carácter reservado, la fecha de su clasificación, su fundamento legal, el período de reserva y la firma de la autoridad correspondiente"*.

Asimismo, en el artículo 21, el Decreto regula el procedimiento de clasificación, exhortando a que la clasificación se realice por la autoridad administrativa por resolución fundada.

Importante deviene el artículo 25 del Decreto, que exige *"prueba de daño"* para que la información pueda ser clasificada como reservada. Esta prueba, implica demostrar la existencia de elementos objetivos que permitan determinar la expectativa razonable de un daño al interés público protegido.

Finalmente, el artículo 26 del Decreto de referencia, establece como supuestos de desclasificación, a) el vencimiento del periodo de reserva; b) la extinción de los motivos que originaron la clasificación; c) a instancias del órgano de control (UAIP- Unidad de Acceso a la Información Pública) y d) cuando una resolución judicial así lo disponga.

En suma, para clasificar información como reservada se requiere:
• Que se trate de alguna de las hipótesis prevista en el artículo 9° de la Ley N° 18.381.
• Haber sometido la información a reservar a "prueba de daño".
• Que se realice por la autoridad competente mediante acto fundado.
• Que la información así clasificada porte leyenda de reserva, fecha de clasificación, fundamento legal, período y firma de autoridad.

4.3 Información confidencial

El artículo 10 de la Ley N° 18.381, considera información confidencial *"aquella entregada en tal carácter a los sujetos obligado siempre que: a) refiera al patrimonio de la persona, b) comprenda hechos o actos de carácter económico, contable, jurídico administrativo, relativos a una persona física o jurídica, que pudiera ser útil para un competidor, c) esté amparada por una cláusula contractual de confidencialidad; los datos personales que requieran previo consentimiento informado".*

El Decreto N° 232/010 por su parte en su artículo 29, nos dice que no es confidencial la información que *"a. por disposiciones legales se encuentre en registros públicos" y "b. la que se encuentre en fuentes de acceso público. En este caso, se dará a conocer a quien la solicita: fuente, lugar y forma de acceder a la información que se pretende".*

En cuanto a la información confidencial entregada por los particulares en tal carácter a los sujetos obligados, conviene tener presente las disposiciones del artículo 30 del citado Decreto, que señala que deberán indicarse los documentos o secciones que contengan tal información, así como presentarse un resumen no confidencial breve y conciso.

De igual forma que la información reservada, la confidencial habrá de clasificarse por resolución fundada de la autoridad administrativa competente, de acuerdo al artículo 31 numeral II del mencionado Decreto.

Por último, corresponde destacar que según lo previene el artículo 32 del Decreto *"la información confidencial no está sujeta a plazos de vencimiento y tendrá ese carácter en forma indefinida".*

En suma, para clasificar información como confidencial se requiere:
• Que se trate de alguna de las hipótesis previstas en el artículo 10 de la Ley N° 18.381.
• Que no se encuentre en registros públicos ni en fuentes accesibles al público.
• Que se haya señalado por el particular los documentos o secciones confidenciales y presentado un resumen breve.
• Que se realice por resolución fundada de la autoridad competente.

5. CONCLUSIONES

El gran desafío que enfrentan las legislaciones latinoamericanas en la materia, radica en evitar que las excepciones se transformen en la regla e impidan que se cumpla con el objetivo de ejercitar el derecho fundamental de acceso a la información pública.

Lograr cumplir la regla, implica evitar que los sujetos obligados encuentren en las excepciones un escape para incumplir la Ley, una excusa bajo cuya

denominación clasificar la mayor parte de la información en su poder, evitando su publicidad.

Entonces ¿cómo hacer para que las excepciones no devengan la regla? Entiendo que la respuesta se encuentra en la redacción de una ley que respete el principio de limitación de excepciones, unida a una responsable clasificación de la información por parte de los sujetos obligados, y un adecuado control desde el órgano competente.

Sin perder de vista que las leyes son herramientas y no soluciones en sí mismas. Tan importante como legislar es educar en relación a que el acceso a la información pública es un derecho fundamental, cuyo ejercicio contribuye a la transparencia en el actuar estatal y consiguiente mejora del Estado de Derecho.

CAPÍTULO XII - OBLIGACIÓN DE TRANSPARENCIA ACTIVA

"La libertad no es posible
más que en aquellos países
en que el derecho predomina
sobre las pasiones."
Henri Dominique Lacordaire.

Dra. Silvana Casciotti

1. INTRODUCCIÓN

Si bien actualmente no parece fácil hablar de democracia sin transparencia, lo cierto es que ésta responde a una nueva forma de relación entre Estado y Sociedad que surge en las últimas dos décadas del Siglo XX. Democracia y transparencia han desarrollado un vínculo cada vez más estrecho hasta el punto de que casi no queda país democrático que no tenga o que no ponga en discusión la pertinencia de poseer una ley de transparencia.

La exigencia de la transparencia es relativamente nueva y su origen no es propiamente político sino de talante económico ya que se ha dado un crecimiento cada vez mayor en las relaciones entre el Estado y la sociedad debido a la globalización e interconexión de los mercados, el flujo de los seres humanos y de los bienes; la tecnología: la posibilidad de transmitir información a velocidades instantáneas, la sistemática comparación entre países y sus ventajas asociadas para la toma de decisiones y, por otra parte, la necesidad de contar con mayor y mejor información sobre su verdadero funcionamiento.

De ahí que los promotores principales de las mejores prácticas de transparencia hayan sido, al menos al comienzo, los grandes organismos económicos internacionales, como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Banco Mundial.

Ha habido un crecimiento de naciones democráticas. La democracia va cambiando y adaptándose a las exigencias de los ciudadanos de los países globalizados. Dicha ciudadanía es más compleja, informada, cultivada políticamente y exigente al momento de solicitar información.

Por intermedio del artículo 4° de la Carta Democrática Interamericana de la Asamblea general de la organización de Estados Americanos, se establece que: "Son componentes fundamentales del ejercicio de la democracia la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa. La subordinación constitucional de todas las instituciones del Estado a la autoridad civil legalmente constituida y el respeto al estado de derecho de todas las entidades y sectores de la sociedad son igualmente fundamentales para la democracia".

Conforme a esta disposición, no es suficiente que un Gobierno sea elegido a través del sufragio universal sino que es necesario que dicho Gobierno sea transparente en el ejercicio de sus actividades gubernamentales. Para lograr la trasparencia es necesario garantizar el derecho de acceso de los ciudadanos a la información gubernamental, ya que les permite analizar, juzgar y evaluar los actos de sus representantes. Por otra parte estimula los actos del Gobierno y de la Administración.

No se debe mirar a la transparencia como un obstáculo engorroso con el cual los gobiernos democráticos deben lidiar, sino como una fortaleza, ya que la transparencia es un principio tan útil como la eficiencia, sólo que no es natural ni armónico con las prácticas típicas de las burocracias antiguas y contemporáneas.

La transparencia debe ser considerada como una forma de gobernar, administrar y gestionar el Estado. Los procesos internos deben desarrollarse con claridad y tienen que ser conocidos, deliberados y expuestos a la crítica y al conocimiento de los ciudadanos. Los gobiernos no solamente deben permitir que los ciudadanos los observen, sino que también deben divulgar activamente la información que poseen.

Existe un gran consenso en la relevancia del tema "transparencia" y en la incorporación como premisa básica en las prácticas gubernamentales. Sin embargo, los alcances de esta práctica gubernamental son confusos y por tanto resulta difícil traducirlo en acciones concretas.

"La transparencia no implica una suerte de rendición de cuentas a una persona determinada, sino que se trata de una práctica democrática mediante la cual se coloca la información gubernamental bajo la lupa de la publicidad, para que las personas puedan efectuar las tareas que entiendan pertinentes vinculadas con su revisión, análisis y en caso de entenderlo adecuado activar mecanismos sancionatorios". "El concepto alude a un sector público abierto al público en general, al electorado y a los mercados financieros, en todo lo que atañe a estructura, comportamiento, intenciones, contabilidad, indicadores y predicciones. Aquí nos referimos al sector público en el sentido amplio, abarcando aun las empresas estatales (o lo que queda de ellas), incluso a ciertas actividades estatales desempeñadas por el sector privado. Transparencia significa acceso fácil y oportuno a información fidedigna, completa, comprensible y comparable en el ámbito internacional."[223]
O´Donnell respondería mediante un esquema que obliga a la rendición de cuentas de manera horizontal y vertical:[224] horizontal por los contrapesos entre instituciones y organizaciones que se vigilan y controlan mutuamente; vertical: por la doble vía que los americanos llaman top-down y bottom up: por un lado las jerarquías de arriba hacia abajo que controlan y exigen cuentas claras a los subordinados, y del otro, los ciudadanos, las organizaciones y las empresas que de abajo hacia arriba quieren ser informados sobre lo que está haciendo el gobierno.

[223] NAHABETIÁN BRUNET, Laura. Ob. Cit., pág. 185.
[224] O`DONNELL, Guillermo. Horizontal Accountability, and New Polyarchies. Kellog Institute for International Studies. Working Paper No.253. Abril de 1998.

De manera que la transparencia se traduce en un sistema de redes en que todos controlan a todos, y todos le piden y rinden cuentas a todos.

El buen funcionamiento de la democracia depende en gran medida de la libre circulación de información y las naciones desarrolladas del mundo reconocen esta realidad. El acceso a la información es crucial para el establecimiento y promoción de la democracia y la tendencia internacional hacia la transparencia queda demostrada por el hecho de que más de cincuenta países han promulgado en la última década una gran cantidad de leyes de acceso a la información.

Si bien actualmente la mayoría de los países están de acuerdo con la importancia del valor de la transparencia y de un gobierno abierto, algunos incluso han avanzado y han adoptado medidas drásticas para promover la transparencia, reconociendo que los ciudadanos tienen el derecho básico a la información y al debate público.

Sin embargo, aún son demasiados los que retienen información y restringen a los medios de comunicación que intentan mantener al público informado.

"Es hora de que las cosas cambien. El acceso a la información constituye un componente fundamental dentro de una estrategia de desarrollo exitosa. Si somos serios en nuestro propósito de reducir la pobreza global, debemos liberar el acceso a la información y mejorar su calidad".[225]

2. CONCEPTO DE TRANSPARENCIA ACTIVA

El concepto de transparencia se usa en ocasiones como sinónimo de rendición de cuentas. La transparencia es una característica que abre la información de las organizaciones políticas y burocráticas al escrutinio público mediante sistemas de clasificación y difusión que reducen los costos de acceso a la información del Gobierno. Sin embargo la transparencia no aplica un acto de rendir cuentas a un destinatario especifico, sino a la práctica de colocar la información en la vitrina publica para que los interesados puedan revisarla, analizarla y, en su caso, usarla con mecanismos para sancionar en caso de que haya anomalías en su interior. Al igual que en el caso de la fiscalización, la transparencia es solo un instrumento de un sistema global de rendición de cuentas.

Cuando se habla de transparencia activa se hace referencia a la obligación de los órganos del Estado de difundir regularmente información actualizada sin que nadie lo solicite, como una manera de transparentar la gestión.

"Así es que las obligaciones de transparencia activa implican la determinación que se hace a las entidades gubernamentales de presentar en forma permanente información sobre sí mismas a través de sus páginas web.

---

[225] "Más y mejor información reduce la pobreza". Diario Clarín, 3 de enero de 2002. Joseph Stiglitz es Premio Nobel de Economía y Roumeen Islam es Gerente del Instituto del Banco Mundial. Copyright Clarín y Le Monde, 2003.

Ahora bien, junto con esto es pertinente tener en cuenta que como dice Manuel Castells, “los poderes tienen miedo de internet”.

Internet y su poder globalizador concretizan los tan ansiados sistemas de acercamiento ampliando y restringiendo al mismo tiempo las libertades y la autonomía de las personas. En el mismo sentido, esto sucede con las entidades públicas que de alguna forma pierden sus posibilidades de control sobre toda su información porque como decía Castells, “internet no se puede controlar”...Lo cierto es que al dar cumplimiento a estas obligaciones, en general, al menos al principio no por voluntad propia sino en función de que se trata de obligaciones de índole legal y constitucional, las entidades públicas quedan expuestas y no pueden ocultar u ocultarse más. Esto es, se verifica una suerte de emplazamiento en la obtención por parte de los ciudadanos de las respuestas que interiormente se hacen, y éstas deben aparecer, lo que en definitiva termina por generar un nuevo tipo de vínculo mucho más democrático y por lo mismo mucho menos asimétrico.

Las obligaciones de transparencia activa se establecen entre otros motivos con finalidades muy claramente determinadas. “El objetivo a más largo plazo debe ser el hacer que la información esté disponible proactivamente, para minimizar la necesidad de que los individuos tengan que recurrir a solicitudes para acceder a la misma”.[226]

¿Qué información debe publicarse?

Los organismos públicos, sean o no estatales, deberán tener en sus sitios Web un banner de Gobierno Transparente, donde se podrá encontrar información sobre: la estructura orgánica, la estructura de remuneraciones por categoría escalafonaria, funciones de los cargos y sistema de compensación, información sobre presupuesto asignado, su ejecución, con los resultados de las auditorías que en cada caso corresponda. Concesiones, licitaciones, permisos o autorizaciones otorgadas, especificando los titulares o beneficiarios de éstos; toda información estadística de interés general, de acuerdo a los fines de cada organismo y mecanismos de participación ciudadana, en especial domicilio y unidad a la que deben dirigirse la solicitudes para obtener información.

Para alcanzar la máxima transparencia y el establecimiento de la cultura de la rendición de cuentas es un tema de conciencia y voluntad política para su concreción.

En América Latina el gobierno del Presidente Vicente Fox, con la aprobación de la Ley Federal Mexicana y la creación del IFAI, ha sido un claro ejemplo de voluntad política y compromiso con respecto a la promoción de políticas anticorrupción y promoción de transparencia.

En este sentido, en uno de sus discursos políticos éste manifestó que: “La eliminación de la corrupción no es imposible. Sin embargo, es sin duda una

[226] NAHABETIÁN BRUNET, Laura. Ob. Cit., pág. 208.

tarea difícil que requiere algo que está claramente presente hoy en esta sala: la voluntad política firme y un deseo compartido por nuestras naciones de asegurar que los recursos necesarios para el desarrollo de los pueblos no sean sustraídos por la delincuencia y la corrupción, en particular dentro de las instituciones estatales. Es una tarea que también requiere gran determinación: la determinación para combatir tanto la criminalidad como sus causas; la perseverancia para cambiar las prácticas perjudiciales arraigadas en una inercia de raíz profunda y de larga data; y la perseverancia para crear una nueva cultura de la legalidad basada en la confianza, la transparencia, la rendición de cuentas y la certidumbre en cuanto a la aplicación efectiva de la ley.

Al fortalecer la lucha contra la corrupción estamos también fortaleciendo nuestros esfuerzos para combatir la pobreza, la exclusión, la desigualdad y la injusticia, y estamos recalcando que, tanto en teoría como en la práctica, el Estado existe para proteger al pueblo y asegurar el establecimiento de las condiciones necesarias para su desarrollo".[227]

Cuando nos referimos a Transparencia y Acceso a la Información del Gobierno, inmediatamente pensamos en un derecho humano que puede ejercer cualquier persona. Comprende pues, un derecho humano irrenunciable.

"Transparencia y acceso a la información son conceptos diferentes. La transparencia es una práctica o un instrumento que utilizan las organizaciones para publicar o volver público cierto tipo de información o bien para abrir al público algunos procesos de toma de decisiones. El derecho de acceso a la información, por su parte consiste en un "conjunto de normas jurídicas que permiten analizar los registros y datos públicos en posesión de los órganos del Estado"[228]. Por consiguiente, es un derecho que permite a los ciudadanos pedir documentos al gobierno.

Dentro del concepto de transparencia se encuentra inserto el de rendición de cuentas (Accountability). Andreas Schedler, explica que el término accountability no tiene una traducción exacta al español, pero que el término que más se aproxima es rendición de cuentas.[229]

El autor expresa que la rendición de cuentas tiene dos dimensiones básicas. Por un lado, se encuentra la obligación de los políticos y funcionarios de informar sobre sus decisiones y de justificarlas en público (answerability). Por otro lado, incluye la capacidad de sancionar a políticos y funcionarios en caso de que hayan violado sus deberes públicos (enforcement).

La rendición de cuentas establece un dialogo entre los actores que exigen y los que rinden cuentas, requiere la participación de ambos actores involucrándolos

---

[227] ORGANIZACIÓN DE LAS NACIONES UNIDAS. Oficina contra la Droga y el Delito, "Acción Mundial contra la Corrupción", Los documentos de Mérida, págs. 4 y 5.
[228] HERNANDEZ VALDEZ, Alfonso. "¿Qué es y para qué sirve la transparencia?", Recta Ratio, año 1, núm. 2 (enero-junio 2005)
[229] SCHEDLER, Andreas. "¿Qué es la rendición de cuentas?" en Cuadernos de Transparencia Nº3 IFAI. México, 2004, pág.11.

en un debate público. “Involucra el derecho a recibir información y la obligación correspondiente de divulgar todos los datos necesarios. Pero también implica el derecho a recibir una explicación y el deber correspondiente de justificar el ejercicio de poder”[230].

Se trata de un juego interactivo en el cual los poderes públicos rinden cuentas a los administrados, y a su vez los ciudadanos participan de forma activa en la política solicitando informaciones y justificaciones de todas las decisiones que se toman. De esta manera los actores que exigen cuentas cuestionan y monitorean el comportamiento inadecuado de los servidores públicos.

El objetivo de la rendición de cuentas en definitiva es limitar las arbitrariedades e incertidumbres del poder, prevenir y sanear sus abusos, en definitiva también se trata de una de las medidas más eficaces para combatir la corrupción.

El concepto de accountability, comprende tanto el de transparencia activa – obligación de los organismos públicos de tener a disposición a través de su portal web toda la información referente al ejercicio del poder y las actividades que los gobiernos llevan a cabo – como el de transparencia pasiva referente a la obligación que tienen las entidades públicas de responder las solicitudes de acceso a la información.

“Transparencia activa implica, por tanto, que la información pueda estar al alcance de todos los ciudadanos sin discriminación. La apertura de la información, cuando las decisiones y políticas se forman, abre por su parte, las oportunidades a la deliberación pública y, por tanto, al control ex ante de parte de la sociedad. En este sentido el libre acceso a la información pública por parte de los ciudadanos constituye un mecanismo que se engrana cabalmente en el concepto de la “accountability social”.[231]

El Dr. Carlos Delpiazzo, expresó con respecto al significado de transparencia que: “La transparencia es más que la publicidad. Publicidad supone dar a conocer algo que ya se hizo, mientras que transparencia supone que la sociedad pueda, efectivamente, ir conociendo lo que la administración hace mientras lo está haciendo.

La propia palabra transparencia indica que visualiza a la Administración como si estuviera en una vidriera; y es así como debe estar. Si los mecanismos de control funcionaran adecuadamente, esto sería más notorio o visible. Incluso, la Ley Anticorrupción dedica un Capítulo a lo que denomina el Control Social y este no es posible de ser llevado a cabo en plenitud si no hay transparencia en el obrar de la Administración”[232]. Por consiguiente, la transparencia implica ver

---

[230] SCHEDLER, Andreas. Ob. Cit., pág.14.

[231] CUNILL GRAU, Nuria. “La Rendición de cuentas y el control social. Una aproximación conceptual”, págs. 1 a 21. Consultable en: http://www.seminarioprotecciondeprogramas.org.mx/ponencias/Conference_Paper_Cunill.pdf página visitada el 15 de febrero de 2011.

[232] RIVOIR, Laura y RÍOS, Mauro. “Análisis general y Diagnóstico sobre la sociedad de la Información y el Conocimiento” en Libro Verde de la SIC en Uruguay. Montevideo, Mayo 2007, pág.100.Disponibleen:http://www.desarrolloregional.org.uy/portal/dmdocumentos/libro_verde_uruguay.pdf. Página visitada el 15 de febrero de 2011.

en tiempo real las actuaciones de la Administración y es un mecanismo eficaz contra la corrupción.

A principios de los años 90, la corrupción no era un tema abarcado por los círculos oficiales, aunque todos sabían de su existencia. Actualmente, están todos de acuerdo en que la corrupción debilita las instituciones democráticas y el Estado de derecho, perjudica el orden social y destruye la confianza pública, dando lugar a que prosperen la delincuencia organizada, el terrorismo y otras amenazas para la seguridad humana. La corrupción es, por consiguiente, un obstáculo importante a la estabilidad política y al éxito del desarrollo social y económico. Por tanto, la eliminación de la corrupción es una responsabilidad de los Estados, y es fundamental contar con el apoyo y participación de la sociedad civil.

El derecho a la información y a la comunicación del ciudadano comprende libre acceso a la información pública. Además de estar consagrados estos derechos en el Pacto de San José de Costa Rica, ellos mismos constituyen normas jurídicas de obligatorio cumplimiento en el derecho nacional de los países miembros de este Pacto por haber sido ratificados por los poderes legislativos de dichos países.

En este sentido, en Uruguay la Transparencia activa es una obligación establecida por la Ley de Acceso a la información pública (Ley Nº 18.381, de 17 de octubre de 2008) en su artículo 5º. Dicho artículo establece que: “Los sujetos obligados deberán prever la adecuada organización, sistematización y disponibilidad de la información en su poder, asegurando un amplio y fácil acceso a los interesados. Los organismos públicos, sean o no estatales, deberán difundir en forma permanente, a través de sus sitios web u otros medios que el órgano de control determine, la siguiente información mínima: a)

Su estructura orgánica, b) Las facultades de cada unidad administrativa, c) La estructura de remuneraciones por categoría escalafonaria, funciones de los cargos y sistema de compensación, d) Información sobre presupuesto asignado, su ejecución, con los resultados de las auditorías que en cada caso corresponda, e) Concesiones, licitaciones, permisos o autorizaciones otorgadas, especificando los titulares o beneficiarios de éstos, f) toda información estadística de interés general, de acuerdo a los fines de cada organismo, g) Mecanismos de participación ciudadana, en especial domicilio y unidad a la que deben dirigirse las solicitudes para obtener información”.

Los sujetos obligados deberán presentar en sus páginas web determinada información denominada mínima sobre una serie de temas que hacen a su estructura, funcionamiento, organización, utilización de recursos entre otros aspectos. De esta manera la persona interesada podrá obtener la información mínima sin necesidad de efectuar solicitud de tipo alguno para acceder a la misma.

El Decreto Nº 484/009, de 19 de octubre de 2009, exhortó al cumplimiento de la transparencia activa estipulada por el artículo 5º de la Ley Nº 18.381.

El Decreto Reglamentario Nº 232/010 de 2 de agosto de 2010, por su parte, en su artículo 38, concreta la información que las entidades están obligadas a difundir en sus sitios web y que deben actualizar mensualmente. Se resalta como positivo que el decreto extiende las obligaciones de cada entidad respecto a la información que debe difundir en su sitio web oficial.

Sin embargo transparencia y el acceso no derivan automáticamente de los regímenes democráticos sino que hay que realizar un arduo trabajo para construirse, aplicarse, concientizarse. No basta con tener una buena ley y decretos que la reglamenten sino que hace falta también cambiar hábitos del modo en el que está organizado el trabajo democrático.

Para que el sistema de transparencia del Estado funcione, éste debe desarrollar políticas públicas coherentes que permitan a los ciudadanos acceder a la información y que promuevan una cultura de transparencia de toda la administración pública.

"La información es poder", quien concentra la información, concentra el poder. Los despotismos aman el secreto porque odian compartir el poder con el pueblo soberano. Una ciudadanía informada es una ciudadanía con poder.

Aquellos países que han cultivado la transparencia de sus instituciones son hoy sociedades desarrolladas cuyos habitantes gozan de buena calidad de vida. Por el contrario, aquellos países con historias de escasa práctica democrática, instituciones débiles y gobiernos autoritarios son proclives al secreto.

"Aquellos países que tienen mejor calificación en el índice de percepción de la corrupción (Corruption Perception index -CPI-) que elabora la organización Transparency International, son aquellos que tienen normas y políticas de amplio acceso a la información pública. Por eso, es fundamental impulsar legislación y políticas activas en esta dirección".[233]

Los Estados que están mejor calificados conforme al mencionado CPI, son algunos de los países más desarrollados del mundo. Dentro de los países con mejores calificaciones se encuentran Finlandia, Islandia, Dinamarca, Nueva Zelanda, Suecia, Holanda, Australia, Noruega, Suiza, Canadá y Reino Unido.
Para poder alcanzar estos objetivos resulta necesario cambiar una sociedad construida desde el secreto y transformarla en una sociedad abierta, donde la corrupción sea la excepción, y no la regla. Para lograr esto se requiere de controles que están o deberían estar a cargo de las entidades estatales creados al efecto.

Pero para que este sistema de controles pueda funcionar eficientemente, todos ellos deben contar con información. Sólo con datos concretos podremos responder algunas de las preguntas críticas que derivan de un adecuado control de la gestión pública. No se puede controlar la gestión de los asuntos públicos si antes no cuenta con información veraz, completa, precisa, relevante

---

[233] THE CARTER CENTER. "La Promoción de la Democracia a través del Acceso a la información", mayo de 2004, pág. 35.

y oportuna. De esta manera, la información debe ser clara, con calidad, ordenada, dirigida al público en general, en un lenguaje simple y directo.

La transparencia no implica únicamente publicar muchos contenidos de la entidad, sino que éstos deben estar disponibles y fáciles de encontrar por los usuarios de la web. Cuando se elaboran los portales web, debe ser tomada en cuenta la presentación de la información de forma que sea sencilla la búsqueda para el usuario.

3. ANÁLISIS DE DERECHO COMPARADO

La totalidad de las leyes en América Latina obligan a publicar cierta información de forma rutinaria y actualizada, aún ante la inexistencia de una solicitud.

La mayoría de las leyes otorgan un listado de categorías, que varía de país a país, de documentos que deben publicarse, así como información sobre las operaciones generales de la entidad, los servicios que brindan y el procedimiento para solicitar información.

3.1 Colombia

Los entes públicos tienen el deber de publicar toda la información requerida para garantizar que las personas puedan ejercer control sobre ellas.

Las normas sobre publicación proactiva están relativamente bien desarrolladas, en los primeros 11 artículos, de la Ley 57 de 12 de julio de 1985.

La forma general de diseminar la información prevista por la mencionada Ley es mediante boletines oficiales o gacetas oficiales. El artículo 1° indica que, en general, la nación, los departamentos y los municipios deben incluir, en sus diarios oficiales respectivos, cualquier información que el público deba conocer sobre el manejo de asuntos públicos o para mantener control efectivo sobre las actividades de los funcionarios, y cualquier otro asunto que se requiera publicar por ley para tener efectos legales. El artículo 2° detalla una lista de categorías de información que debe publicarse, además en el Diario Oficial, incluyendo las leyes adoptadas por el Congreso Nacional, los decretos gubernamentales, las resoluciones ejecutivas, los contratos que la ley requiere que se publiquen, y los actos de otras entidades públicas o entidades delegadas que crean situaciones objetivas de interés general.

De acuerdo al artículo 5°, cada departamento debe emitir un boletín o gaceta que contenga, entre otras cosas, las ordenanzas de la Asamblea Departamental, los actos de la asamblea y el Consejo Directivo relacionados con la ejecución de su presupuesto y el manejo del personal a su servicio, los decretos y resoluciones del gobernador, los contratos, cuando lo requieran las normas fiscales, y los actos de varias entidades que crean situaciones legales objetivas de interés general. El artículo 4°, por su parte, requiere que estos boletines se publiquen al menos una vez al mes. La entidad responsable de estas publicaciones decidirá la cantidad de copias papel que se necesitan de acuerdo al artículo 11.

3.2 Chile

Adoptó la Ley N° 20.285 sobre el Acceso a la Información Pública, publicada el 20 de Agosto de 2008.

En el artículo 7°, se exponen las obligaciones generales de publicación proactiva para la mayoría de los órganos públicos. El listado incluye información acerca de: su estructura orgánica; las facultades, las funciones y atribuciones de cada una de sus unidades u órganos internos; el marco normativo aplicable; la planta del personal y el personal a contratar y por honorarios, con las correspondientes remuneraciones; las contrataciones para el suministro de bienes muebles, para la prestación de servicios, para la ejecución de acciones de apoyo y para la ejecución de obras, y las contrataciones de estudios, asesorías y consultorías relacionadas con proyectos de inversión; las transferencias de fondos públicos que efectúen, incluyendo todo aporte económico entregado a personas jurídicas o naturales, directamente o mediante procedimientos concursales; los actos y resoluciones que tengan efectos sobre terceros; los trámites y requisitos que debe cumplir el interesado para tener acceso a los servicios que preste al respectivo órgano; el diseño, montos asignados y criterio de acceso a los programas de subsidios y otros beneficios que entregue el respectivo órgano, además de las nóminas de los beneficiarios de los programas sociales en ejecución, sin incluir datos personales; los mecanismos de participación ciudadana, en su caso; la información sobre el presupuesto asignado, así como los informes sobre su ejecución, en los términos previstos en la respectiva Ley de Presupuesto de cada año; los resultados de las auditorías al ejercicio presupuestario del respectivo órgano y, en su caso, las aclaraciones que proceda; todas las entidades en que tengan participación, representación e intervención, cualquiera sea su naturaleza y el fundamento normativo que la justifica.

Esta información debe proporcionarse de forma completa y actualizada en los sitios web de los órganos públicos, y de una manera que resulte de fácil acceso. Aquellas entidades públicas que no cuenten con un sitio web propio deberán proporcionar la información mediante los sitios de las entidades de las que dependen o están relacionados.

Las disposiciones son de naturaleza general y va a depender en gran medida de qué tan amplia o estrechamente se interpreten. Así por ejemplo, la referencia a la información presupuestaria puede entenderse de muchas maneras. Varias normas de derecho a la información prevén más detalle en relación con la información presupuestaria y financiera.

Finalmente, la Ley hace hincapié en los sitios web como vehículos para la extensión proactiva de la información.

3.3 México

Fue uno de los primeros países de América Latina en aprobar una ley sobre el derecho a la información, con la aprobación bajo la rúbrica del Presidente Fox

de la Ley Federal de Transparencia y Acceso a la información Pública del Gobierno en junio de 2002, con una posterior modificación en el 2006. La ley se encuentra entre las más progresistas sobre el derecho a la información en todo el mundo. Incluye fuertes garantías de procedimientos conjuntamente con un enfoque innovador para asegurar su aplicación a todas las entidades públicas, independientemente de su situación constitucional. Asimismo, establece un mecanismo muy intenso e independiente de vigilancia en forma del Instituto Federal de Acceso a la Información Pública (IFAI).

"Un gobierno abierto es condición necesaria más no suficiente para lograr una plena rendición de cuentas. No basta con que los servidores públicos no oculten la información que manejan. La rendición de cuentas implica una actitud proactiva hacia la información pública y exige que los servidores públicos periódicamente informen, expliquen y presenten en un lenguaje accesible al público lo que están haciendo".[234]
Por ejemplo, el artículo 7° de la Ley Mexicana, establece una obligación amplia de publicar sujeto al régimen de excepciones. Dispone que las entidades públicas deberán, de conformidad con las regulaciones promulgadas por IFAI, publicar 17 categorías de información de una manera accesible y comprensible.

Dichas categorías incluyen información sobre las operaciones generales de la entidad, los procedimientos y formularios, los servicios que ofrecen, informes emitidos, oportunidades para participación y contratos celebrados.

"Un gobierno abierto es condición necesaria más no suficiente para lograr una plena rendición de cuentas. No basta con que los servidores públicos no oculten la información que manejan. La rendición de cuentas implica una actitud proactiva hacia la información pública y exige que los servidores públicos periódicamente informen, expliquen y presenten en un lenguaje accesible al público lo que están haciendo".[235]

Por otra parte, el artículo 12 estipula que las entidades públicas deben publicar toda aquella información relativa a los montos y las personas a quienes entreguen, de todos aquellos recursos públicos que estén bajo su responsabilidad.

La Ley estipula la forma de hacer disponible esta información. El artículo 9 dispone que: "La información a que se refiere el Artículo 7 deberá estar a disposición del público, a través de medios remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas equipo de cómputo, a fin de que éstas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, éstos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

La Ley también incluye indicaciones específicas sobre la publicación proactiva de la información.

---

[234] ACKERMAN, John M. y otra. Ob. Cit., pág. 32.
[235] ACKERMAN, John M. y otra. Ob Cit., pág. 32.

De acuerdo con el artículo 8°, el Poder Judicial deberá publicar todas las sentencias que hayan causado estado o ejecutoria, sin perjuicio de la posibilidad de las partes de oponerse a la publicación de sus datos personales. Las entidades deben publicar todas las reglas y detalles administrativos formales 20 días antes de adoptarlas, a menos que esto pueda frustrar su éxito.

Los informes que presenten los partidos políticos y las agrupaciones políticas nacionales al Instituto Federal Electoral, así como las auditorías y verificaciones que ordene la Comisión de Fiscalización de los Recursos Públicos de los Partidos y Agrupaciones Políticas, deberán hacerse públicos al concluir el procedimiento de fiscalización respectivo.
También se requiere que las dependencias produzcan de forma semestral y por rubros temáticos, un índice de los archivos que tengan clasificados como reservados, indicando la unidad que produjo el documento, la fecha y plazo de clasificación. Este índice no podrá considerarse en sí mismo, en ningún caso, como información reservada.

3.4 Perú

La Ley Peruana N° 27.806 de 2 de Agosto de 2002, establece la obligatoriedad de todos los sectores del Estado a someterse al principio de publicidad, lo que implica poner a disposición de los ciudadanos la información sobre su gestión.

El propósito de la ley se encuentra establecido en el artículo 1° que reza: "promover la transparencia de los actos del Estado" y regular el derecho a la información previsto en la Constitución. El artículo 7° por su parte, dispone que toda persona tiene derecho a solicitar y recibir información de cualquier entidad de la Administración Pública. El artículo 3° apoya esto disponiendo que toda la información que se encuentra en manos del Estado, aparte de la que está cubierta por las excepciones, se presume pública y el Estado tiene la obligación de proporcionar información ante la respectiva solicitud, de conformidad con el principio de publicidad.

El artículo 10 establece el alcance de la información cubierta por la Ley. Indica que: "Las entidades de la Administración Pública tienen la obligación de proveer la información requerida si se refiere a la contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato, siempre que haya sido creada u obtenida por ella o que se encuentre en su posesión o bajo su control". Además, cualquier documentación financiada por el presupuesto público, en base a las decisiones de naturaleza administrativa, es información pública, incluyendo los registros de las reuniones oficiales. El artículo 3° amplía más aun, disponiendo que todas las actividades y regulaciones de entidades públicas están sujetas al principio de publicidad.

La Ley peruana se considera una muy buena norma por sus disposiciones extremadamente extensas respecto a la publicación proactiva. La Ley dedica un total de 14 artículos sobre este tema.

El Título IV contiene obligaciones detalladas y extensas sobre la publicación proactiva. Incluye su propia sección sobre el propósito y definiciones (Artículo 23), así como una disposición sobre los mecanismos para publicar información (Artículo 24). La publicación puede ser en páginas Web o en periódicos de importancia, dependiendo de los recursos disponibles, así como las regulaciones sobre la publicación donde el número de habitantes es bajo. Se debe establecer la metodología utilizada a recopilar la información y se elaboren los términos utilizados en los documentos, para permitir un análisis apropiado de la información. Requiere también que la información publicada en forma trimestral salga dentro de los 30 días después del final de cada trimestre, conjuntamente con la información de los dos trimestres anteriores, con fines comparativos.

El artículo 5° dispone la entrega por los departamentos del gobierno, dependiendo del presupuesto, de varios tipos de información mediante internet, incluyendo información general sobre la dependencia, su presupuesto, incluyendo los sueldos de todo el personal, información detallada de bienes y servicios, e información sobre las actividades oficiales con sus altos funcionarios. Las entidades públicas deberán identificar públicamente al funcionario responsable de desarrollar su página web.

3.5 Uruguay

La Ley N° 18.381 sobre el Derecho de Acceso a la Información Pública se adoptó el 17 de octubre de 2008 para dar vigor al derecho a la información.

El artículo 5° impone las categorías de información que todas las entidades públicas deben divulgar de manera proactiva, mediante sitios web u otros medios de su elección. La lista incluye información sobre: su estructura orgánica; facultades de cada unidad administrativa; estructura de remuneraciones por escalafón, funciones y sistema de compensaciones; información sobre presupuesto asignado, su ejecución y auditorías en caso de corresponder; concesiones, licitaciones, permisos o autorizaciones otorgadas, con especificación de titulares y beneficiarios; información estadística de interés general, en función de los fines de cada organismo; mecanismos de participación ciudadana con especificación del domicilio y la unidad a la que deben dirigirse las solicitudes para la obtención de la información.

De acuerdo con lo establecido en el artículo 5 de la Ley Nº 18.381, la forma de divulgación de la información que en él se establece es a través de los respectivos sitios web u otros medios que el órgano de Control determine. Esto debe ser efectuado de manera tal que resulte fácil el acceso a los interesados, con documentación organizada y sistematizada. Los organismos deberán difundir cierta información mínima, - que se encuentra detallada en el artículo - en forma permanente. Asimismo por el artículo 32, se ha establecido un plazo perentorio de un año a partir de la fecha de la publicación de la Ley Nº 18.381, para proceder a tal implementación; en la medida que esta ley fue publicada con fecha 7 de noviembre de 2008, el plazo para concretar esta previsión venció el 7 de noviembre de 2009.

Finalmente vemos como la tendencia en los países latinoamericanos es que cada vez más se ponga a disposición información de forma proactiva, buscando promover mayor eficiencia para el sector público y un mejor servicio. La mayoría de las leyes proporcionan una lista de las categorías de documentos que se deben publicar, así como información sobre las operaciones generales de la entidad, los servicios que proporciona y cómo solicitar información, aunque las listas varían de país a país.

4. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la ley es un aspecto importante a considerar dado que varía de acuerdo a las diferentes legislaciones y se presentan problemas de orden terminológico.

Es importante su estudio para analizar el alcance de las obligaciones y es necesario tener claro quiénes son los sujetos obligados a los cuales se les puede exigir el cumplimiento de las obligaciones de transparencia activa.

La Dra. Laura Nahabetián Brunet por su parte, indica que: "se debe aclarar que, además de las autoridades públicas nacionales, estatales, municipales o locales, que son los entes obligados a suministar la información pública, también se deben incluir personas naturales y jurídicas en cuya gestión y administración reciban aportes del Estado. De esta forma, se encuentran incluidas las concesionarias de obras públicas financiadas por el Estado en tanto entidades que en su caso podrán encontrarse obligados a entregar información a las personas sobre todos aquellos aspectos de la concesión que sean de interés para la colectividad.

Para determinar la procedencia de la obligación de presentación de información pública, deberán configurarse los siguientes requisitos:

- Debe tratarse de asuntos públicos del Estado.
- Éstos deberán tener relación directa con el patrimonio público del Estado y/o con los derechos humanos.
- No tratarse de las excepciones previstas en la ley"[236].

A continuación, se examinaran las distintas previsiones legislativas en Chile, Ecuador, México, Panamá y Uruguay.

4.1 Chile

La Ley N° 20.285 de la República de Chile dispone lo siguiente en cuanto al ámbito de aplicación: "Las disposiciones de esta ley serán aplicables a los ministerios, las intendencias, las gobernaciones, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa.

[236] Material preparado para el Taller de la Fundación Ciencias de la Documentación: "Legislación en materia de acceso a la información pública" por la Dra. Laura Nahabetián Brunet. Madrid, 2010.

La Controlaría General de la República y el Banco Central se ajustarán a las disposiciones de esta ley que expresamente ésta señale, y a las de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el artículo 1°.

También se aplicarán las disposiciones que esta ley expresamente señale a las empresas públicas creadas por ley y a las empresas del Estado y sociedades en que ésta tenga participación accionaria superior al 50% o mayoría en el directorio.
Los demás órganos del Estado se ajustarán a las disposiciones de sus respectivas leyes orgánicas que versen sobre los asuntos a que se refiere el artículo 1° precedente".

4.2 Ecuador

La Ley N° 2004-34 de 2004, de la República del Ecuador determina: "Esta Ley es aplicable a:
a) Los organismos y entidades que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República;
b) Los entes señalados en el artículo 1 de la presente Ley[237];
c) Las personas jurídicas cuyas acciones o participaciones pertenezcan en todo o en parte al Estado, exclusivamente sobre el destino y manejo de los recursos del Estado:
d) El derecho de acceso a la información de los diputados de la República, en la Ley Orgánica de la Función Legislativa y su Reglamento Interno;
e) Las corporaciones, fundaciones y organismos no gubernamentales (ONG´s) aunque tengan carácter de privadas y sean encargadas de la provisión o administración de bienes o servicios públicos, que mantengan convenios, contratos o cualquier forma contractual con instituciones públicas y/u organismos internacionales, siempre y cuando la finalidad de su función sea pública;
f) Las personas jurídicas de derecho privado, que sean delegatorias o concesionarias o cualquier otra forma contractual de servicios públicos del Estado, en los términos del respectivo contrato;
g) Las personas jurídicas de derecho privado, que realicen gestiones públicas o se financien parcial o totalmente con recursos públicos y únicamente en lo relacionado con dichas gestiones o con las acciones o actividades a las que se destinen tales recursos; y,
h) las personas jurídicas de derecho privado que posean información pública en los términos de esta Ley".

4.3 México

[237] Ley N° 2004-34 de 2004, de la República del Ecuador. Artículo 1°: "Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado; instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG´s), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley".

La Ley Federal de Transparencia y Acceso a la información Pública de México determina en su artículo 3° los sujetos obligados, y éstos son:
"a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal; d) Los órganos constitucionales autónomos; e) los tribunales administrativos federales, y f) Cualquier otro órgano federal."[238]

4.4 Panamá

La Ley N° 6 de 2002, de la República de Panamá determina en su artículo 1° que las instituciones obligadas a entregar la información pública son: "toda agencia o dependencia del Estado, incluyendo las pertenecientes a los órganos Ejecutivo, Legislativo y Judicial, el Ministerio Público, las entidades descentralizadas, autónomas y semiautónomas, la Autoridad del Canal de Panamá, los municipios, los gobiernos locales, las juntas comunales, las empresas de capital mixto, las cooperativas, las fundaciones, los patronatos y los organismos no gubernamentales que hayan recibido o reciban, capital o bienes del Estado".

4.5 Uruguay

La normativa nos obliga a interpretar quiénes son los sujetos obligados, ya que al hacer referencia a "organismos públicos sean o no estatales", se generan muchos problemas.

El artículo 2° Ley N° 18.381 establece que: "Se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública".

El Decreto Reglamentario N° 232/010, de 2 de agosto de 2010, en su artículo 2°, dispone que: "El presente Decreto será de aplicación a todos los organismos públicos, sean o no estatales".

"En el caso de Uruguay, por ejemplo, la pretensión de la norma es la transparencia de la actividad gubernamental, en mérito a la cual la interpretación debería ser contextual y todas las entidades que manejen dineros públicos, deberían constituirse en sujetos obligados.

En tal sentido se coincide con el Dr. Carlos Delpiazzo, quien expresa: "la estatalidad de las empresas reguladas por el Derecho privado pero en las que participa alguna entidad estatal, está dada precisamente por esa pertenencia -total o parcial, cualquiera sea su proporción- a la colectividad organizada. Por lo tanto, si bien se coincide en que el carácter estatal o no estatal viene dado

[238] Ley de Transparencia y Acceso a la Información Pública de los Estados Unidos Mexicanos.

por el capital o patrimonio, no se comparte la apreciación de que la persona jurídica privada será estatal sólo cuando su patrimonio pertenezca mayoritariamente o íntegramente a una entidad estatal, en tanto que no lo será cuando esa participación sea minoritaria. A nuestro criterio, la sola presencia del Estado (en sentido amplio) califica en todos los casos a la institución de que se trate, cualquiera sea el quantum de su aporte."[239]

Richard Calland, determinó una serie de argumentos que estarían justificando la necesidad de inclusión en las leyes de transparencia de las entidades del sector privado. En este sentido indica que: "En el mundo entero, las privatizaciones y otras políticas similares como la subcontratación de terceros para la provisión de servicios públicos y las asociaciones entre el sector público y el sector privado, han alterado visiblemente el panorama respecto al poder público. Los servicios públicos municipales, como la recolección de residuos, se encuentran ahora en manos privadas. El sistema de transporte público es provisto por una compleja coalición entre el gobierno y algunas grandes empresas. En algunos lugares, aún incluso las prisiones han sido puestas en manos privadas.

Aún más importante para la vida cotidiana de las personas, los servicios de provisión de agua han sido también privatizados. La provisión de agua es hoy en día una industria multimillonaria en el mundo entero. Desde las sierras de Cochabamba en Bolivia a los poblados empobrecidos de Sudáfrica, los ciudadanos continúan resistiendo los aumentos en los costos del agua que siguieron a las privatizaciones...El argumento en favor de la transparencia del sector estatal y de la consecuente rendición de cuentas que debiera acarrear, pierde todo sentido si grandes espacios del poder estatal privatizados están exceptuados de la obligación de transparencia y de permitir el acceso a la información en su poder."[240]

Sin embargo, ésta no es una concepción unánime. El Prof. Sayagués por otra parte, entiende que: "los conceptos tradicionales han sido superados por las nuevas tendencias del derecho. ...la distinción entre las personas públicas y privadas no puede hacerse sobre la base de su calidad de estatal o no, sino en razón del régimen jurídico en que se mueven: si se regulan por el derecho público, en todo o en parte, serán personas públicas; si exclusivamente por el derecho privado, serán personas privadas."[241]. Se tratará de personas públicas cuando se encuentren reguladas primordialmente por el Derecho Público y de personas privadas cuando primordialmente lo estén por el Derecho Privado.

5. OBLIGACIONES DE TRANSPARENCIA ACTIVA

[239] Material preparado para el Taller de la Fundación Ciencias de la Documentación: "Legislación en materia de acceso a la información pública" por la Dra. Laura Nahabetián Brunet. Madrid, 2010.
[240] THE CARTER CENTER. Ob. Cit., pág. 44.
[241] SAYAGUÉS LASO, Enrique. Tratado de Derecho Administrativo. Tomo I. 8va. Montevideo, 2002.

Las obligaciones de transparencia activa instan a diferentes entidades a difundir regularmente determinada información actualizada sin que nadie lo solicite, como una manera de transparentar la gestión.
Todas las leyes de América Latina imponen a las entidades públicas el deber de publicar cierta información clave de manera proactiva. La ley peruana es una de las más completas en este punto, en comparación con cualquier otra ley en el mundo.

La mayoría de las leyes proveen una lista de categorías de documentos que se deben publicar, como información sobre las operaciones generales de la entidad, los servicios que proporciona y cómo solicitar información, aunque el listado varía de país a país.

Como se mencionara ut supra, en Uruguay las obligaciones de transparencia activa se encuentran establecidas en el artículo 5° de la Ley N° 18.381. En este sentido, las entidades públicas se encuentran obligados a publicar en sus sitios web información respecto a la estructura orgánica, las facultades de cada unidad administrativa, la estructura de remuneraciones por categoría escalafonaria, información respecto del presupuesto asignado, concesiones, licitaciones, permisos o autorizaciones otorgadas, información estadística de interés general y mecanismos de participación ciudadana.

El Decreto N° 484/009, de 19 de octubre de 2009, por su parte, concreta las obligaciones de transparencia con cumplimiento 7 de noviembre de 2009. Sin perjuicio de su cumplimiento en fecha, de todas formas, éstas se ven concretadas tanto en la ley cuanto en el decreto reglamentario N°232/010. A continuación analizaremos la información que deben difundir los sujetos obligados en sus sitios web, de acuerdo con el artículo 38 del decreto.
Dicho artículo exige difundir en sus sitios web la siguiente información que deberá ser actualizada mensualmente:
1. Creación, evolución histórica y sus cometidos.
2. Estructura orgánica. Colocar un organigrama es muy importante para que quienes visiten la página sepan cómo se encuentra estructurada la entidad.
3. Listado de los funcionarios a partir del jefe del departamento hasta el jerarca máximo. Se deben incluir los CV, según corresponda en cada caso.
4. Programas operativos de largo y corto plazo y mecanismos que permitan visualizar metas y su cumplimiento. Se trata de información relevante para que las personas conozcan el nivel de cumplimiento y efectividad en el manejo de los recursos que se destinan a cada actividad dentro de cada una de las entidades de que se trata.
5. Información referente a la utilización de los recursos públicos.
6. Presupuesto asignado, ejecución y auditorías. Se debe especificar la cantidad de ingresos recibidos por cualquier concepto, ingresos asignados por el presupuesto nacional y las donaciones.
7. En cuanto a las auditorías, se debe incluir información sobre los resultados, el número y el tipo de auditoría, las observaciones que se realizaren, sanciones y aclaraciones efectuadas por el sujeto obligado.
8. Salarios y compensaciones recibidas por los funcionarios. Debe figurar el salario nominal, sin ningún tipo de descuentos legales ni los que refieren a

préstamos, retenciones judiciales, afiliación sindical, pensiones alimenticias o cualquier otro descuento de la misma índole.
Con respecto a las compensaciones, deben publicarse todas las que sean accesorias al salario base y signifiquen un beneficio para el funcionario como: diferencia de tabla, uniformes, tickets de alimentación, entre otros).
9. Contratos de funcionarios que no perteneciendo al organismo cumplen funciones en el mismo.

Muchas leyes, como las de Ecuador y Perú, incluyen listas especiales de información que deben publicar de forma proactiva determinadas entidades públicas específicas. En Ecuador, todos los recursos invertidos por los partidos políticos se deben publicar de manera proactiva.

En Guatemala, las sentencias relacionadas con el erario público, sentencias sobre crímenes cometidos por funcionarios públicos y las pronunciadas por órganos judiciales en relación con crímenes de derechos humanos y crímenes contra la humanidad, también deben ser publicadas de forma proactiva.

Varias leyes en América Latina destacan la información de naturaleza comercial o financiera. La ley Peruana, incluye un capítulo exclusivo sobre la información financiera pública, que requiere además de publicar la información de forma proactiva, hacerlo propio con la metodología utilizada para reunir la información.

Las leyes de Chile, Panamá y Perú, solicitan que la información publicada se actualice con regularidad, generalmente de forma anual. En Colombia, las entidades públicas deben publicar diarios con ciertas categorías de información cada mes, y éstas deben enviarse de forma gratuita a las oficinas públicas, medios de comunicación, universidades, entidades públicas y asociaciones. En Perú, cierta información financiera debe publicarse trimestralmente.

En Uruguay, Ecuador y Perú, todas las entidades públicas estaban obligadas a publicar en sitios web un año después de la entrada en vigencia de la ley. La ley mexicana requiere que las entidades públicas pongan una computadora a disposición del público con la finalidad de brindar acceso a la información, junto con una impresora, y soporte técnico de ser necesario.

En Reino Unido, la ley requiere que las entidades públicas diseñen esquemas de publicación, que deberán ser aprobados por el Comisionado de Información independiente, o bien pueden utilizar un esquema de publicación modelo proporcionado por el propio Comisionado.

La tendencia predominante en todos los países es que cada vez sea más la información que se pone a disposición de forma proactiva. Es un paso positivo ya que promueve la eficiencia del sector público enfocado hacia el beneficio al ciudadano, y el acercamiento hacia formas más representativas de gobierno.

6. CONCLUSIONES

No se puede negar la importancia de la transparencia activa en un gobierno democrático, pero el cuestionamiento es porqué ha crecido tanto la corriente de transparencia y acceso a la información en estos últimos tiempos.

Transparencia y acceso no derivan automáticamente de los regímenes democráticos sino que hay que realizar un arduo trabajo para construir, aplicar, concientizar, dado que la transparencia activa es importante para la democracia no sólo como sistema de gobierno sino como formulación de vida ciudadana.

Un enfoque interesante es el efectuado por The Carter Center, donde propone desafíos para mejorar la entrega de información de la gerencia pública. Estos son:

"**I. Establecer sistemas de información**
Para que la comunicación externa sea adecuada a los intereses de los ciudadanos es necesario que las entidades públicas desarrollen sistemas de información que muestren la identidad institucional, donde se reflejen sus objetivos, funciones, el proyecto organizativo, la cultura organizacional, los valores compartidos, es decir, todo aquello que puede ser observable y constatable. …Es fundamental que los gobiernos establezcan políticas claras y lineamientos precisos para el desarrollo de sistemas de información y comunicación adecuadamente concebidos, que permitan compatibilizar los datos que generan las distintas entidades y consolidar información sistematizada con contenidos útiles, coherentes, oportunos y veraces.

II. Fortalecer la relación con el público
Así como las empresas privadas están centrando su mayor atención en los clientes para enfrentar los desafíos del siglo XXI, del mismo modo, las administraciones públicas deberían estar fundamentalmente orientadas a los ciudadanos y proyectarse como entidades conscientes de que su misión principal es el servicio y la atención de las necesidades de la población y de sus demandas razonables. Entre las vertientes que alimentan esa conducta pública está el establecimiento de sistemas de comunicación recíproca entre los ciudadanos y la administración pública. Para comunicarse con los ciudadanos, las entidades públicas deben mejorar sus sistemas de información y de atención al público; al mismo tiempo, deben fortalecer la generación de información externa en un marco de transparencia. ¿Cómo definir políticas y objetivos institucionales si las entidades desconocen las demandas sociales? ¿Cómo la ciudadanía puede tomar conciencia de las posibilidades o dificultades de la administración estatal si no logra acceder a la información necesaria para ese propósito? Son tan solo algunas de las interrogantes que se pueden formular para motivar la búsqueda de soluciones a los problemas de transparencia que enfrentan tanto el gobierno central como los gobiernos locales del país. Se debe tener en cuenta que la comunicación Estado—Sociedad es bidireccional. Esa aseveración significa que para comunicarse con los ciudadanos la administración estatal debe mejorar sus sistemas de información y potenciar la emisión de información externa dirigida hacia los ciudadanos, creando asimismo sistemas de consulta que le provean de

información de las prioridades ciudadanas en diversos campos de los servicios públicos y de las preferencias y expectativas de la población.

III. No enfatizar demasiado en nuevas tecnologías

Si bien es creciente el número de entidades públicas que están utilizando nuevas tecnologías de información y comunicación, como apoyo a la gestión pública, esas novedosas formas de comunicación entre la administración y los ciudadanos, no podrán todavía tener un alcance generalizado debido a los fuertes desequilibrios que se presentan en el desarrollo de estos medios entre las principales capitales de departamento y el resto del país. Pero los desequilibrios también se presentan entre las entidades públicas ya que es perfectamente verificable que muchas de ellas no han logrado aún implantar la totalidad de los sistemas de administración y control que establece la ley SAFCO, por lo tanto, las bases mismas de la gestión pública y de la generación de información están en construcción o simplemente están detenidas.

IV. Facilitar la capacitación de funcionarios públicos

Basta recorrer las entidades públicas para tomar conciencia que innumerables puestos de trabajo están plenamente ocupados generando datos, listados, cuadros, reportes, informes y en fin, una interminable y ferviente actividad de generación de información. A ciencia cierta ni los propios empleados que la producen saben si será utilizada efectivamente o si simplemente formará parte de las toneladas de papel que contienen información para responder a formalidades administrativas o para cumplir con instrucciones dadas en algún momento por un funcionario jerárquico del que ya no se tiene memoria, con un propósito también olvidado o porque también se supone que son documentos de “descargo” para posibles, aunque inciertas operaciones de control posterior. Lo cierto es que en las entidades públicas se generan y acumulan volúmenes incalculables de información que en su mayor parte no tiene utilidad desde la perspectiva de la eficacia, eficiencia y economía de las operaciones. Es una acumulación desordenada, caótica y asistémica, que incluso da lugar a fenómenos de fuga de documentos que han costado esfuerzos y recursos al Estado. En sociedades pobres como la boliviana, la paradoja de este tipo de despilfarro es una realidad que contrasta con la falta de transparencia.

V. Enfocarse en la implementación

Es indudable que el proceso de implantación de los sistemas de administración y control establecidos en la Ley SAFCO ha tropezado con varias dificultades que han repercutido en el procesamiento y generación de información. Empero, se debe reconocer que en los últimos años el Sistema Integrado de Gestión y Modernización Administrativa (SIGMA) está permitiendo un proceso gradual de centralización de la información referida a presupuestos, contabilidad, tesorería, crédito público, compras y contrataciones, manejo y disposición de bienes y administración de personal. Sin embargo, los distintos módulos del SIGMA no tienen todavía desarrollados los componentes para generar reportes sistematizados que permitan su difusión a los ciudadanos. Se debe también señalar que en el campo de la información centralizada están en ejecución los procesos de implantación de otros sistemas como el Sistema de Información de Contrataciones Estatales (SICOES) que centralizará la información de todo el sector público referida al Sistema de Administración de Bienes y Servicios y el

Sistema de Inversión Pública (SIP) que estará encargado de difundir información relacionada con la inversión pública, las líneas de financiamiento para formular, evaluar y ejecutar proyectos de inversión pública."[242]

La Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) dio un paso positivo para capacitar y concientizar a los sujetos obligados al crear una "Guía para Diseño e implementación de Portales estatales".[243] Su principal objetivo es mejorar el acceso al Estado a través del desarrollo de la Web. Esta guía fue pensada como material de apoyo para los equipos que tienen la responsabilidad de diseñar e implementar portales estatales. La misma reúne un conjunto de buenas prácticas y recomendaciones donde se incluyen conceptos de planificación, diseño, implementación, usabilidad, accesibilidad, normativa y seguridad.

Este trabajo vaya si vale la pena, ya que el derecho a la información en su vertiente activa de acceso a la información pública es un derecho humano irrenunciable y vuelve más eficaz a las instituciones porque "ayudan a que las dependencias del gobierno no sean desviadas de sus objetivos públicos para servir a intereses privados, por ejemplo, los intereses de los funcionarios que las controlan"[244].

"La acción más positiva en un Estado que se precie de ser democrático: es la transparencia, la rendición de cuentas, la apertura hacia quien se sirve: el ciudadano.

El valor más grande que puede tener cualquier gobierno, de cualquier filiación política, es la honorabilidad en el servicio público.

Poner al honor como valor fundamental de la acción del gobernante es una virtud poco destacada, pero indispensable en nuestros tiempos. Y hacer de la tarea de gobierno una *casa de cristal*, en la que el ciudadano observe a sus elegidos, a sus representantes, a sus gobernantes, es el medio para rescatar este valor del que hablo. El honor es una de las virtudes que nuestra sociedad ha ido dejando en el olvido y, por ello, la indignidad, la vileza, la bajeza, la indecencia, la corrupción, van ganando la batalla."[245]

---

[242] THE CARTER CENTER. Ob. Cit., pág. 23.

[243] http://www.agesic.gub.uy/innovaportal/v/548/1/agesic/guia_para_diseno_e_implementacion_de_portales_estatales.html

[244] VERGARA, Rodolfo. "La Transparencia como problema" en Cuadernos de Transparencia Nº5. IFAI, pág. 23.

[245] SANCHEZ CORDERO DE GARCÍA VILLEGAS, Olga. "Derecho, ciudadanía y transparencia. Trilogía estructural de lo social", Participación en la 2ª Reunión Nacional de abogados de la Secretaría de Desarrollo Social, organizada por la misma Secretaría, el 25 de Agosto de 2005, en el auditorio "Alfonso García Robles", de la Secretaría de Relaciones Exteriores, en Tlaltelolco, Ciudad de México.
http://www.scjn.gob.mx/conocelacorte/ministra/derecho-ciudadania-y-transparencia.pdf

CAPITULO XV – EQUILIBRIO ENTRE DOS DERECHOS: ACCESO Y PRIVACIDAD

Prof. Dra. Esc. María José Viega

1. INTRODUCCION

AGESIC impulsó la Ley de Protección de Datos Personales y Acción de Habeas Data Nº 18.331. 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[246].

La Ley 18.331 se aprobó el 11 de agosto de 2008 y el 17 de octubre del mismo año se aprueba la Ley Nº 18.381 de Acceso a la Información Pública, estableciéndose en el artículo 10 la información confidencial, los datos personales que requieren previo consentimiento informado.

Se consagraron 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 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.

La más amplia accesibilidad y visibilidad, lejos de comprometer el correcto funcionamiento del aparato administrativo, refuerza su legitimidad democrática y la configuración esencialmente servicial[247]. Para Antonio Troncoso 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 constitucionales[248].

---

[246] VIEGA, María José. "La armonización entre las leyes de transparencia y los estándares internacionales de protección de datos". Ponencia presentada en el Seminario Regional de la Red Iberoamericana de Protección de Datos realizado en Montevideo entre el 1 y 4 de junio del 2010.

[247] 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.

[248] 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.

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"[249].

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.

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

2. ANALISIS DE RESOLUCIONES ADMINISTRATIVAS DEL LA UAIP Y LA URCDP

Se ha realizado un análisis teórico del equilibrio entre los derechos, pero nos parece pertinente comentar algunos casos prácticos.

2.1 Acceso a correos electrónicos por un Consejero de la Facultad de Ciencias Económicas

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 Nº 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 Nº 18.381. Por otra parte,

[249] 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.

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 Nº 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 Nº 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 Nº 16/2009 de 22 de octubre de 2009 resuelve confirmar la Resolución Nº 2/2009.

2.2 Acceso información de los concursos de oposición y mérito en la Administración Pública

La Resolución Nº 4/2009 de 14 de julio de 2009[250] responde a una consulta sobre la armonización de la Ley Nº 18.331 y la Ley Nº 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 UAIP 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 sicológicas".

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 Nº 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

[250] http://www.informacionpublica.gub.uy/sitio/consejo-resoluciones.html página visitada el 21 de mayo de 2010.

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.

2.3 Transparencia activa y datos personales

La URCDP, por el Dictamen Nº 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.

También la URCDP Dictamen N° 7 del 7 de agosto de 2009 resuelve sobre la consulta realizada por la Junta Departamental de Maldonado, quien consulta

acerca de las solicitudes de residentes del Departamento que consideran que la publicación en la página web de expedientes que contienen datos personales podría violar su intimidad o ser utilizados con fines delictivos y se solicita que se eliminen los datos personales consignados en los expedientes.

El Consejo consideró que los expedientes de la Junta Departamental de Maldonado contienen datos personales, que respecto al tratamiento de datos personales se debe considerar el principio de finalidad contenido en el art. 8° de la LPDP, por el cual no se deben utilizar datos personales para una finalidad distinta para la que fueron recabados. No constando en dichos expedientes ninguna referencia a la publicación en la web de éstos. Por otra parte, que de acuerdo al principio de proporcionalidad se considera desproporcionado publicar *in totum* los expedientes llevados por la Junta. Además, en el considera una buena práctica la publicidad de la actuación administrativa del Estado como elemento coadyuvante a la democracia y a la transparencia y la LPDP recoge en el art. 4 literal g) el procedimiento de disociación de los datos que se podría utilizar para no identificar a los titulares.

Finalmente aconsejar la realización de versiones públicas de los expedientes que se publiquen en su sitio web sin revelar datos personales utilizando la técnica de la disociación y aplicando el principio de divisibilidad.

2.4 Obtención del padrón de egresados de la Facultad de Ciencias Económicas

La URCDP resuelve por Dictamen N° 14 del 25 de setiembre del 2009. Una consulta relativa a las posibilidades de obtener de parte de la Facultad de Ciencias Económicas el padrón de egresados con sus correspondientes direcciones electrónicas o incluso éstas disociadas, al amparo de la Ley Nº 18.381.

El Consejo considera que ante todo debe apreciarse que el integrante de un órgano colegiado regido por el Derecho Público, como es el caso, carece de legitimación para pretender este tipo de informaciones a título individual, ya que todos sus actos deben revestir un carácter oficial para considerarlos legítimos, que permita identificarlos clara e inequívocamente como actividades preparatorias enderezadas a formar la voluntad del órgano al que pertenece el miembro en cuestión.

Que de acuerdo con los arts. 2, 8 y 10 numeral II de la Ley N° 18.331 se entiende que los datos personales cuyo registro y tratamiento por organismos públicos (estatales y no estatales) requiere consentimiento de sus titulares, son información confidencial y, como tal, están excluidos del derecho de acceso a la información pública.

Declara que la solicitud de correos electrónicos de estudiantes o egresados de las Facultades pertenecientes a la Universidad de la República, por parte de un Consejero de la misma, no es conforme a derecho.

2.5 Solicitud de datos de automotores y sus propietarios a la Intendencia Municipal de Montevideo

Por Dictamen N° 12 de 7 de junio de 2012, la Unidad de Protección de Datos se expidió sobre la consulta fue formulada por la Unidad de Acceso a la Información Pública. El Consejo considera que la solicitud de información pública presentada ante la Intendencia Municipal de Montevideo (IMM), contiene datos personales como: N° padrón, propietarios, domicilios y datos () de vehículos, como la marca y el modelo de matrículas especificadas.

El Consejo de la URCDP entiende que las intendencias son sujetos obligados en el marco de lo previsto por la Ley N° 18.381, que si bien establece la obligación de brindar acceso a la información que les es solicitada dentro del plazo estipulado, también obliga a analizar y clasificar la información que se encuentra amparada por alguna de las excepciones. Por otra parte, en la petición analizada, hay datos que deben ser considerados información confidencial, pues se trata de datos personales que requieren previo consentimiento informado según se establece en el art. 10 Num. II de la Ley N° 18.381. Por ende, la IMM no puede solicitar a los particulares sus datos personales para entregarlos posteriormente en desmedro de la privacidad de los administrados, pues ello no se ajusta a los principios contenidos en la Ley N° 18.331, sobre todo al de Proporcionalidad y de Finalidad (arts. 7° y 8°).

Se podría brindar a los interesados toda información estadística relativa a la cantidad, tipo y marcas de vehículos que tributan en el departamento, sin incluir detalles que permitan identificar a los titulares, pues efectivamente en ese caso, se estaría vulnerando el art. 10 Num.II de la Ley 18.381 así como las disposiciones de la Ley N° 18.331 (art. 1°, 5°, 7°, 8°, 9°, 11, 13 y 17).

2.6 Carácter que poseen determinados datos personales incluidos en una solicitud de acceso a la información pública

La Unidad de Acceso a la Información Pública consulta a la URCDP respecto al carácter que poseen determinados datos personales que se incluyen en una solicitud de acceso a la información pública presentada ante el Ministerio de Relaciones Exteriores (MRREE).

El Consejo se expide mediante Dictamen N° 24 de 4 de octubre de 2012. En el cual se hace referencia a que lo que se solicita refiere a: tipo de función (ejemplo auxiliar administrativo), representación donde desempeña funciones (ejemplo Consulado General de Barcelona), nacionalidades (ejemplo uruguayo y español), fecha de nacimiento, fecha de inicio de funciones en la representación, número de años completos en funciones, partida de contratación asignada (total en moneda local y conceptos incluidos: (sueldo neto, aportes empleador/empleado, impuesto a la renta), fecha de última modificación -ajustes por inflación, aumentos de sueldo.

El Dictamen diferencia tipos de datos, refiriendo a los siguientes casos:

a. Los datos referidos al tipo de función, representación, fecha de inicio de funciones y número de años completos en funciones, -datos que en definitiva hacen al rol que cada funcionario cumple para y en la actividad pública-, deben ser considerados públicos sin más análisis, aunque es cometido atribuido legalmente a la UAIP determinar en última instancia tal carácter, en base a los establecido en la Ley N° 18.381 y su Decreto Reglamentario.

b. Los datos relativos a la nacionalidad y fecha de nacimiento de estos funcionarios, deben ser incluidos dentro de lo previsto en el art. 9 C) de la Ley N° 18.331, por lo tanto para su tratamiento no se requiere el previo consentimiento informado.

c. Los datos que refieren a los ingresos de estos funcionarios o sea la partida de contratación asignada (total en moneda local y conceptos incluidos: sueldo neto, aportes empleador/empleado, impuesto a la renta, fecha de última modificación -ajustes por inflación, aumentos de sueldo), corresponde realizar la prueba o test del interés público, lo que implica interpretar y en definitiva aplicar las disposiciones contenidas en la Ley N° 18.381 y su decreto Reglamentario N° 232/2010, actividad que se entiende inmanente al Órgano de Control designado a tales efectos, o sea a la Unidad de Acceso a la Información Pública.

3. REFLEXION FINAL

El objetivo del presente trabajo es mostrar los avances de Uruguay en la consagración de dos derechos fundamentales. Pero esto no ha sido solamente en el plano jurídico, sino que se ha proveído de dos órganos garantes, que como surge de las resoluciones administrativas referidas funcionan en armonía, respetando sus competencias y colaborando entre ellas.

El modelo institucional uruguayo es atípico, ni organismos con competencia conjunta, ni organismos totalmente separados. Las Unidades tienen un Consejero en común, garante de una buena gestión y custodio del equilibrio entre ambas. Pero también con consejeros que poseen independencia técnica y son especializados en cada una de sus materias, reza en cada una de las leyes.

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”[251].

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

Finalmente, debemos tener presente que, ambas leyes establecieron como garantía jurisdiccional la acción de habeas data, propia e impropia, previendo un mismo trámite para el ejercicio de ambos derechos, con las diferencias mínimas que caracterizan a cada uno de ellos. Por lo tanto, aquellas zonas grises que no puedan ser resueltas en vía administrativa, podrán ser llevadas ante el Poder Judicial, de forma tal que estos derechos ciudadanos estén plenamente protegidos.

CAPITULO I – DERECHOS CIUDADANOS
Prof. Dra. Esc. María José Viega

1. Gobierno electrónico y gobierno en red
2. El gobierno electrónico como derecho ciudadano
3. La protección de datos personales
    3.1 Orígenes
    3.2 Evolución histórica
    3.3 Fundamentos del derecho a la protección de datos personales
4. Acceso a la información pública
    4.1 Orígenes
    4.2 Evolución histórica
    4.3 Fundamentos del derecho de acceso a la información pública

CAPÍTULO II – PRINCIPIOS Y DERECHOS DE LA PROTECCIÓN DE DATOS PERSONALES
Dra. Esc. Beatriz Rodríguez

1. Principios en materia de protección de datos personales
    1.1 Introducción
    1.2 Principio de calidad de los datos
    1.3 Principio de veracidad
    1.4 Principio de finalidad
    1.5 Principio de previo consentimiento informado
    1.6 Principio de seguridad de los datos
    1.7 Principio de reserva
    1.8 Principio de responsabilidad
2. Derechos en materia de protección de datos personales
    2.1 Introducción
    2.2 Derecho de información
    2.3 Derecho de acceso
    2.4 Derecho de rectificación, actualización, inclusión, supresión, u oposición
    2.5 Derecho a la impugnación de valoraciones personales
    2.6 Otros derechos referentes a la comunicación de datos
3. Conclusiones

CAPÍTULO III – LA LEY Nº 18.331 DE PROTECCIÓN DE DATOS PERSONALES
Dra. María José Rodríguez Tadeo

1. Introducción
2. El derecho a la protección de los datos personales
    2.1 Ámbito subjetivo de aplicación de la Ley
    2.2 Ámbito objetivo de aplicación de la Ley
3. Definiciones contenidas en la Ley (artículo 4º)
    3.1 Dato personal
    3.2 Dato sensible

CAPÍTULO IV – DECRETOS Nº 664/008 Y Nº 414/009
Dra. Flavia Baladán

3.1 Ámbito de aplicación
3.2 Definiciones incluidas
3.3 Regulación del previo consentimiento del titular
3.4 Regulación de la seguridad de las Bases de Datos
3.5 Regulación de los derechos de los titulares
3.5.1 Requisitos para su ejercicio
3.5.2 Particularidades
3.5.3 Comunicación o cesión de datos
3.6 Inscripción de base de datos
3.6.1 Requisitos formales
3.6.2 Inscripción provisoria
3.6.3 Fecha de inscripción
3.6.4 Actualizaciones
3.7 Normas de actuación
3.7.1 Aspectos administrativos
3.7.2 Aspectos procedimentales
4. Conclusiones

CAPÍTULO V – AUTORIDADES DE CONTROL EN PROTECCIÓN DE DATOS
Esc. Sandra Mazzone

1. Introducción
2. Clases de órganos de control
3. Derecho Comparado
   3.1 Alemania
   3.2 Argentina
   3.3 España
   3.4 Francia
   3.5 Portugal
   3.6 Italia
   3.7 Unión Europea. Supervisor Europeo de Protección de Datos
4. Órgano de Control uruguayo. Unidad Reguladora y de Control de Datos Personales
   4.1 Creación
   4.2 Cometidos
   4.3 Actuación de la URCDP
   4.4 Consejo Consultivo
5. Conclusiones

CAPÍTULO VI – DATOS ESPECIALMENTE PROTEGIDOS
Dr. Marcelo Bauzá

1. Introducción
2. Datos sensibles
   2.1 Concepto y alcances
   2.2 Antecedentes nacionales y derecho comparado
   2.3 Análisis de la definición contenida en el art. 4º lit. E) de la Ley Nº 18.331
   2.4 Régimen legal aplicable a su recolección y tratamiento
3. Datos relativos a la salud

7. Principio de Existencia de Procesos de Facilitación del Acceso
8. Principio de Gratuidad
9. Principio de Reuniones Abiertas
10. Principio de Transparencia Precedente
11. Principio de Protección de Denunciantes
12. Conclusiones

CAPÍTULO IX – LA LEY Nº 18.381 DE ACCESO A LA INFORMACIÓN PÚBLICA
Dra. Graciela Romero

1. Introducción
2. Ámbito de aplicación
   2.1 Sujetos obligados
   2.2 Concepto de información pública
3. Derecho de acceso a la información pública
   3.1 Legitimación activa
   3.2 La solicitud y sus requisitos
4. Obligaciones atribuidas a los sujetos obligados
   4.1 Relacionadas con el derecho de acceso
   4.2 Relacionadas con los archivos
   4.3 Relacionadas con el Órgano de Control (UAIP)
5. Límites al Derecho de Acceso a la Información Pública
   5.1 Breve reseña de las excepciones
   5.2 Análisis del art. 14
6. Plazos para entregar la información solicitada
   6.1 Análisis del art. 15
   6.2 La hipótesis de “silencio positivo” del art. 18
7. La acción de acceso a la información pública
   7.1 Procedencia
   7.2 Competencia y legitimación
   7.3 Aspectos procesales
8. Responsabilidades y sanciones
9. Conclusiones

CAPÍTULO X – EL DECRETO Nº 232/010
Dra. Rosario Ierardo

1. Introducción
2. Ámbito de Aplicación
   2.1 Ámbito objetivo
   2.2 Ámbito subjetivo
3. Principios generales
   3.1 Principios referidos a la información
   3.2 Principios vinculados con los archivos
4. Definiciones incluidas en el Decreto Reglamentario
5. Tipos de información
6. Regulación de los archivos
7. Informes que deben presentar los sujetos obligados
   7.1 Informe anual

7.2 Informe semestral
8. Regulación de las obligaciones de los responsables
9. Órgano de control
10. Responsabilidad de los funcionarios
11. Conclusiones

CAPÍTULO XI – AUTORIDADES DE CONTROL EN ACCESO A LA INFORMACIÓN PÚBLICA
Dra. Jimena Hernández

1. Introducción
2. Derecho Comparado
   2.1 Leyes de acceso a la información en el mundo y modelos de control
   2.2 Unión Europea
   2.2.1 Suecia
   2.2.2 Francia
   2.2.3 Portugal
   2.2.4 Inglaterra
   2.3 América Latina
   2.3.1 México
   2.3.2 Honduras
   2.3.3 Chile
   2.4 Estados Unidos
3. Órgano de Control Uruguayo
   3.1 Creación de la Unidad de Acceso a la Información Pública
   3.2 Consejo Ejecutivo
   3.2.1 Integración
   3.2.2 Cometidos
   3.2.3 Normas introducidas por el Decreto Nº 232/010
   3.3 Consejo Consultivo
   3.3.1 Integración y funcionamiento
   3.3.2 Normas introducidas por el Decreto Nº 232/010
4. Conclusiones

CAPÍTULO XIII – CLASIFICACIÓN DE LA INFORMACIÓN
Dra. Bárbara Muracciole

1. Introducción
2. Información Pública
3. Excepciones
   3.1 Principio de Limitación de Excepciones
   3.2 Derecho Comparado
   3.2.1 Chile
   3.2.2 Colombia
   3.2.3 Ecuador
   3.2.4 Guatemala
   3.2.5 Honduras
   3.2.6 México
4. Clasificación de la Información
   4.1 Información secreta

4.1.1 Secretos comerciales-industriales
4.1.2 Secretos que deben guardar los funcionarios
4.1.3 Secreto de las comunicaciones
4.1.4 Secreto bancario – tributario
4.1.5 Secreto estadístico
4.1.6 Secreto profesional
4.1.7 Secreto político y militar
4.1.8 Otras disposiciones
4.2 Información reservada
4.3 Información confidencial
5. Conclusiones

CAPÍTULO XII – OBLIGACIÓN DE TRANSPARENCIA ACTIVA
Dra. Silvana Casciotti

1. Introducción
2. Concepto de transparencia activa
3. Análisis de Derecho Comparado
   3.1 Colombia
   3.2 Chile
   3.3 México
   3.4 Perú
   3.5 Uruguay
4. Ámbito de Aplicación
   4.1 Chile
   4.2 Ecuador
   4.3 México
   4.4 Panamá
   4.5 Uruguay
5. Obligaciones de Transparencia Activa
6. Conclusiones

CAPITULO XV – EQUILIBRIO ENTRE DOS DERECHOS: ACCESO Y PRIVACIDAD
Prof. Dra. Esc. María José Viega

1. INTRODUCCION
2. ANALISIS DE RESOLUCIONES ADMINISTRATIVAS DEL LA UAIP Y LA URCDP
   2.1 Acceso a correos electrónicos por un Consejero de la Facultad de Ciencias Económicas
   2.2 Acceso información de los concursos de oposición y mérito en la Administración Pública
   2.3 Transparencia activa y datos personales
   2.4 Obtención del padrón de egresados de la Facultad de Ciencias Económicas
   2.5 Solicitud de datos de automotores y sus propietarios a la Intendencia Municipal de Montevideo
   2.6 Carácter que poseen determinados datos personales incluidos en una solicitud de acceso a la información pública

3. REFLEXION FINAL

INDICE