Acceso a la información y datos personales: una vieja tensión, nuevos desafíos

Natalia Torres (compiladora)

Índice

Acceso a la información y datos personales: una vieja tensión, nuevos desafíos

Natalia Torres
Investigadora Principal del CELE[1]

"Aparentemente sin afectar al Estado, los burgueses crean en las logias –fuero interior secreto dentro de ese Estado- un lugar en el que se verifica, protegida por el secreto, la libertad civil.
La libertad en secreto pasa a ser el secreto de la libertad" (Koselleck, 2007: 60)

1. Introducción

El objetivo de este proyecto es generar conocimiento de la tensión entre el concepto de información personal y de acceso a la información. También tiene objetivo de desarrollar un conjunto de principios sobre la armonización de ambos conceptos.

La regulación del derecho a saber se ha extendido en el mundo y también en América Latina. Hoy, nuestra región cuenta con una serie de países[2] que han avanzado en el reconocimiento del derecho a acceder a información pública, y enfrentan los desafíos de la implementación de estas nuevas regulaciones. Uno de los principales desafíos emerge de la articulación con el entramado normativo e institucional preexistente y de la coordinación con aquellas legislaciones cuyo contenido regulan –también- la gestión de la información pública. La armonización del derecho a saber y la protección de los datos personales aparecen como uno de los nudos problemáticos y de los principales desafíos que deben enfrentar los encargados de llevar a la práctica los contenidos de las leyes de acceso a la información. Este documento es el resultado del proyecto "Acceso a la información y datos personales: una vieja tensión, nuevos desafíos", desarrollado por el Centro de Estudios sobre Libertad de Expresión y Acceso a la Información con el apoyo de Open Society Foundation. El proyecto apuntó a generar conocimiento sobre la tensión entre el concepto de datos personales y acceso a la información y a desarrollar algunas claves para la armonización entre los dos conceptos.

En esta primera sección realizaremos un breve relevamiento conceptual sobre el tema que permitió al equipo de investigación sentar los primeros pasos para el desarrollo de una metodología de trabajo uniforme para la realización de los casos de estudio en Argentina, Chile, Uruguay, México y Perú.

El documento se encuentra estructurado en cuatro secciones: en una primera se presentará una breve discusión conceptual sobre el derecho a la privacidad y la protección de los datos personales; en la segunda se esbozarán las complementariedades y tensiones existentes entre los derechos de acceso a la información y la protección de los datos personales. En esta segunda sección se analizarán las zonas de confluencia, los diseños institucionales para implementar las normativas que regulan ambos derechos y claves para la resolución de controversias. En la tercera sección se describirán los principales avances en el reconocimiento del derecho a saber y en la protección de los datos personales en América Latina. Por último, se presentará la propuesta metodológica que fue diseñada en consenso con los investigadores del proyecto.

1. El derecho a la privacidad y la protección de los datos personales

El concepto de privacidad es elusivo. Muchas veces, en lugar de encontrar definiciones cerradas, damos con definiciones negativas, que detallan los abusos, las intromisiones, los intentos por avasallarla: "…privacy is something that arouses more thought and interest in its absence or when it is threatened than in its presence" (Crompton, 2001: 2003). El recurso de la definición negativa proviene de la tradición liberal clásica que coloca al

[1] Es investigadora especializada en políticas de transparencia y acceso a la información. Es licenciada en Ciencia Política de la Universidad de Buenos Aires -donde fue docente y participó en diferentes proyectos de investigación- y fue becaria del CONICET. Recientemente, se graduó de Magister en Políticas Públicas en el University College London del Reino Unido gracias al apoyo del programa Chevening. Fue Coordinadora en temas de transparencia en la Fundación Poder Ciudadano –Capítulo Argentino de Transparencia Internacional- y Coordinadora del Área de Transparencia del Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC) desde donde lideró la promoción del derecho de acceso a la información entre el 2003 y el 2007. Como investigadora ha realizado consultorías para agencias gubernamentales, organismos multilaterales y organizaciones de la sociedad civil. Actualmente, Natalia Torres trabaja en los proyectos del CELE "Información pública y datos personales y "Hacia una política pública de la gestión de la información".
Este documento se realizó con la colaboración de Laura Cirulnik y Lucy McDonald-Stewart.

[2] Antigua y Barbuda, Brasil, Chile, Colombia, Ecuador, El Salvador, Guatemala, Jamaica, Honduras, México, Nicaragua, Panama, Perú, República Dominicana y Uruguay.

individuo en el centro de la escena y considera a todo aquello que la niega o invade como una violación a la privacidad (Paterson, 2011). La privacidad se relaciona con la protección de la autonomía individual frente a la comunidad y con la habilidad de los individuos para desarrollar sus planes de vida, sus ideas y opiniones (Banisar, 2011). Es hermana del "right to be let alone", una idea de claro contenido anti político, que pone el énfasis en los límites y las barreras más que en el contenido. La idea de privacidad aparece en los fundamentos de la Ilustración o en las condiciones de su emergencia, en aquellos fenómenos que ocurrían por fuera de la esfera pública y que dieron origen el pensamiento crítico en los albores de la modernidad. Allí, en ese espacio clandestino, allende al Estado, ahí donde los individuos construían sus opiniones emergía la clave para la construcción de la idea de privacidad y libertad: como diría Koselleck (2007), la libertad del secreto era el secreto de la libertad.

El debate, como veremos, no se da sólo sobre el contenido del derecho a la privacidad, sino también sobre el modo de nombrarlo, etiquetarlo. "Right to privacy", privacidad, derecho a la intimidad, derecho a la vida privada, son todas formas de referirse a un mismo universo de problemas. O al menos a un universo de problemas vinculados o relacionados. En este documento preferimos aproximarnos al concepto mediante su distinción, su constitución como espacio diferenciado frente a su concepto antagónico: la vida o espacio público. Siguiendo la tradición arendtiana y teniendo como horizonte la necesidad de entender el concepto frente al de acceso a la información, la distinción entre espacio público y esfera privada guiará nuestras reflexiones.

La clave entonces es encontrar la frontera entre lo público y privado o, mejor, descubrir cómo se traza la frontera entre ambos espacios. Es difícil dibujar una línea clara y definitiva: si el concepto de privacidad es elusivo, las fronteras entre lo público y lo privado se construyen local y comunitariamente. Qué es público y qué es privado finalmente dependerá de las fronteras que cada una de las comunidades erijan, de la extensión y alcance de la esfera pública, del nivel de tolerancia de sus miembros a la exposición e injerencia de su vida íntima. Llegados a este punto, si es imposible arribar a definiciones cerradas y definitivas, ¿cuál es el objetivo de este trabajo? Pues bien, el objetivo será tratar de identificar las modalidades, instituciones, mecanismos y procedimientos disponibles para definir (o desafiar) esas fronteras.

Como lo dice el título de nuestro proyecto, nuestro objetivo es analizar la tensión existente entre acceso a la información y datos personales. Nótese que hemos dicho datos personales y no privacidad, esto es, hemos decidido focalizarnos en el correlato documental de la privacidad o la materialización física y registrada del concepto. Ahora bien, privacidad y datos personales ¿son conceptos equivalentes?

Siguiendo a Banisar (2006), el concepto de privacidad se puede desconstruir en cuatro elementos:

- Privacidad informativa, que involucra las reglas para gestionar los datos personales.
- Privacidad corporal, vinculada a la protección de nuestra seguridad física frente a procedimientos invasivos
- Privacidad comunicacional, relativa a la seguridad y privacidad de la correspondencia y las comunicaciones telefónicas
- Privacidad territorial, que establece los límites a las intrusiones en los ambientes domésticos.

Como vemos en esta definición, los datos personales se relacionan exclusivamente con el primero de los elementos, el de la privacidad informativa. Sin embargo, si la privacidad informativa se vincula a la protección de los datos personales, la protección de los datos personales no se limita exclusivamente al resguardo de la privacidad, sino que refiere a un universo de problemas que lo contiene: "…el derecho a la protección de los datos personales garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada, aspecto que, de hecho, se soslaya" (Silva, 2011: 171). El espacio en donde la protección de datos personales atañe al resguardo de la privacidad es aquel espacio que ha sido protegido mediante la etiqueta de "datos personales de carácter sensible", definidos como "…aquellos datos que revelan información merecedora de especial resguardo por el mayor peligro que su tratamiento implica para las libertades y derechos ciudadanos…(…)…Entre estos se cuentan los datos relativos al origen racial o étnico de una personal, su color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo así como sobre la participación en una asociación o la afiliación a un sindicato. Algunos países, según su propia experiencia, agregan la información genética, la afiliación política u otros datos a este listado" (Silva, 2011: 171).

La relación entre datos personales y privacidad es la de dos universos que, paradójicamente, pueden contenerse mutuamente. Si, como dice Banisar, la regulación de los datos personales se corresponde exclusivamente a la privacidad informativa, la idea de privacidad (en general) contendría a los datos personales: "La protección de datos es más estrecha que la privacidad en el sentido de que la privacidad ha sido interpretado como extraviándose en los ámbitos de los derechos de la personalidad y la autonomía, mientras que la protección de datos tiene una preocupación con poner en marcha un conjunto de reglas para el manejo de datos personales." (McDonagh, 2011: 1). Pero a su vez, los datos personales pueden considerarse como un universo contenedor del concepto de privacidad: "…se comprende un conjunto de reglas para el tratamiento de los datos personales que cubren asuntos más allá del alcance de las medidas de protección de la privacidad. Estas normas abordan cuestiones como la validez, integridad, disponibilidad, pertinencia y exhaustividad de los datos personales. Además, el ámbito de aplicación de la ley de protección de datos puede ser más amplio que el de la privacidad, ya que se aplica respecto

de los datos personales, la definición de lo que puede incluir información que no puede, según el contexto, calificar como privados" (McDonagh, 2011: 1).

Contemplando esta elasticidad terminológica, pasemos entonces a analizar el universito vinculado a los datos personales y en especial lo concerniente a su regulación3. La legislación destinada a proteger los datos personales aparece recién a partir de 1960 frente al avance de las nuevas tecnologías y su capacidad de procesar gran cantidad de información sobre las personas. Recién en 1980 el derecho a la protección de los datos personales cobra autonomía bajo la etiqueta de autodeterminación informativa o libertad informativa (Silva, 2011).

La revolución informática ha llevado la protección de datos personales a un nuevo nivel. Hoy, los gobiernos enfrentan desafíos impensados en relación a la protección de la privacidad, especialmente en el contexto donde el uso extensivo de las redes sociales parece dar cuenta de una ausencia -al menos- de reflexión por parte de los usuarios sobre las implicancias de compartir datos en línea.

Novoa Monreal (1997) da cuenta de la creciente inquietud que suscitan los nuevos cambios tecnológicos para la defensa de la vida privada: "Las principales razones de inquietud provienen de: a) la expansión sin precedentes de los medios masivos de comunicación y el aumento de las informaciones de índole sensacionalista; b) nuevos descubrimientos e inventos que facilitan grandemente el acceso a la vida privada sin que el afectado se dé cuenta de ello; c) la intensificación de las relaciones y los contactos sociales, especialmente dentro de las grandes conglomeraciones humanas; d) la creciente injerencia del estado en la vida de los ciudadanos para fines de ayuda social principalmente" (Novoa Monreal, 1997: 37).

La regulación de los datos personales llegó al ámbito multilateral mediante la Directiva emitida en el Parlamento Europeo en 1995. Esta directiva constituye en cierto modo la referencia por excelencia para la definición de los datos personales que son entendidos como "toda información sobre una persona física identificada o identificable (el «interesado»); 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, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social" (PE y CUE 1995: 9).

En el contexto de la era informática, algunos organismos multilaterales y gobiernos4 han desarrollado principios orientativos para la gestión de los datos personales. Como reseña Banisar (2011), estos principios son:

- Limitación en la recolección de datos: la recolección de datos personales debe ser limitada y los datos deben ser obtenidos a través de medios legales y, cuando sea necesario, bajo el consentimiento de los sujetos propietarios de los datos.
- Calidad de los datos personales: los datos recolectados deben servir exclusivamente para el objeto que guía e impulsa su recolección y deben ser precisos y actualizados.
- Determinación del objetivo de la recolección de los datos personales: el objetivo de la recolección de la información debe encontrarse precisamente determinado y explicitado al momento del relevamiento de los datos y debe orientar su uso posterior.
- Limitación en el uso de los datos: los datos personales no deben ser publicados o entregados por motivos ajenos a los especificados en el objeto de la recolección a menos que el titular de los datos otorgue consentimiento o mediante la autorización expresa de unos funcionarios legalmente autorizados a hacerlo.
- Seguridad de las bases de datos: la información recolectada debe ser protegida frente a eventuales riesgos como pérdida, sabotajes, destrucción, etc.
- Política de apertura y rendición de cuentas: las políticas implementadas para la gestión de los datos personales deben ser públicas. La definición de lo que se considera datos personales, los objetivos de su recolección y uso, el lugar en el que se almacena y el controlador de esa información deben ser publicados. Todo controlador de base de datos de información debe dar cuentas de las políticas implementadas y el cumplimiento de los principios de la gestión de la información.
- Participación de los titulares de la información:

[3] Distinta fue la suerte de la protección de la privacidad, altamente reconocida en tratados internacionales dentro de los cuales encontramos la Declaración Universal de Derechos Humanos, El Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos, la Declaración Americana de Derechos y Deberes del Hombre y la Convención Interamericana Derechos Humanos, entre otros. Estos tratados protegen la vida privada en general y muchos de ellos sí mencionan otros aspectos de la privacidad como el territorio cuando hace referencia a violación de domicilio o la comunicación cuando hace referencia a correspondencia. Además, organismos internacionales como la Corte Europea de Derechos Humanos y el Comité de Derecho Humanos de las Naciones Unidas también han reglamentado el derecho a la privacidad. (Banisar, 2006) .

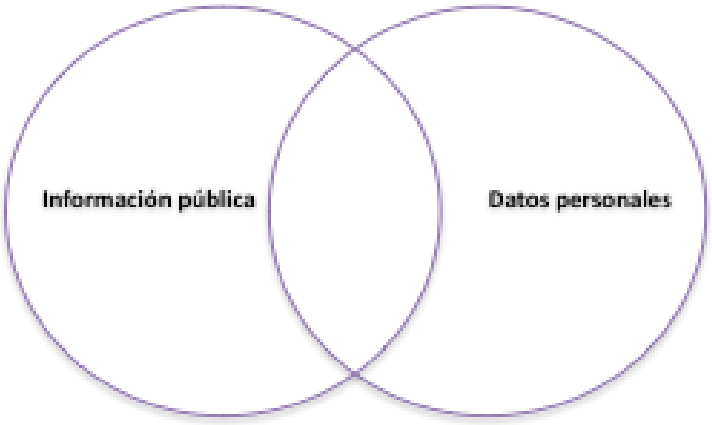
[4]Estos principios surgen de la OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data (1980), del Model Code for the Protection of Personal Information (1996) de Canadian Standards Association y de un reporte titulado Records, Computers and the Rights of Citizens (1973). del Department of Health, Education and Welfare's seminal. Y luego han sido incorporados por el Consejo Eurpeo (1981), La Asamblea General de las Naciones Unidas (1990), La Unión Europea (1995), La secretaria de la Commonwealth (2002) (Banisar, 2006).

Todo individuo debe poder confirmar si el controlador de una base de datos tiene o no datos personales suyos.

- Todo individuo debe poder obtener esa información dentro de un tiempo razonable
- Todo individuo debe recibir una explicación si la información se deniega
- Todo individuo debe poder solicitar una corrección de la información contenida en la base, ya sea rectificándola, completándola, amendándola o borrándola.

2. Acceso a la información y datos personales: una vieja tensión, nuevos desafíos

- "El hambre por la transparencia por un lado, la preocupación – la preocupación por la protección de la vida privada por el otro: dos formas de protección contra el Estado Leviatán que tienen el objetivo de restablecer el equilibrio entre el ciudadano y el Estado" (Gentot, 1999: 1).
-
- Tanto el acceso a la información como los datos personales tienen sus propias áreas de influencia donde sus normas se implementan sin injerencia de las otras, respetando la lógica interna de cada uno de los derechos bajo tutela. El objetivo de este proyecto es analizar los espacios en donde la protección y garantía de ambos proyectos confluyen, sus tensiones y sus complementariedades.



Un primer recorte sería distinguir los ámbitos de acción exclusiva. Por un lado, aquella información pública que no posee datos personales y que, por lo tanto, podría ser publicada sin consideración de los esquemas de protección a la privacidad (un presupuesto de un ministerio, por ejemplo). Por el otro, encontramos aquellos datos personales en manos de personas físicas o en manos de personas jurídicas privadas que no mantienen una relación contractual con un organismo público y que no se encuentra alcanzada por ninguna obligación de dar cuentas frente a la administración pública. Esta información podría constituir el universo de los datos protegidos por la regulación de los datos personales y excluidos del alcance de la normativa que regula el derecho a saber.

Llegados a este punto vale aclarar que el núcleo del conflicto no se da en el conocimiento de un documento público que posee determinados datos personales sino en la divulgación de esta información: "…la colisión se sitúa, en tales casos, entre la divulgación de un hecho concerniente a la vida privada de alguien y la libertad de información. Porque sabemos bien que la primera y a veces la única fase de una violación a la intimidad, se da mediante la sola intrusión que permite a otro tomar conocimiento indebido de ella. No es, entonces, esa simple toma de conocimientos de la vida privada ajena, sino la divulgación de los hechos correspondientes –que como lo sabemos es una forma derivada y no indispensable de atentar contra el bien jurídico de la intimidad. Lo que se presentará como ilícito que se lleva a cabo a través de un ejercicio abusivo de la libertad de información" (Novoa Monreal, 1997: 180).

Ahora bien, ¿cuál es entonces el área de conflicto o, mejor, cuál es el espacio en donde ambas normativas necesitan articularse para proteger y salvaguardar ambos derechos de manera armoniosa? Alberto Silva hace un primer planteo conceptual sobre el tema: "La protección de los datos personales satisface fines de interés público inherentes a una sociedad democrática. Dicha protección no solo evacua la necesidad individual de quien quiere excluirse de la vida social, sino que también actúa como salvaguarda para el libre ejercicio de sus derechos. Así, por ejemplo, al imponer limitaciones al tratamiento de datos relativos a nuestras opciones políticas, religiosas o sexuales, se fortalece el libre ejercicio del derecho de asociación, de la libertad de pensamiento y de la autodeterminación sexual, entre otros" (Silva, 2011: 166).

Banisar (2011) comienza a analizar la zona de confluencia pensando las complementariedades antes que las tensiones entre los dos derechos*: "Both rights provide an individual access to his or her own personal information from government bodies, and privacy laws allow for access to personal information held by private entibies. They also mutually enhance each other: privacy laws are used to obtein policy information in the absence o fan RTI law, and RTI laws are used to enhance privacy by revealing abuses"* (Banisar, 2011: 10). Un ejemplo de esto, siguiendo el análisis de Banisar, es la utilización de las leyes que regulan la gestión de datos personales para acceder a información en manos de empresas que de otro modo no podría ser obtenida mediante los regímenes de acceso a la información.

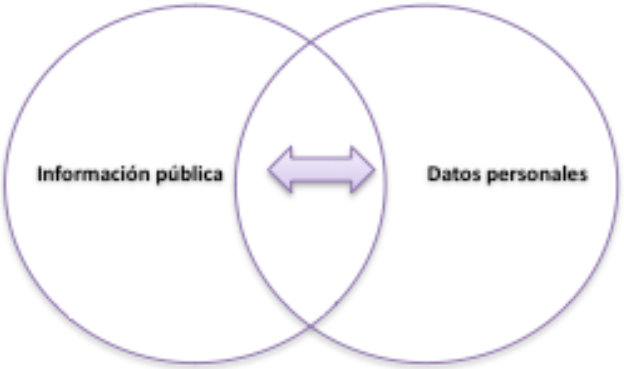
En la misma línea, Paterson (2011) destaca el rol de control que se encuentra en el centro de la legislación de datos personales: estas leyes -argumenta- apuntan a otorgarle a los individuos mayor control sobre la gestión de sus datos personales y regulan la recolección, uso, almacenamiento y publicación de la información identificable legislación. Este énfasis es el que le permite construir un modelo en el que la legislación de datos personales no debe contraponerse a la rationale de las normativas que regulan el derecho a saber: ".Hay una opinión general de que la libertad de información y la privacidad son inherentemente contradictorios: la libertad de información tiene una preocupación con la transparencia y el acceso, mientras la privacidad está preocupado con el secreto/confidencialidad y con la protección de la información de su divulgación. Sin embargo, mientras es cierto que los intereses de privacidad de los terceros pueden, en algunas circunstancias, estar en conflicto con los objetivos fundamentales de la libertad de información, la privacidad en el sentido de la privacidad de la información tiene un base principal en el control más bien que en el secretismo" (Paterson, 2011: 3). La idea de control le permite a Paterson argumentar a favor de una conceptualización más positiva de la privacidad en donde ésta no se refiera simplemente a la ausencia de información de nosotros en la mente de otros sino al control que nosotros tenemos sobre la información referida a nuestras vidas (Paterson, 2011). Paterson sale de la tradición liberal para pensar positivamente, políticamente.

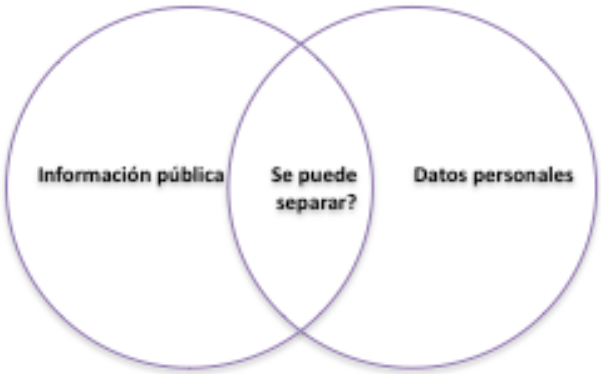
2.1 Zonas de confluencia

Uno de los temas en donde la regulación de ambos derechos confluye aparece en el modo en que es gestionada y protegida la **información de los individuos en los organismos públicos**. Un punto quizás menos conflictivo, aparece en la necesidad de determinar, ya sea mediante reglas escritas o a través de prácticas administrativas, el modo en que deben responder la solicitud de los individuos de la información que sobre ellos se encuentra en organismos públicos. Cuando un país cuenta con ambas normativas, ¿qué régimen o mecanismo es el que prima en estos casos: el recurso de habeas data o el pedido de información pública? ¿Qué sucede en aquellos países que cuentan con una normativa pero no la otra? Será como dice Banisar (2011) que el acceso a la información, ¿puede asistir a los individuos para acceder a la información que sobre ellos poseen los organismos públicos? Casos más conflictivos se presentan cuando se presenta un pedido de información pública sobre un tercero cuando éste no es un funcionario público. Aquí el abanico de situaciones que pueden presentarse es bastante extensa y van desde los listados de beneficiarios de planes sociales hasta los registros en causas judiciales hasta información de carácter sensible contenida en documentos públicos.

Otro de los puntos que han generado más tensiones que complementariedades es el modo en que es gestionada, protegida y divulgada la **información sobre funcionarios públicos**. Las tensiones se dan a lo largo de un extenso abanico que va desde la solicitud de la nómina de los funcionarios y empleados públicos hasta el pedido de conocer los antecedentes médicos de los altos mandatarios.

Ahora bien, las tensiones no se dan solamente sobre el contenido de la intersección entre los espacios de acción de los dos conceptos, sino también en relación a la extensión de la zona de confluencia, el tiempo en que determinada información pública que posee datos personales debe ser preservada y a cuán separable es aquella información que puede ser publicada de la que debe ser protegida (Szekely, 2007):





2.3. Claves para la resolución de controversias

Definir las fronteras, establecer qué tan amplio es el espacio de convergencia para la garantía de ambos derechos, identificar los modos de separar la información pública que debe ser publicada de la que necesita ser resguardada, todo esto requiere de algunas claves, de criterios que orienten la resolución de controversias. A continuación veremos algunas indicaciones que permiten la actividad interpretativa en estos temas.

Las excepciones vinculadas a la privacidad y a la gestión de los datos personales establecidas las leyes de acceso a la información son una de las principales claves para resolver las controversias o tensiones entre ambos derechos. Cómo determinar si estas excepciones deben ser aplicadas o no es el punto nodal del dilema y es este punto el que ha sido abordado tanto la Ley Modelo de Acceso a la Información de la OEA como la Guía para la Implementación de la Ley Modelo de la OEA.

La Ley Modelo en su artículo 40 establece que el acceso a la información podrá restringirse cuando: "Dañare los siguientes intereses privados: 1. el derecho a la privacidad, incluyendo privacidad relacionada a la vida, la salud o la seguridad". Con respecto a este punto aclara que "las excepciones (…) no deberán aplicarse cuando el individuo ha consentido en la divulgación de sus datos personales o cuando de las circunstancias del caso surja con claridad que la información fue entregada a la autoridad pública como parte de aquella información que debe estar sujeta al régimen de publicidad" (OEA, 2010)

Más adelante, en un comentario de el mismo artículo 40, brinda más aclaraciones sobre el modo en que debe interpretarse este punto: "Para cumplir con los estándares del sistema interamericano requiriendo un régimen de excepciones claro y preciso, se entenderá que el texto en corchetes del literal (b) "definido de manera más detallada mediante ley", incluye las definiciones realizadas a través de la legislación o de la jurisprudencia, de las cuales resultará una definición de las excepciones. Asimismo, aunque este texto permite que se definan de manera más detallada por ley, la operación de dichas definiciones adicionales se limita por los principios y disposiciones de esta ley. A dicho efecto, la ley establece un derecho amplio de acceso a la información basado en el principio de máxima divulgación (artículo 2); establece que esta ley prevalece sobre cualquier otra legislación, en casos de inconsistencia (artículo 4); y requiere que cualquier persona a cargo de interpretar la ley o algún otro instrumento que puede llegar a afectar el derecho de acceso a la información adopte cualquier interpretación razonable a favor de la divulgación (artículo 8)".

La ley avanza en la incorporación del test de interés público como guía máxima para la aplicación de las excepciones:
"52. La carga de la prueba deberá recaer en la autoridad pública a fin demostrar que la información solicitada está sujeta a una de las excepciones contenidas en el artículo 41. En particular, la autoridad deberá establecer:

a) que la excepción es legítima y estrictamente necesaria en una sociedad democrática basada en los estándares y jurisprudencia del sistema interamericano;

b) que la divulgación de la información podría causar un daño sustancial a un interés protegido por esta ley; y

c) Que la probabilidad y el grado de dicho daño es superior al interés público en la divulgación de la información".

La Guía de Implementación de la Ley Modelo explica el modo en que la prueba de interés público y las pruebas de daño deben aplicarse. Básicamente la guía explica que estas pruebas "son normas contra las que se deben ponderar la justificación de una excepción a la divulgación a fin de determinar si satisface los requisitos de proporcionalidad y necesidad. Al aplicar esas pruebas, es necesario adoptar una interpretación restrictiva de la excepción, como se señala en este capítulo. La presunción de la divulgación requiere, pues, que la excepción sea lo menos restrictiva posible; es decir, la no divulgación debe tener un efecto directo en el ejercicio de una excepción en particular, ser proporcionada para el interés público o privado e interferir lo menos posible con el ejercicio efectivo del derecho de acceso" (OEA, 2010bis: 11). La guía se apoya en el aporte de la Relatora Especial para la Libertad de Expresión que destacó que "…la excepción debe pasar una prueba de tres partes: a) debe estar relacionada con uno de los objetivos legítimos que la justifican; b) debe demostrarse que la divulgación de la información efectivamente amenaza causar un perjuicio sustancial a ese objetivo legitimo; y c) debe demostrarse que el perjuicio al objetivo es mayor que el interés público en contar con la información" (OEA, 2010bis: 11).

Por su parte, la Corte Interamericana de Derecho Humanos también se ha pronunciado sobre el modo en que la regulación del derecho a saber debe atender a las excepciones. Al respecto afirma que las restricciones al derecho de acceso a la información deberán cumplir los siguientes requisitos:

- "Deben estar previamente fijadas por ley como medio para asegurar que no queden al arbitrio del poder público. Dichas leyes deben dictarse por razones de interés general y con el propósito para el cual han sido establecidas" (CIDH 2006: 47).
- "La restricción establecida por ley debe responder a un objetivo permitido por la Convención Americana" (CIDH 2006: 47). -
- "Deben ser necesarias en una sociedad democrática (…) Entre varias opciones para alcanzar ese objetivo, debe escogerse aquélla que restrinja en menor escala el derecho protegido. Es decir, la restricción debe ser proporcional al interés que la justifica y debe ser conducente para alcanzar el logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho." (CIDH 2006: 47)

- También la emisión de lineamientos interpretativos es una buena alternativa para la resolución uniforme de las controversias. Mendel (2011) da cuenta de esta opción: "se utilizan normalmente las reglas secundarias tanto cuando se requiere flexibilidad (porque se pueden atender con mucha más facilidad que la legislación primaria) como cuando el nivel de RETAIL? requerida es tanto que resulta más eficaz para dejar el asunto a ser elaborado por un ministro en lugar de toda una legislature" (Mendel, 2011: 17). Un ejemplo regional de este tipo de regulaciones secundarias se refleja en la acción del IFAI que ha emitido una serie de lineamientos para ordenar la gestión de los datos personales en el ámbito público5.
-
- Otra vía para la resolución de controversias puede ser cierta armonización normativa mediante la reforma de la legislación. Mendel (2011) analiza las diferentes posibilidades de reforma legislativa que pueden presentarse en la efectiva implementación de las leyes de acceso a la información y en la armonización con otros marcos normativos. Las reformas pueden no sólo contemplar estas cuestiones de articulación con otras normativas sino dirigirse a corregir una amplia serie de problemas. De acuerdo a Mendel (2011), gran parte de estas reformas han tenido por objeto corregir el régimen de excepciones de las propias leyes de acceso a la información, pero hay otros casos en los que son las normativas preexistentes las que son modificadas.

Ahora bien, como decíamos con anterioridad, el objetivo de este proyecto es indagar sobre el modo en cada uno de los países ha establecido reglas para resolver las controversias, y esto supone considerar los mecanismos e instituciones encargadas de hacer efectivo el contenido de las normativas. En la próxima sección analizaremos los diseños institucionales disponibles en la experiencia internacional para implementar las leyes de acceso a la información y la protección de los datos personales.

2.2 Diseño institucional

La experiencia internacional muestra que el abanico de diseños institucionales disponibles para implementar las normativas que regulan el derecho a saber pueden ser descriptos de acuerdo a dos aspectos o funciones que los organismos deben ejecutar a la hora de hacer efectivo el contenido de las normativas: la implementación de políticas promotoras del derecho a saber (políticas que deben considerar tanto a la administración pública como a la comunidad en general); y la resolución de controversias. Ésta última es un aspecto clave para distinguir entre diseños institucionales y resultará fundamental a la hora de analizar el modo en que las diferentes unidades de estudio definen qué información pública con datos personales puede ser entregada o no. En términos generales, la

[5] http://ifai.org.mx/regulacion/regulacion

clave se encuentra en determinar cuál es la instancia institucional a cargo de decidir la publicación de la información (Torres, 2009).

Siguiendo a Banisar (2006) y a Torres (2009), es posible identificar en la experiencia internacional los siguientes diseños institucionales:

- revisión interna: la posibilidad de revisar internamente la decisión de brindar o no una información aparece en casi todos los países incluso si estos tienen otros mecanismos específicos para la resolución de controversias vinculadas a la gestión de la información pública. La revisión interna puede ser utilizada en los casos en que, frente a la denegatoria de cierta información, los particulares quieren apelar a una instancia superior la decisión de un organismo público. Las excepciones a este modelo son Bulgaria, Japón y Turquía que no cuentan con estos mecanismos. Otros países solo tienen este tipo de revisiones, a veces combinadas con la posibilidad de apelar a las cortes: Austria, Georgia, Holanda, Tajikistan, Ucrania y Estados Unidos (Banisar, 2006; Torres, 2009).

- revisión del Defensor del Pueblo: la capacidad de revisión que poseen los defensores del pueblo resulta de una decisión delegativa explícita (en la legislación sobre acceso a la información) o de una extensión de sus atribuciones generales de defender el interés público de los abusos de poder de los gobiernos. Los defensores son generalmente oficiales independientes designados por los cuerpos legislativos y pueden tener el poder de emitir decisiones de carácter vinculante. Los defensores pueden revisar las decisiones de los organismos públicos en Albania, Armenia, Australia, Azerbaijan, Belize, Bosnia y Herzegovina, Republica Checa, Dinamarca, Ecuador, Finlandia, Grecia, Kosovo, Moldova, Nueva Zelanda, Noruega, Pakistán, Perú, Filipinas, Polonia, Rumania, España, Suecia y Trinidad y Tobago (Banisar, 2006; Torres, 2009).

Revisión por una Comisión de Información: este particular diseño institucional fue establecido por diferentes legislaciones para garantizar su enforcement e independencia (Diaz and Valdivia, 2006). La ubicación de estas comisiones dentro del organigrama puede variar: “Las comisiones pueden ser parte del Parlamento, una parte independiente de un otro órgano de gobierno o de la oficina del Primer Ministro (como en Tailandia) o un órgano complete y independiente" (Banisar, 2006: 23). Angola, Antigua & Barbuda, Belgium, Canada, Estonia, France, Germany, Hungary, Iceland, India, Ireland, Macedonia, Mexico, Portugal, Serbia, Slovenia, Switzerland, Thailand and UK crearon comisiones de este tipo, que varían en presupuesto y atribuciones, principalmente en su capacidad de emitir decisiones vinculantes (Banisar, 2006; Torres, 2009).

- revisión por un tribunal especial: para resolver controversias Australia, Jamaica, Japón y UK han delegado esa atribución a tribunales especializados en acceso a la información (Banisar, 2006; Torres, 2009). Estos tribunales –como cualquier otros tribunales- se encuentran generalmente separados de la administración que es analizada (Shapiro, 2002) y son generalmente establecidos para reducir el acopio de trabajo de las cortes generales y para desarrollar expertise y uniformidad en la resolución de casos (Hansen et al, 1995).

- revisión por las cortes nacionales: la posibilidad de apelar a las cortes ha sido garantizada en casi todos los países. Una vez que el acceso a la información ha sido reconocido como derecho, cualquier persona debe tener la posibilidad de presentar una demanda toda vez que su derecho a saber ha sido vulnerado. En estos casos, la legislación sobre el derecho a saber, ha delegado explícita o implícitamente no solo la capacidad de resolver controversias a los jueces sino también alguna capacidad de policy-making en tanto ellos serán quienes interpreten el contenido de las regulaciones (Shapiro, 2002). En casi todos los casos las cortes supremas permanecen como la instancia revisora final. Bulgaria, Israel, US y Uzbekistan poseen solo esta instancia institucional (Banisar, 2006). Esta situación puede traer aparejados algunos problemas: primero, estos sistemas requieren que los solicitantes formalicen su presentación, lo cual puede excluir a aquellos que carecen de los recursos económicos o simbólicos para presentar una demanda en sede judicial. En segundo lugar, en países con sistemas judiciales continentales puede ser más difícil arribar a patrones uniformes para la resolución de controversias y limitar la discrecionalidad de los jueces. En tercer lugar, en tanto las cortes no poseen la capacidad de implementar sus resoluciones (Rosenberg, 1991), la posibilidad de generar un cambio en la política burocrática generalmente depende del análisis de costo-beneficio de las agencias para seguir la decisión de las cortes (Spriggs II, 1996). Finalmente, en sistema con una cultura del secreto fuertemente instalada, puede resultar complejo revertir estas prácticas culturales en la administración con la sola acción de los jueces.

Si este ha sido el modo en que la experiencia internacional ha definido el modo en que se implementa la normativa y se resuelven las controversias vinculadas a la publicación o protección de información pública, ¿qué ocurre cuando pensamos la implementación del derecho a saber en relación a la protección de los datos personales? ¿Cómo se ha legislado este tema, como se ha organizado la implementación de las políticas de salvaguarda de la información de los individuos, cómo se ha resuelto la resolución de controversias?

Un primer nivel de análisis corresponde al plano meramente normativo: ¿cómo ha definido el legislador la regulación del derecho a la información y la protección de los datos personales?

Algunos países han resuelto esta cuestión emitiendo una legislación común para los dos temas. Este es el caso de Hungría o Tailandia, por ejemplo, cuyas leyes regulan tanto el acceso a la información como la protección de los datos personales. Según Banisar, existen algunas desventajas en esta modalidad: "...tener ambas funciones juntas puede engendrar confusión legislativa sobre el intento de las leyes y puede resultar en la oposición de algunos partidos que de otra manera apoyarían a un acto u otro. Una cuestión más práctica es la complejidad de la legislación, que puede resultar a los legisladores no dispuestos a revisarlo porque les falta el tiempo" (Banisar, 2011: 17). En otros casos, los países han regulado el derecho a saber pero no la protección de los datos personales (por ejemplo, Bélice, Brasil, Jamaica, Guatemala); otros han regulado la protección de los datos personales pero no el acceso a la información (Costa Rica y Paraguay, por nombrar algunos casos); en otros casos, no se han regulado ninguno de los dos (Venezuela, por ejemplo). En la sección 3 presentaremos un relevamiento de las diferentes situaciones encontradas en América latina.

Un segundo nivel de análisis corresponde a los diseños institucionales aplicados para la implementación de políticas destinadas a garantizar el acceso a la información y la salvaguarda de los datos personales. Consideremos las diferentes situaciones que podrían derivarse del nivel normativo:

- Aquellos países que no han regulado ninguno de los dos derechos, es de imaginar que las controversias sobre la publicación o no de la información pública con datos personales sea resuelta mediante mecanismos de revisión administrativa o en sede judicial. Así lo demuestra el caso de Venezuela.
- Aquellos países que han regulado el derecho a saber pero no la protección de los datos personales. En estos casos, los gobiernos seguramente harán uso del abanico de diseños institucionales descriptos con anterioridad, esto es, los diseños destinados a implementar las leyes de acceso a la información (revisión interna, revisión en manos de un defensor del pueblo, revisión en manos de una comisión de información específicamente creada para la implementación de la ley de acceso a la información, revisión a cargo de un tribunal especializado o en manos de las cortes nacionales).
- Aquellos países que han regulado la protección de los datos personales pero no la gestión de la información pública. En estos casos, podría conjeturarse que los países se han servido de la posibilidad de crear nuevos organismos independientes similares a las comisiones de información descriptas –como ha ocurrido en Europa donde la Unión Europea consignó como requisito que las comisiones de protección de datos personales debían ser independientes. Otro caso posible es la creación de un órgano interno a la administración, como en el caso de Argentina en donde la Dirección Nacional para la Protección de Datos Personales, que funciona en el ámbito del Ministerio de Justicia, es el organismo encargado de implementar políticas para salvaguardar estos datos y emitir directivas sobre la gestión de la información personal. En este caso, de todos modos, la resolución de controversias recae finalmente en sede judicial.

Aquellos países que han regulado ambos derechos pero que han instituido organismos separados para implementar las leyes de acceso a la información y protección de datos personales respectivamente. En estos casos, los organismos encargados de hacer efectivo el contenido de las regulaciones del derecho a saber obedecerán a la gama de opciones que hemos descrito con anterioridad. En el caso de los organismos destinados a garantizar la salvaguarda de los datos personales, el diseño institucional puede seguir el modelo de comisión independiente –como es el caso del modelo de los países de la Unión Europea- o, en instancia administrativa, como vimos anteriormente en el caso argentino. Esta situación, de acuerdo a Banisar, presenta sus ventajas: "... una comisión independiente para cada uno de los dos Derechos puede crear defensores específicos para tales Derechos, no limitados por la necesidad de equilibrar los intereses potencialmente competitivos" (Banisar, 2011: 23) y desventajas: "... una preocupación principal de tener dos organismos es que habrá conflicto entre los dos - y que podría llegar a ser complicado, costoso y vergonzoso. (...) También hay una preocupación de que los organismos públicos y el público recibirán consejos contradictorios de los dos comisionados cuando ellos no están de acuerdo" (Banisar, 2011: 24).

Aquellos países que han regulado ambos derechos y han instituido un solo organismo para garantizar tanto el derecho a saber como la protección de datos personales. Esta situación se presenta más comúnmente cuando ambos derechos son contemplados en una única normativa –como en el caso de México con el IFAI-, pero esta situación no se da exclusivamente en esas circunstancias: "En la mayoría de los casos, una comisión existente se da autoridad suplementaria a la adopción de una nueva legislación. En el Reino Unido, la Comisión de Protección de Datos se desarrolló en la Comisión de Información. Un proceso similar también ocurrió en Alemania, Malta y Suiza. En Eslovenia, los dos organismos se unieron en una sola nueva comisión encabezada por el comisionado de información anterior" (Banisar, 2011: 25). A diferencia de lo que ocurre cuando se tienen dos organismos diferenciados, el contar con un solo organismo tiene el beneficio de desarrollar expertise compartido y reducir las situaciones de conflicto. También permite crear interlocutores uniformes para la consulta por parte de los funcionarios y de la ciudadanía. También se ha afirmado que este diseño permite optimizar recursos, aunque habría que evaluar si efectivamente esto sucede, en tanto se deben implementar dos tipos de políticas, ya sea desde uno o desde dos organismos. Sin embargo, este modelo también ha cosechado críticas: "el peligro de que un interés

puede ser más fuerte o se puede percibir como más poderosos y que los organismos no se protegen igualmente ni se equilibran igualmente los ambos intereses" (Paterson, 2011: 25).

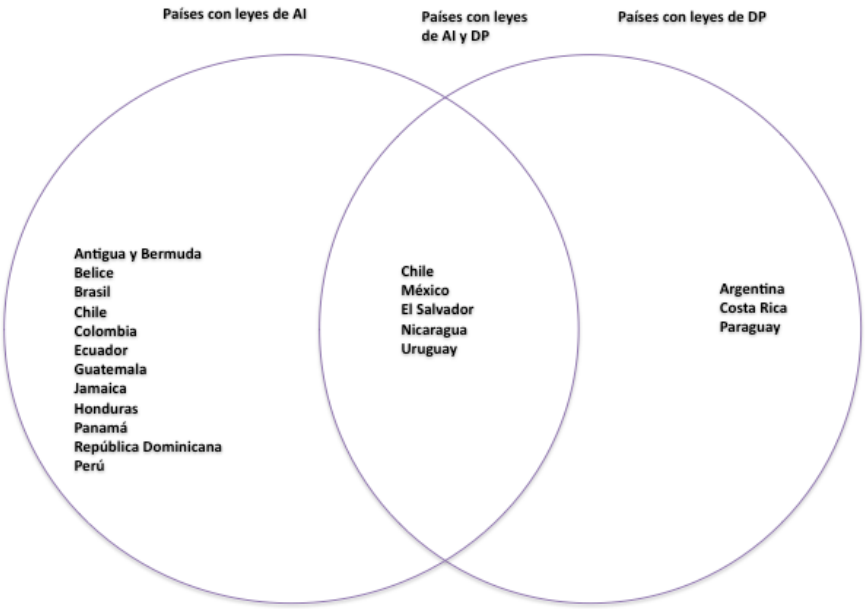
En la próxima sección analizaremos el modo en que el derecho a saber y la protección de datos personales han sido reconocidos normativamente en América Latina y presentaremos descriptivamente los diseños institucionales empleados en los países de la región.

3. Acceso a la información y datos personales en América Latina

"América Latina está adoptando leyes que reglamentan el tratamiento de datos personales de un modo integral, esto es, en las que sea comprendido el procesamiento de la información tanto por el sector público como por el privado. Diversas razones explican este fenómeno: los nuevos bríos democráticos, que invitan a brindar adecuada protección a los derechos de las personas; el afán de minimizar la incertidumbre de un modelo de protección basado solo en disposiciones constitucionales; pero más significativamente, la aspiración de transformarse en un país que brinda un nivel de protección adecuado, de acuerdo con los estándares promovidos por la Unión Europea, a efectos de acceder a la transferencia de datos personales desde esta y, con ello, facilitar la inversión de aquellos nichos de mercado que suponen tratamiento de datos provenientes de aquella. Así, al temprano reconocimiento de Argentina como país seguro, se suma el inminente de Uruguay; en tanto, Colombia, Costa Rica, México y el Perú han modificado recientemente su legislación interna para tales efectos; mientras que Brasil y Chile cuentan ya con iniciativas legislativas en la materia"
(Silva, 2011: 170).

De acuerdo a Silva (2011), en América Latina se registró un avance importante en el reconocimiento de la protección de datos personales como derecho autónomo y brindándole vías de acción específicas para su reclamo como la acción de amparo o el habeas data, pero ha fallado en los altos costos transaccionales que supone dirimir controversias vinculadas a la protección de datos personales en sede judicial: "la normativa constitucional no ha sido suficiente para garantizar un adecuado nivel de protección de los datos personales en América Latina. Esto sucede porque dicho resguardo se verifica preferentemente en sede judicial y ello trae aparejado una serie de limitaciones, tales como sus altos costos transaccionales; su ineficacia para prevenir infracciones y su falta de experiencia en temas que, en ocasiones, resultan altamente técnicos. Además, como en los demás países depositarios de la tradición del derecho civil, en los países latinoamericanos, los precedentes judiciales carecen de fuerza obligatoria en casos futuros, salvo limitadas excepciones. Así en la práctica, ello obliga a reiniciar acciones judiciales individuales a cada uno de los titulares de los datos personales afectados por un ilegítimo tratamiento…" (Silva, 2011: 169). Es por eso que es tan importante analizar qué sucede con la aparición de las leyes que regulan el derecho a saber y la llegada de mecanismos institucionales para la resolución de controversias. ¿Podrán reducir estos costos transaccionales? ¿Los aumentarán?

En el siguiente diagrama podemos observar los países de la región que han avanzado en la regulación del derecho a saber y de los datos personales.



Como muestra el diagrama Antigua y Barbuda6, Belice7, Brasil8, Chile9, Ecuador10, Guatemala11, Jamaica12, Honduras13, Panamá14, República Dominicana15, Colombia16, México17, Nicaragua18, Uruguay19, El Salvador20 y Perú21 han avanzado en el reconocimiento del derecho a saber.

Argentina, Costa Rica y Paraguay cuentan con normativas vinculadas a los datos personales pero han quedado rezagados en el reconocimiento del derecho de acceso a la información, aunque esto podría revertirse en un futuro cercano si consideramos que se han presentado proyectos legislativos para superar esta área de vacancia. Hace falta aclarar en este contexto que Argentina cuenta con un decreto que regula el acceso a la información en el ámbito de los ejecutivos nacionales.

Argentina22, Costa Rica23 y Paragua24, Chile25, El Salvador26, Uruguay27, Perú28, México29 y Nicaragua30, le han dado un marco normativo a la protección de datos personales.

Mientras tanto,
Chile, México, Nicaragua, Perú, Uruguay y El Salvador se destacan en el diagrama como los países que han logrado sancionar regímenes normativos para la protección de la información pública y los datos personales.

Es interesante apreciar cierta oleada en la sanción de las normativas, si consideramos la dimensión cronológica-temporal. En el caso de las leyes que regulan el derecho a saber, es claro que la oleada se dio con la llegada del nuevo milenio:

Año de sanción de la ley	País
1985	Colombia
1994	Bélice
2002	Jamaica
2002	México
2002	Panama
2002	Perú
2004	Antigua y Barbuda
2004	Ecuador
2004	República Dominicana
2006	Honduras
2007	Nicaragua
2008	Chile
2008	Guatemala
2008	Uruguay
2011	Brasil
2011	El Salvador

[6] http://www.laws.gov.ag/acts/2004/a2004-19.pdf
[7] http://www.freedominfo.org/documents/Belize%20FOIA%201994.pdf
[8] http://www.freedominfo.org/2011/11/president-rousseff-signs-access-to-information-law/
[9] http://www.leychile.cl/Navegar?idNorma=276363&tipoVersion=0
[10] http://www.wipo.int/wipolex/es/text.jsp?file_id=251793
[11] http://168.234.200.197/docs/infpublic.pdf
[12] http://www.jis.gov.jm/special_sections/ATI/ATIACT.pdf
[13] http://www12.georgetown.edu/sfs/clas/pdba/Security/citizensecurity/honduras/leyes/LeyInfoPublica.pdf
[14] http://www.presidencia.gob.pa/ley_n6_2002.pdf
[15] http://optic.gob.do/Portals/4/docs/Ley_200-04_Acceso_Informacion_Publica.pdf
[16] http://www.unal.edu.co/secretaria/normas/ex/L0057_85.pdf
[17] http://www.redipd.org/documentacion/legislacion/common/legislacion/mexico/por_estados/mexico.pdf
[18] http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2?OpenDocument
[19] http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18381&Anchor=
[20]
http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCUQFjAA&url=http%3A%2F%2Fwww.minec.gob.sv%2Findex.php%3Fop
[21] http://www.produce.gob.pe/RepositorioAPS/1/jer/DERACUI/docs/ley_27086_ley_acceso_info_pub.pdf
[22] http://www.protecciondedatos.com.ar/ley25326.htm
[23] http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=508:ley-proteccion-de-datos-personales-costa-rica&catid=1:datos-personales&Itemid=54
[24] http://www.morinigoyasociados.com/todas_disposiciones/2001/leyes/ley_1682_01.htm
[25] http://www.leychile.cl/Navegar?idNorma=141599
[26]
http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCUQFjAA&url=http%3A%2F%2Fwww.minec.gob.sv%2Findex.php%3Fop
[27] http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331
[28] http://www.pcm.gob.pe/Transparencia/Resol_ministeriales/2011/ley-29733.pdf
[29] http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010
[30] http://www.presidencia.gob.ni/index.php?option=com_content&task=blogcategory&id=95&Itemid=1

En el caso de la regulación de la protección de los datos personales, parecería que esta es una etapa que recién se inicia:

Año de sanción de la ley	País
1999	Chile
2000	Argentina
2001	Paraguay
2001	República Dominicana
2002	México
2008	Uruguay
2011	Costa Rica
2011	Perú
2012	Nicaragua

Pasemos ahora a presentar los diseños institucionales encargados de implementar las normativas de acceso a la información y protección de los datos personales:

Como podemos observar, México, Antigua y Barbuda, Chile, Guatemala, El Salvador, Honduras, Jamaica, Nicaragua y Uruguay han creado un organismo para implementar el contenido del derecho a saber. Por otro lado Republica Dominicana ha creado para esta tarea distintas oficinas de acceso a la información. En el caso de Ecuador, Perú y Belice, han decidido delegar dichas tareas en manos del Defensor del Pueblo.

En el caso de México y El Salvador, las legislaciones de acceso a la información alcanzan también la regulación y protección de datos personales y la autoridad de aplicación es la misma: el IFAI, el Instituto Federal de Acceso a la Información Pública en el caso de México y el Instituto de Acceso a la Información en el caso de El Salvador.

4. Propuesta metodológica

La metodología que fue aplicada para el desarrollo de los casos de estudio en México, Perú, Uruguay, Chile y Argentina fue desarrollada de manera colaborativa junto a los consultores del proyecto en un encuentro realizado a partir de una propuesta metodológica elaborada por el CELE.

La descripción completa de la metodología ha sido incluida en este documento en el Anexo I. Pero solo como referencia aquí mencionaremos que la estrategia metodológico fue de carácter cualitativo cuya intención fue analizar principalmente cuatro aspectos: el reconocimiento de los derechos de acceso a la información y datos personales, los diseños institucionales destinados a implementar ambas normativas, las acciones desarrolladas en cada uno de estos países para armonizar ambos derechos y las buenas prácticas identificadas.

Bibliografía General

- Alianza Regional (2011) *Informe Saber más III. Informe regional sobre acceso a la información pública y protección de datos personales*, disponible en
. http://www.scribd.com/doc/66655681/Informe-SABER-MAS-III

- Banisar, D. (2001) *Freedom of information and acces to record arround the world*, disponible en
http://obcan.ecn.cz/docs/FOI_survey.pdf

Banisar, D. (2006) "*Freedom of Information around the world 2006*", Privacy International

-Banisar, D, (n.d) *Government Secrecy. Decisions without Democracy, People for de the American Way Foundation*, disponible en
http://www.openthegovernment.org/sites/default/files/otg/govtsecrecy.pdf

- Banisar, D. (2011) *the Right to Information and Privacy: Balancing Rights and Managing Conflicts*. The World Bank, Accesos to Information Program. Washington

- Canadian Standards Association Group (1996), *Model Code for the Protection of Personal Records, Department of Health, Education and Welfare's seminal Computers and the Rights of Citizens*.

- Cerda Silva, A. J. (2011), *"Protección de datos personales y prestación de servicios en línea en América Latina*" en Hacia una internet libre de censura. Propuestas para América Latina, Universidad de Palermo, Facultad de Derecho, Centro de estudios para la Libertad de Expresión y Acceso a la Información, Buenos Aires

-Cromptom, M. (2001) *what is Privacy? In Privacy and Security in the Informarion Age Conference*, 16.17 Agust 2001

- European Public Sector Information Platform (n.d), *ECJ rules on Farm Subsidy case*, disponible en
http://epsiplatform.eu/content/ecj-rules-farmsubsidy-case-privacy

- Gentot, M. (1999) *Access to Information and Protection of Personal Data*, 21st International Conference on Privacy and Personal Data Protection, Office of the Privacy Commissioner for Personal Data, Hong Kong.

- Gregorio, C., G. (n.d.) *América Latina - Juan Pérez ante una disyuntiva de progreso y bienestar*. Argentina, Instituto de Investigación para la Justicia, disponible en
http://www.iijlac.org/docs/juanperez.pdf

- Global Internet Liberty Campaign (n.d.) *Privacy and Human Rights. An international survey of privacy laws and practice*, disponible en: http://gilc.org/privacy/survey/intro.html.

- Hensen, W., Johnson, R., and Unah, I. (1995) *Specialized courts, bureaucratic agencies and the politics of US Trade Policy*, American Journal of Political Science, August 1995, v. 39, nº 3, pp. 529-577

- Koselleck, R (2007) Crítica y crisis en el mundo burgués, Madrid, Rialp.

- McDonagh, M (2011*) Balancing privacy and access in European law*. [Invited Oral Presentation], First Global Conference on Transparency Research, Rutgers University, Newark, New Jersey, disponible en
http://spaa.newark.rutgers.edu/home/conferences/1stgctr/indexed-papers.html#privacy

- Minutti Zanatta, R. (2012) *Acceso a la Información Pública y a la Justicia Administrativa en México*. UNAM, México, disponible en: http://biblio.juridicas.unam.mx/libros/libro.htm?l=3044

Novoa Monreal, E (1997)

- Organización de Estados Americanos (2010*) Ley Modelo Interamericana sobre Acceso a la Información Pública*

- Organización de Estados Americanos (2010) *Comentarios y guía de Implementación para la Ley Modelo Interamericana sobre Acceso a la Información*

- Organización de Estados Americanos (2010) *Proyecto de Principios y Recomendaciones Preliminares sobre la Protección de Datos*

- Organization for Economic Co-oparation and Development (1980*) OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data*

- Rosenberg, G. (1991) *The hollow hope: can courts bring about social change?* University of Chicago Press.

- Shapiro, M (2002) *Judicial delegation doctrines: the US, Britain and Grance*, West European Politics, January 2002, v. 25, nº 1, pp. 125-147.

- Spriggs II, J. (1996*) The Supreme Court and federal administrative agencies: a resource-based theory and analysis of judicial impact*, American Journal of Political Science, November 1996, v. 39, nº 3, pp. 529-577.

- Székely, I (2007). *Freedom of Information vs. Privacy (Privacy vs. Freedom of Information?)*, disponible en En http://www.cpdpconferences.org/Resources/Szekely.pdf

- Szekely, I., Szabo, D. (2004) *Privacy and data protection at the workplace in Hungary*di, sponible en http://szabomat.hu/tanulmany/privwphung.pdf

-Thomas, R. (2008) Freedom of Information and Privacy – the Regulatory Role of the Information Commissioner. United Kingdom, Centre for Regulated Industries, disponible en http://www.ico.gov.uk/upload/documents/library/freedom_of_information/notices/cri_lecture_jan08.pdf

- Travieso, J. A. *Conferencia Magistral Desarrollo y Globalización. Biblioteca Jurídica virtual del instituto de investigaciones jurídicas de la UNAM*, disponible en *http://www.bibliojuridica.org/libros/6/2502/5.pdf*

- UNESCO Paris (2008), *History of Humanity: scientific and cultural development. The twentieth century*, Paris, United Nations Scientific and Cultural Organization, disponible en http://books.google.com.ar/books?id=DtnHLh9HgqAC&pg=PA542&lpg=PA542&dq=david+banisar+personal+data&source=bl&ots=kF-wI7Hlpd&sig=LFYij7w6lXLRtKubaScX9V0NCg0&hl=es-19&sa=X&ei=IvcOT5bKMeLL0QGnjKyUAw&ved=0CGgQ6AEwCQ#v=onepage&q=david%20banisar%20personal%20data&f=false

-Villanueva, E. (2009) *Leyes de acceso a la información pública en América Latina*, disponible en http://alianzaregional.net/site/images/pdf/reuniones/quinta_reunion/ppt_villanueva.pdf

Ward, C. (n.d.) *The Bavarian Lager and TGI Cases: Transparency v Privacy and Investigations*, disponible en (http://www.actnow.org.uk/media/articles/BavarianLagerAndTGI.pdf)

Legislación general

- Antigua y Barbuda (2004) Ley Nº 19 del 2004.
- Argentina (2000) Ley 25.326. Protección de los Datos Personales.
- Argentina (2003) Decreto N° 1172/2003 Sobre Acceso a la Información Pública.
- Bélice (1994) Ley Nº 9 de 1994 Freedom of Information Act.
- Bolivia (2004) Decreto Supremo Nº 2732, Decreto Sobre la Transparencia y el Acceso a la Información.
- Brasil (2012) Ley Nº 12.527
- Chile (1999) Ley Nº 19.628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal.
- Chile (2008) Ley Nº 20.2858 Sobre Acceso a la Información Pública.
- Colombia (1985) Ley 57 DE 1985 por la cual se ordena la publicidad de los actos y documentos oficiales.
- Convención Americana sobre Derechos Humanos (1969), arti. 11.
- Convenio Europea de Derechos Humanos (1950), art. 8.
- Costa Rica Ley Nº 8968 Protección de la Persona Frente al Tratamiento de sus Datos Personales.
- Comisión Europea (2001) Reglamento (CE) Nº 1049/2001 del Parlamento Europeo y del Consejo.
- Declaración Universal de Derechos Humanos (1948), art. 12.
- Declaración Americana de Derechos y Deberes del Hombre (1948), art. 5,9 y10.
- Ecuador (2004) Ley Orgánica de Transparencia y Acceso a la Información Pública.
- El Salvador (2011) Decreto No. 534Ley De Acceso a la Información Pública.
- Guatemala (2008) Ley De Acceso a la Información Pública.
- Jamaica (2002) Ley Nº 21-2002 The Acces to Information Act.
- Honduras (2006) Ley De Transparencia y Acceso a la Información Pública.
- México (2003) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Nicaragua (2007) Ley Nº 621 Ley de Acceso a La Información Pública.
- Nicaragua (2012) Ley de Protección de Datos Personales.
- Pacto Internacional de Derechos Civiles y Políticos (1966), art. 17.
- Panamá (2002) Ley N° 6 de 2002 Que dicta Normas para la Transparencia en la Gestión Pública, establece la acción de Hábeas Data y dicta otras disposiciones.

- República Dominicana (2004) Ley Nº 200-04 General de Libre Acceso a la Información Pública.
- República Dominicana (2005) Decreto Reglamento Nº 103-05 De La Ley General De Libre Acceso A La Información Pública.
- Perú (2002) Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública
- Perú (2011) Ley Nº 29733Ley de Protección de Datos Personales.
- Paraguay (2001) Ley Nº 1.682/01 “Ley que reglamenta la información de carácter privado”
- Parlamento europeo (1995) 95/46/CE del Parlamento Europeo y del Consejo.
- Uruguay (2008) Ley Nº 18.381 Derecho de Acceso a la Información Pública.
-Uruguay (2008) Ley Nº 18.331 Protección de Datos Personales y Acción de "Habeas Data".

Jurisprudencia

- Corte Interamericana de Derechos Humanos (2006), Caso Claude Reyes y otros Vs. Chile (Fondo, Reparaciones y Costas).
- Tribunal de Justicia de la Unión Europea (Gran Sala) (2010) caso: C-28/08.
- Tribunal de Justicia de la Unión Europea (Gran Sala) (2010) casos unidos: C-92/09 y C-93/09.

Caso de estudio: Argentina

Preparado por Natalia Torres,
Investigadora Principal del CELE[31]

Introducción

El presente estudio apunta a describir el diseño institucional de las agencias encargadas de garantizar el derecho a saber y la protección de datos personales en la Argentina. Para llevar a cabo esta tarea se trabajó con una metodología cualitativa que recogió información a partir de relevamiento bibliográfico y documental y a través de entrevistas a expertos en estos temas. El estudio fue realizado durante 2012.

1. Relevamiento normativo

Argentina reguló la protección de datos personales a través de la Ley 25326 en octubre del 2000. Este reconocimiento del valor de los datos personales no tiene contrapartida semejante en el ámbito de la información pública ya que nuestro país no posee una ley nacional de acceso a la información pública. Sí, en cambio, posee un decreto que regula el derecho en el ámbito exclusivo del Poder Ejecutivo Nacional, emitido en 2003. En esta sección presentaremos en primer lugar, la normativa existente sobre el derecho de acceso a la información, el contexto de surgimiento, sus objetivos, finalidades y principios. Luego presentaremos la ley nacional de protección de datos personales, dando cuenta de su contexto de surgimiento y sus principales contenidos. A continuación daremos cuenta de las posibilidades de articulación entre ambas normativas considerando que fueron elaboradas de manera autónoma, sin especial referencia entre ellas.

1.1 Legislación sobre derecho de acceso a la información pública

La historia del reconocimiento del derecho a saber es una historia de frustraciones. En esta última década, el Congreso de la Nación debatió diversos proyectos de ley para regular el acceso a la información pública sin arribar a la sanción definitiva. Sin embargo, si vamos a relatar esta historia, debemos comenzar por el principio. La Constitución Nacional reconoce el derecho a acceder a la información pública en los artículos 1, 33, 41 y 42. El argumento que sostiene este reconocimiento es sencillo: si nuestra forma de gobierno es democrática y representativa, nosotros, los representados, tenemos derecho a saber qué se hace en nuestro nombre. A este puntapié fundacional debe agregarse otro capítulo auspicioso en la historia del reconocimiento del derecho a saber: la incorporación en la reforma constitucional de 1994 de los tratados internacionales que reconocen el derecho a la información como derecho humano. El artículo 75, inciso 22 incluye tratados internacionales que regulan de manera explícita el derecho a saber[32].

Ahora bien, la inclusión de los tratados internacionales fue un paso fundamental en la historia del reconocimiento del derecho pero no suficiente para garantizar la implementación de políticas públicas sobre información pública y el ejercicio efectivo del derecho a saber. En línea con ciertos desarrollos y experiencias internacionales en la materia[33], se empezó a percibir la necesidad de avanzar en la sanción de una ley que permitiera regular de manera clara cómo solicitar información y cómo proveerla. Esto se dio en el contexto de la mayor crisis política e institucional de la historia reciente del país, que culminó en el 2001 con la renuncia del entonces Presidente de la Nación, Dr. Fernando De la Rúa, y con una traspaso vertiginoso de siete presidentes en una semana. Durante la presidencia de De la Rúa, un grupo de funcionarios impulsó desde la -entonces flamante- Oficina Anticorrupción, un proceso de elaboración participada de normas[34]para desarrollar un proyecto de ley de acceso a la información. El proyecto consensuado tras un año de deliberaciones con diferentes sectores, fue enviado para su análisis por el Congreso de la Nación a principio de 2002 por el Presidente Provisional Dr. Eduardo Duhalde. En paralelo a estos desarrollos, la Mesa de Diálogo convocada por Naciones Unidas y la Iglesia Católica[35] de la que participaban diferentes organizaciones sociales promovieron las denominadas "Leyes de mayo", un conjunto de propuestas normativas que apuntaban a recomponer el vínculo con la ciudadanía y a mejorar la calidad institucional. Entre esas regulaciones se

[31] Este trabajo fue realizado con la colaboración de Laura Cirulnik, Asistente de Investigación del CELE.
[32] El Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos establece que el derecho a la libertad de expresión comprende la libertad de buscar, recibir y difundir información. El Artículo IV Declaración Americana de los Derechos y Deberes del Hombre reconoce que cada persona tiene el derecho a la libertad de investigación, de opinión, y de expresión y difusión del pensamiento por cualquier medio. El Artículo 13 de la Convención Interamericana de Derechos Humanos también protege el derecho y la libertad de buscar, recibir, y difundir informaciones e ideas de toda índole.
[33] Durante las últimas décadas asistimos a una serie de "oleadas" de avances sobre el reconocimiento normativo del derecho a saber. El resultado de estos fenómenos se refleja en los países que hoy cuentan con leyes que regulan el acceso a la información pública http://right2info.org/access-to-information-laws
[34] http://www.anticorrupcion.gov.ar/Documentos%5CLibro%20Elab%20Partic%20-%202ed.pdf
[35] http://www.presidenciaduhalde.com.ar/system/contenido.php?id_cat=37

encontraba el proyecto de ley de acceso a la información[36]. El contexto no podía ser mejor: la ley de acceso a la información venía a dar una respuesta concreta para canalizar el descontento social; México avanzaba en la sanción de una ley de transparencia que marcaría el ritmo y el contenido de las discusiones de la región; las organizaciones de la sociedad civil se organizaban y trabajan fuertemente en el ámbito legislativo. Hubimos *momentum*.

En 2003, en concordancia con este clima, la Cámara de Diputados de la Nación dio media sanción[37] al proyecto elaborado por la Oficina Anticorrupción y lo remitió para su remisión al Senado. Allí, el proyecto sufrió modificaciones que alteraron sustantivamente su espíritu. Esta versión fue aprobada por el Senado en 2004 y terminó en una encrucijada: los diputados podían aceptar los cambios de esta nueva versión del proyecto; o insistir con su propia versión para lo que necesitaban una mayoría especial y partir al bloque oficialista que había impulsado los cambios. El resultado es bastante conocido: el proyecto perdió su estado parlamentario y Argentina se quedó sin ley de acceso a la información[38].

Recién en 2010 volvió el Congreso a analizar el tema. Los cambios en la composición de las cámaras con posterioridad a las elecciones legislativas del 2009 llegaron con promesas de la oposición a impulsar algunas agendas rezagadas. Así, a principios de 2010, en un hecho –al menos- inusual para la vida parlamentaria, dos comisiones –una en el Senado y otra en Diputados- se disputaron por el liderazgo del debate. En ambas comisiones, participaron las organizaciones de la sociedad civil, aportando su perspectiva para enriquecer y mejorar los proyectos[39].El Senado dio finalmente el puntapié inicial y dio media sanción[40] a un proyecto que pasó para su revisión en la Cámara de Diputados. El interés de la Comisión en la cámara baja por liderar el tema pareció entonces haberse esfumado en tanto el proyecto remitido por el Senado nunca fue analizado por los diputados de la nación. Así, dos capítulos de frustraciones en el ámbito legislativo, dos versiones diferentes con el mismo resultado[41]. El proyecto perdió estado parlamentario a fines de 2012[42].

Hasta aquí la sucesión de desilusiones parlamentarias que llevaron a que la Argentina no tenga una ley nacional de acceso a la información pública. Sin embargo, tanto a nivel provincial como a nivel del Ejecutivo Nacional se registraron avances significativos. En el ámbito provincial, algunas provincias regularon el derecho a saber incluso antes de los debates en el Congreso Nacional. Ese es el caso de la Provincia de Chubut y de la Ciudad Autónoma de Buenos Aires que aprobaron legislaciones en 1992 y 1998 respectivamente. Luego se sumaron otros distritos provinciales: Buenos Aires, Catamarca, Chaco, Córdoba, Corrientes, Entre Ríos, Jujuy, La Pampa, Misiones, Rio Negro, Salta, Santa Fe, Santiago del Estero y Tierra del Fuego[43]. A estos desarrollos legislativos provinciales deben incluirse los que se realizaron a nivel de gobiernos locales[44].

En 2003, el entonces Presidente de la Nación, Dr. Néstor Kirchner, emitió el Decreto 1172/03[45] que regula –entre otras cosas[46]- el derecho a saber en el ámbito del Poder Ejecutivo Nacional. El decreto recoge de manera casi lineal el contenido del proyecto elaborado por la Oficina Anticorrupción y que fuera enviado al Congreso Nacional. Es un texto sencillo que respeta estándares internacionales en la materia.

El objeto del Reglamento de Acceso a la Información Pública "…es regular el mecanismo de Acceso a la Información Pública, estableciendo el marco general para su desenvolvimiento" (Artículo 1) garantizando el respeto de los principios de igualdad, publicidad, celeridad, informalidad y gratuidad (Artículo 7). Su finalidad, de acuerdo a su artículo 4, "…es permitir y promover una efectiva participación ciudadana, a través de la provisión de información completa, adecuada, oportuna y veraz". El reglamento describe al acceso a la información como "…una instancia de participación ciudadana por la cual toda persona ejercita su derecho a requerir, consultar y recibir información" y define a la información pública como "toda constancia en documentos escritos, fotográficos, grabaciones, soporte magnético, digital o en cualquier otro formato y que haya sido creada u obtenida por los sujetos mencionados en el artículo 2º o que obre en su poder o bajo su control, o cuya producción haya sido financiada total o parcialmente por el erario público, o que sirva de base para una decisión de naturaleza administrativa, incluyendo las actas de las reuniones oficiales".

---

[36] http://www.lanacion.com.ar/442532-las-ong-impulsan-un-plan-para-atacar-la-corrupcion

[37] El texto del proyecto aprobado puede consultarse acá http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=CD&tipo=PL&numexp=16/03&nro_comision=&tConsulta=3

[38] Para conocer el trámite parlamentario del proyecto puede accederse acá http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=CD&tipo=PL&numexp=16/03&nro_comision=&tConsulta=2.

[39] El CELE participó activamente del debate en la Comisión de Asuntos Constitucionales en el Senado de la Nación. Ver notas en http://www.palermo.edu/cele/pdf/Presentacion-senado.pdf http://www.palermo.edu/cele/noticias/ley-de-acceso-a-la-informacion.html http://www.palermo.edu/cele/noticias/proyectos-debate-en-el-senado.html

[40] Sobre este punto ver http://www.freedominfo.org/2010/10/argentine-senate-passes-access-to-information-bill/

[41] Para conocer más sobre esto puede consultarse a tale of two Chambers http://www.freedominfo.org/2011/01/argentines-access-to-information-law-a-tale-of-two-chambers/

[42] Este punto fue debatido y aún hoy quedan dudas sobre la vigencia del proyecto.

[43] Para conocer la legislación provincial visitar http://blogs.lanacion.com.ar/data/category/acceso-a-la-informacion-2/

[44] Para conocer la legislación municipal visitar http://blogs.lanacion.com.ar/data/acceso-a-la-informacion-2/el-derecho-de-acceso-a-la-informacion-en-argentina-un-mapa/

[45] http://www.infoleg.gov.ar/infolegInternet/anexos/90000-94999/90763/norma.htm

[46] El decreto reglamenta los mecanismos de audiencias públicas, gestión de intereses, elaboración participada de normas y reuniones abiertas de entes reguladores.

El decreto le otorga a "toda persona física o jurídica, pública o privada" el derecho "a solicitar, acceder y recibir información, no siendo necesario acreditar derecho subjetivo, interés legítimo ni contar con patrocinio letrado".

De acuerdo a su artículo 2, los sujetos pasivos alcanzados por esta normativa son aquellos comprendidos exclusivamente al ámbito del Poder Ejecutivo Nacional: "El presente Reglamento General es de aplicación en el ámbito de los organismos, entidades, empresas, sociedades, dependencias y todo otro ente que funcione bajo la jurisdicción del Poder Ejecutivo Nacional. Las disposiciones del presente son aplicables asimismo a las organizaciones privadas a las que se hayan otorgado subsidios o aportes provenientes del sector público nacional, así como a las instituciones o fondos cuya administración, guarda o conservación esté a cargo del Estado Nacional a través de sus jurisdicciones o entidades y a las empresas privadas a quienes se les hayan otorgado mediante permiso, licencia, concesión o cualquier otra forma contractual, la prestación de un servicio público o la explotación de un bien del dominio público".

1.2 Legislación sobre protección de datos personales

La Constitución Nacional regula la acción de habeas data en el artículo 43, inciso 1 y 3:
"Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.
Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".

La mención del tema en la carta magna obedece a la inclusión realizada en la reforma constitucional del ´94. Es por eso que, al arrancar el debate parlamentario en la Cámara de Senadores de la Nación para regular la protección de los datos personales, el Senador Eduardo Menem recordaba: "Se trata del proyecto por el que se reglamenta la institución del hábeas data. Resalto la importancia del tema por cuanto se trata de la reglamentación de una garantía, de un derecho fundamental consagrado por la Constitución Nacional en su reforma de 1994. Es decir que se trata de una de las leyes denominadas "de mandato constitucional", porque se trata de implementar la vigencia de un derecho"[47].

El reconocimiento del derecho de habeas data y la protección de datos personales apareció entonces –al igual que con el tema de la información pública que analizamos posteriormente- con la reforma constitucional del ´94. Sin embargo, la protección de los datos personales, a diferencia de lo ocurrido con el derecho a saber, tuvo su tratamiento legislativo a poco tiempo de realizada la reforma. Cabe especular que esto se dio de esta manera en tanto que la mención del derecho es más explícita en el nuevo texto constitucional y que, por lo tanto, había sido objeto de debate en la asamblea constituyente del ´94. Es más, si analizamos los protagonistas de la discusión parlamentaria de la ley nacional de protección de datos personales encontramos que gran parte de ellos había participado en la asamblea legislativa encargada de reformar la constitución nacional.

Los primeros proyectos que se registran en materia de regulación de protección de datos personales datan de 1996 y fueron presentados por los senadores Menem, López y Berhongaray. La cámara alta aprobó el 23 de octubre de 1996 el primer proyecto sobre el tema que se convirtió en la ley 24.745 y que fue luego vetada por el Poder Ejecutivo de la Nación en diciembre de 1996 a través del Decreto 1616/96[48]. De acuerdo al veto, la ley creaba una Comisión Bicameral de Seguimiento de Protección Legislativa de Datos con el fin de salvaguardar los datos personales. El problema, de acuerdo al veto, era la ausencia de especificación o delimitación de las funciones de la comisión que "…devienen de tal amplitud que vulneran la distribución constitucional de incumbencias estatales dado que en nuestro sistema legal el único poder con atribuciones para resolver sobre la protección de los derechos de los individuos es el Poder judicial de la Nación" (Decreto 1616/1996).

En ocasión del debate parlamentario del 1998, el Senador Menem explicaba lo ocurrido entonces: "Pero ocurre, señor presidente, que ya hemos considerado en esta Cámara un proyecto de ley sobre este tema. (…) El proyecto de ley fue girado al Poder Ejecutivo y finalmente vetado. (…) Ahora bien, ¿cuáles fueron las razones por las que el Poder Ejecutivo vetó este proyecto de ley? El Poder Ejecutivo vetó este proyecto de ley por entender, en primer término, que la norma invadía atribuciones que le eran propias; en segundo lugar, por la amplitud de facultades de la Comisión Bicameral establecida como órgano de control; en tercer término, por la posibilidad del dictado de códigos deontológicos sin intervención de la autoridad de control; y, finalmente, por cuestiones atinentes al flujo

[47] Para consultar la versión taquigráfica del debate en el Senado de la Nación puede accederse a este sitio http://www.senado.gov.ar/web/taqui/taqui_op_adjunto.php?clave=F31013/041000.htm#6
[48] Ni la ley ni el decreto del veto son accesibles online. Ambos textos se encuentran incluidos en Pierine 23

transfronterizo de datos, en los supuestos de cooperación internacional"[49]. Como vemos, la definición del órgano de control estuvo desde el inicio en el centro de las discusiones parlamentarias. La Dra. Carrió, en el análisis del proyecto en el debate en la Cámara de Diputados de la Nación, explicaba el veto de esta manera: "En su momento la Cámara de Diputados sancionó un proyecto de ley sobre hábeas data que fue modificado por el Senado. Posteriormente la Cámara de Diputados insistió en su sanción y luego fue vetada por el Poder Ejecutivo Nacional, con fuertes presiones provenientes de distintos lobbies que pretendían garantizar el mercado en desmérito de la integridad y protección de las personas"[50].

Menem, López y Berhongaray serán nuevamente protagonistas del tema en 1998, año en el que reintrodujeron sus proyectos en el Senado de la Nación. A estos proyectos se sumaron las iniciativas legislativas de los senadores Del Piero, Branda, Romero Ferisy Villaverde[51]. Es recién entonces, en 1998, que se reinició el debate parlamentario en la cámara alta. El proyecto obtuvo media sanción y fue remitido para su análisis a la Cámara de Diputados. La cámara baja modificó y aprobó el proyecto en 2000 y lo reenvió para su revisión al Senado. Los senadores insistieron parcialmente en la versión aprobada en la media sanción y lo enviaron para su promulgación al Poder Ejecutivo que observó parcialmente la ley en un punto clave: la constitución del órgano de control. El Senado insistió ese mismo año en su versión pero la insistencia caducó en 2002 por la falta de tratamiento en la Cámara de Diputados. Esa es, en brevísimo, la historia de la aprobación de la Ley 25326 de Protección de Datos Personales.

Más allá de las idas y vueltas, las sanciones y los vetos, el carácter polémico de la iniciativa no pareciera que hubiera generado en el momento un interés crucial en los legisladores, algo que se reflejó en los pocos asistentes al debate parlamentario en la cámara alta[52].

Ley 25326 de Protección de Datos Personales
Objeto, finalidad, sujetos y definiciones conceptuales. Principios

La ley tiene como objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional" (Ley 25326, Artículo 1).

En su artículo 2, la ley presenta una serie de definiciones conceptuales:
"— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
— Archivo, registro, base o banco 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.
— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general

[49] Para consultar la versión taquigráfica del debate en el Senado de la Nación puede accederse a este sitio http://www.senado.gov.ar/web/taqui/taqui_op_adjunto.php?clave=F31013/041000.htm#6
[50] Para consultar la versión taquigráfica del debate en la cámara baja se puede acceder a este sitio http://www.protecciondedatos.com.ar/debatedip.htm
[51] Los proyectos pueden consultarse acá:
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=606/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1042/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=577/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1094/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=684/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1537/98&nro_comision=&tConsulta=3
http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1582/98&nro_comision=&tConsulta=3
[52] Sobre el tema debatían los legisladores:
"Sr. VILLARROEL.- Señor presidente: para alivio de los pocos colegas que están asistiendo esta tarde al debate...
Sr. BRANDA.- ¡Somos pocos, pero cada uno vale por diez!
Sr. VILLARROEL.-...desde ya anuncio que no pretendo ni intento asestarles un discurso.
En realidad, un discurso estaría de más, pero no me refiero al hecho de la escasa asistencia sino a que, en esta oportunidad, lo único que toca decir y fundar es cuál va a ser el sentido del voto en general, que es la cuestión que se está tratando ahora. Comparto, en alguna medida, la suerte de lamento del señor senador por La Rioja, miembro informante del dictamen de mayoría, en cuanto a la escasa concurrencia. Pero también debo decir, para su consuelo y el de todos nosotros, que respecto de este proyecto sobre hábeas data, como contrapartida, está el hecho documentado -a través de los numerosos dictámenes con disidencias parciales y con proyectos propios de algunos señores senadores- de que muchos colegas se han interesado en este asunto. Y se han interesado no de manera episódica sino con trabajos fecundos, lo cual es importante."

el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable".

El Capítulo II de la ley establece una serie de principios para la protección de datos considerando su licitud, la calidad de los datos, las condiciones que deben cumplirse en la recopilación, tratamiento y cesión de los datos (información, seguridad, consentimiento), el tratamiento de los datos en función del tipo de dato (categorías de datos) y los temas que deben contemplarse en los casos de transferencia internacional.

El Capítulo III es quizás el que más se vincula con la regulación del artículo 43 de la Constitución Nacional en tanto regula los derechos de los titulares de los datos a informarse y acceder a la información sobre datos personales que existan en base de datos públicos o privados. Asimismo, el capítulo regula el derecho a rectificar, actualizar o suprimir datos personales, cuando corresponda.

El Capítulo IV establece una serie de obligaciones para los usuarios y responsables de archivos, registros y bancos de datos. Principalmente, quienes tengan este tipo de archivos y registros deberán registrarlos.

La ley 25326 cuenta con 14 reglamentaciones y 19 actualizaciones que son incluidas en la sección bibliográfica de este documento.

Más allá de la regulación de la protección de los datos personales en la Ley Nacional 25326, algunas constituciones provinciales han reconocido el derecho y/o sancionado legislaciones específicas sobre el tema. La situación federal es descripta por Pucinelli: "…mientras que algunos estados federados consideraron en sus constituciones solo un aspecto de la protección de datos de carácter personal ocupándose de los antecedentes policiales y penales (La Rioja, Salta y San Juan), o de establecer el derecho de acceso a las fuentes de información (Catamarca y Formosa, además de Río Negro y San Luis, que por otra parte también regularon el hábeas data como acción específica de garantía (Buenos Aires, Ciudad Autónoma de Buenos Aires, Córdoba, Chaco, Chubut, La Rioja, Jujuy, Río Negro, San Luis, San Juan, Santiago del Estero y Tierra del Fuego)" (Pucinelli, 2004: 67).

2. Diseño institucional

En un trabajo anterior (Torres, 2009) se analizó la relevancia de la teoría positiva de las instituciones (Majone, 1996) y la teoría de la política estructural (Moe, 1989) para explicar los procesos delegativos y sus correlatos institucionales. Allí se afirma que "The positive theory of institutions has focused on the study of two concepts: delegation and its reverse side, political control (Majone, 1996). When authority is delegated principals need to control if agencies are accomplishing their goals and following the enacting coalition´s interests. Structural politics (Moe, 1989) describes the process of creating a bureaucratic structure to isolate agencies from political interference and to protect it from political uncertainty (Moe, 1989). By bureaucratic structure Moe understands the rules for decision-making, the incentives established to reward or sanction public officers, and the oversight mechanisms to control them (Moe, 1989). This structure, along with scope of delegation and agency´s governance structure, is defined by principals according to the institutional features available in the legislative choice (Horn, 1995)" (Torres, 2008).

Así, la teoría de la política estructural explica lo que ocurrió en la sanción de la ley nacional de protección de datos personales, en donde una porción muy importante del debate se centró en la forma y entidad que adquiriría el órgano de control y en tipo de dirección que finalmente fue establecida; y explica también lo que pasó con la frustrada sanción de una ley de acceso a la información, donde el Congreso falló en garantizar el derecho a saber, y en donde el decreto que regula el tema en el Poder Ejecutivo Nacional establece como autoridad de aplicación a una subsecretaría, sin recursos, sin capacidades para hacer valer sus recomendaciones que se encuentra totalmente expuesta a la influencia política.

Ahora bien, hace falta aquí hacer explícito un argumento que subyace a este análisis: la convicción de que la delegación del control de la gestión de la información pública o la protección de los datos personales debe depositarse en órganos autónomos. Otra aclaración, en este trabajo entendemos la autonomía organizacional en línea a las teorías de Majone, Demarigny, Carpenter y Wilson:" Majone (1996) y Demarigny (en Majone, 1996) definen una agencia como independiente si se opera fuera de la jerarquía administrativa, si sus autoridades no

pueden ser eliminados por desacuerdo con la política presidencial, si es creado por y sus programas se definen a través de "leyes aprobadas por el Congreso," y si su independencia está garantizada por normas claras sobre su composición. Basado en un enfoque socio-administrativo, Carpenter (2001) identifica tres condiciones para la autonomía: la diferenciación política, la capacidad de organización propia, y la propia legitimidad política. Wilson (1989) distingue dos características que podrían mejorar la independencia: externo - relacionada con una jurisdicción formalmente definida - y aspectos internos - relacionados con la cultura de la organización que distingue a una agencia. Por lo tanto, la autonomía se entiende "... como una condición de independencia suficiente para permitir a un grupo para elaborar y mantener una identidad propia" (Wilson, 1989:182)" (Torres, 2008:25)

Esta investigación se apoya en la convicción de que la regulación del acceso a la información implica crear mecanismos para controlar las decisiones políticas en relación a la publicación y reserva de información pública. Lo mismo en relación a la protección de los datos personales: el Estado es la base de datos más extensa y amplia. Cuidar a los ciudadanos de una gestión indebida de esa información supone conformar organismos públicos que aseguren la credibilidad institucional y protejan a los ciudadanos de cualquier abuso.

En los próximos apartados presentamos los diseños institucionales que fueron creados en el ámbito nacional para implementar el decreto de acceso a la información y la ley nacional de datos personales.

2.1 Diseño institucional para la implementación de la regulación de acceso a la información: Subsecretaría para la Reforma Institucional y el Fortalecimiento de la Democracia

En esta sección analizaremos las principales características de la Subsecretaría para la Reforma Institucional y el Fortalecimiento de la Democracia dependiente de la Jefatura de Gabinete de Ministros del Poder Ejecutivo Nacional, organismo establecido por el Decreto 1173/03 para implementar el Reglamento de Acceso a la Información Pública. Vale la pena aclarar que el equipo de investigación intentó sin éxito entrevistar a las autoridades del organismo y que por ese motivo se carece de testimonios de la agencia. Gran parte de la información aquí presentada es tomada de un trabajo previo (Torres, 2009). En tanto los datos referidos fueron recolectados en 2008 carecen de actualidad pero pueden servir de referencia inicial para el estudio.

2.1.1 Aspectos externos

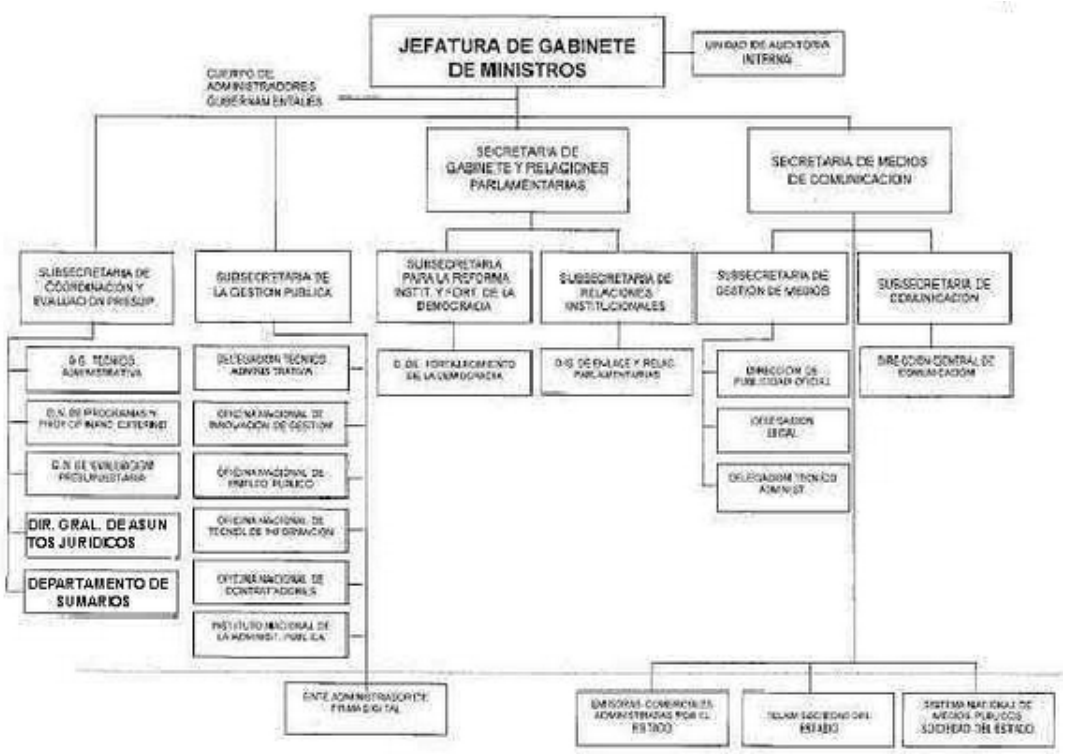
Tipo de legislación que crea la agencia, posición de la agencia en el organigrama y cobertura territorial. Como mencionamos anteriormente, en diciembre del 2003, el Presidente Néstor Kirchner emitió el Decreto 1172/03 que regula el acceso a la información dentro del Poder Ejecutivo. Éste decreto establece en su artículo 18 la autoridad de aplicación a cargo de llevar a la práctica los contenidos del Reglamento de Acceso a la Información Pública: "La Autoridad de Aplicación del presente Reglamento es la SUBSECRETARIA PARA LA REFORMA INSTITUCIONAL Y FORTALECIMIENTO DE LA DEMOCRACIA de la JEFATURA DE GABINETE DE MINISTROS (SRIyFD), quien tendrá a su cargo verificar y exigir el cumplimiento de las obligaciones establecidas en el mismo". El mismo decreto establece también a la Oficina Anticorrupción (OA) como el organismo "…encargado de recibir, formular e informar a las autoridades responsables, las denuncias que se formulen en relación con el incumplimiento del presente régimen". En este apartado nos focalizaremos en la SRIyFD en tanto es ella la que debe realizar políticas para hacer efectivo el texto de la ley. En la sección dedicada a los mecanismos para resolver controversias, analizaremos el rol desempeñado por la OA.

Ahora bien, esta mención en el decreto no es la que crea o constituye la agencia. La Subsecretaría surge de una re-estructuración realizada en la Jefatura de Gabinete Ministros (JGM) formalizada en el Decreto 78/02[53]. Este decreto fue posteriormente revocado por el Decreto 624/03[54], que ordenó una nueva estructura organizativa de la JGM. Esta regulación puso a la SRIyFD en el ámbito de la JGM, como dependiente de la Secretaría de Gabinete y Relaciones Parlamentarias. Los objetivos de la SRIyFD de acuerdo a esa normativa son:
"…1. Fortalecer la relación entre el Estado y la Sociedad Civil a fin de proponer las reformas institucionales necesarias para desarrollar una democracia gobernable, transparente, legítima y eficiente.
2. Proponer los lineamientos básicos y propuestas de modificación de los sistemas electorales nacionales, de la organización y funcionamiento de los partidos políticos y de su financiamiento.
3. Promover la implementación de los mecanismos de democracia directa y de democracia participativa contemplados en la Constitución Nacional.
4. Participar, en coordinación con el Ministerio del Interior, en la elaboración de instrumentos eficaces de control ciudadano en las distintas etapas del proceso electoral.
5. Participar con el Ministerio del Interior en la asistencia a los Estados Provinciales en la formulación de proyectos sobre organización de partidos, sistemas electorales y mecanismos de democracia directa y de democracia participativa."

[53] http://www.infoleg.gov.ar/infolegInternet/anexos/70000-74999/71657/norma.htm
[54] http://www.infoleg.gov.ar/infolegInternet/anexos/85000-89999/87826/texact.htm

El decreto 1172/03 viene entonces a agregarle una función extra, como resultado de la decisión de presidencial de avanzar en la implementación de una política de información y de la iniciativa de la Dra. Marta Oyhanarte, Subsecretaria en funciones en ese momento, que transformó ese espacio institucional.

La posición de la SRIyFD en el organigrama puede ser representada de la siguiente manera:



Organigrama extraído del Decreto 624/03

De acuerdo a la posición de la SRIyFD, un ex funcionario de esa dependencia consideraba: "…si pensamos en un organismo externo, la creación de una agencia por fuera del Poder Ejecutivo debe tener una ley. El punto es si se podría hacer con un decreto. En este contexto pienso que el mejor espacio organizacional para poner una autoridad de aplicación es la JGM debido a que facilita una política transversal" (Torres, 2009). Otra funcionaria opinaba: "…evidentemente en una situación ideal la autoridad de aplicación debe ser como la que hay en México. Un organismo independiente mejora el cumplimiento con la regulación. De todas formas, nuestra actividad como autoridad de aplicación es cada vez más reconocida y respetada" (Torres, 2009).

Si consideramos que la normativa que regula el derecho a saber es un decreto y que rige para todo el ejecutivo nacional, la ubicación en el ámbito de la Jefatura de Gabinete de Ministros es una buena opción. El problema es, como veremos más adelante, la dependencia funcional de ésta para desarrollar sus tareas ordinarias y la falta de blindaje político para la designación de autoridades. Es decir, la Subsecretaría no se encuentra limitada para desarrollar políticas de información para todo el ejecutivo nacional por el lugar en donde se encuentra ubicada. Se encuentra limitada para garantizarle a la ciudadanía el acceso efectivo a la información pública por su dependencia institucional y política. Este punto requiere un análisis más detenido. Nada de malo tiene que el Poder Ejecutivo tenga su propia área para la implementación de las políticas de información. El problema aparece cuando esta área debe resolver controversias entre particulares y el propio ejecutivo. Es por eso que generalmente –en la experiencia internacional- se posiciona la instancia de resolución de controversias en espacios dotados de autonomía y blindados de potenciales interferencias políticas[55].

Atribuciones

Las atribuciones otorgadas por el Decreto 624/03 tienen relaciones indirectas o mediatas con la promoción del derecho a saber:

> "1. Fortalecer la relación entre el Estado y la Sociedad Civil a fin de proponer las reformas institucionales necesarias para desarrollar una democracia gobernable, transparente, legítima y eficiente.

[55] Sobre este tema puede consultarse la Guía Modelo para la Implementación de la Ley de Acceso a la Información de la OEA.

2. Proponer los lineamientos básicos y propuestas de modificación de los sistemas electorales nacionales, de la organización y funcionamiento de los partidos políticos y de su financiamiento.
3. Promover la implementación de los mecanismos de democracia directa y de democracia participativa contemplados en la Constitución Nacional.
4. Participar, en coordinación con el Ministerio del Interior, en la elaboración de instrumentos eficaces de control ciudadano en las distintas etapas del proceso electoral.
5. Participar con el Ministerio del Interior en la asistencia a los Estados Provinciales en la formulación de proyectos sobre organización de partidos, sistemas electorales y mecanismos de democracia directa y de democracia participativa" (Decreto 624/03).

Unos meses después, el Decreto 1172/03 le asignó a la Subsecretaria lo que constituiría el centro de su labor en la primera etapa de su conformación, entiéndase por esta la que se encuentra marcada por la gestión de la Dra. Oyhanarte que arranca en junio 2003 y culmina con su renuncia en 2009.Vale aclarar que si bien el decreto constituye a la SRyFD como autoridad de aplicación, el texto no establece una descripción minuciosa de las atribuciones a su cargo, solamente establece que la subsecretaría "...tendrá a su cargo verificar y exigir el cumplimiento de las obligaciones establecidas en el mismo" (Decreto 1172/03)

En 2011 se llevó a cabo una nueva re-estructuración de la Jefatura de Gabinete. En esa ocasión, el Decreto 22/11 establece que la SRIyFD ya no dependería de la Secretaría de Relaciones Parlamentarias sino de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la Jefatura de Gabinete.

Mucho se ha dicho de las transformaciones ocurridas en la SRIyFD desde que la Dra. Oyhanarte renunciara a su cargo al frente del organismo, principalmente en relación a la falta de cumplimiento de la atribución establecida por el Decreto 1172/03 con posterioridad a su partida, pero poco se ha dicho del cumplimiento de esta Subsecretaría de los mandatos establecidos en su decreto de conformación. No constan, por ejemplo y al menos en esta primera etapa de funcionamiento de la SRIyFD, actividades realizadas en coordinación con el Ministerio de Interior para el mejoramiento del control ciudadano en el proceso electoral. Es decir, el cambio de orientación de la Subsecretaría a partir de la sanción del Decreto 1172/03 puso en segundo lugar las atribuciones por las que fue creado el organismo. Al mismo tiempo, poca información tenemos del cumplimiento de estas atribuciones y las del decreto 1172/03. Tal como lo señalamos con anterioridad, el equipo de investigación no logró entrevistarse con los responsables del organismo.

Existencia de organizaciones rivales

Uno de los primeros conflictos que surgieron del texto del decreto 1172/03 era la ambigüedad en cuanto a la atribución de la Subsecretaría de resolver controversias, ya que, como vimos con anterioridad, el decreto le otorgaba a la Oficina Anticorrupción la potestad de "…recibir, formular e informar a las autoridades responsables, las denuncias que se formulen en relación con el incumplimiento del presente régimen" (Decreto 1172/03). Esta ambigüedad se resolvió recién 2008, cuando finalmente ambas organizaciones crearon un procedimiento específico para tramitar las controversias. El mecanismo fue elaborado de manera coordinada entre ambas agencias y con la participación de organizaciones de la sociedad civil. El resultado de ese trabajo es la Resolución Conjunta de la Secretaría de Gabinete y Relaciones Parlamentarias y la Fiscalía de Control Administrativo 1/2008 y 3/2008[56].

2.1.2 Aspectos internos
Capacidad organizativa
Presupuesto

La SRIyFD no tiene autonomía presupuestaria y tampoco tiene su propio SAF, el sistema administrativo financiero para gestionar las asignaciones presupuestarias en las agencias públicas argentinas. La consecuencia de esta ausencia es la imposibilidad de la subsecretaría para gestionar sus propios fondos sin la intervención de su superior. También esta ausencia impide conocer la asignación presupuestaria específica destinada a la entidad ya que el presupuesto nacional no desagrega los datos a este nivel de sub-jurisdicción.

Sólo para dar algunos indicios sobre el presupuesto de la agencia, un funcionario nos informó que para el año 2008 la Subsecretaría contaba con un presupuesto aproximado de AR $ 271400 (Torres, 2008).

Personal

No contamos con información sobre la dotación de personal de la SRIyFD. Para 2008 y de acuerdo con la información brindada por un funcionario entonces, la SRIyFD contaba sólo con nueve empleados abocados a implementar la política de acceso a la información (Torres, 2008).

[56] http://www.anticorrupcion.gov.ar/documentos_relacionados/SGRP%201-08%20y%20FCA%203-08.pdf

Diferenciación política

Reglas para designación y remoción de autoridades y duración del mandato
El decreto no establece ningún procedimiento especial para nombrar a los altos cargos dentro de la autoridad de aplicación. La designación de funcionarios se basa en las reglas generales con las que se rige la administración pública. Esta ausencia de reglas para la designación y remoción deja desprotegida a la subsecretaría de posibles interferencias políticas.

La Dra. Marta Oyhanarte fue designada como Subsecretaria para la Reforma Institucional y el Fortalecimiento de la Democracia mediante el Decreto 289/03[57]. En la designación no se hace referencia a sus antecedentes ni a ningún requisito que deba cumplirse para cubrirse el cargo. Esto no es una falta, sencillamente el cargo no requiere del cumplimiento de requisitos para ocuparlo.

En la investigación previamente mencionada, los funcionarios a cargo del organismo en 2008 afirmaban que la ausencia de reglas para designación y remoción tenía poca relevancia y que no afectaba la independencia de la subsecretaría para garantizar el ejercicio del derecho a saber por parte de la ciudadanía: "La SRIyFD tiene su propio estilo dentro de la administración, probablemente debido a su objetivo de fortalecer la relación entre el Estado y la sociedad. Este aspecto se expresa en cada acción: desde la forma en que contrata personal hasta su compromiso de trabajar en colaboración con los organismos regulados "(Torres, 2009). Coincidentemente, Oyhanarte expresaba en el mismo estudio "Tenemos un estilo distintivo, probablemente debido a que se promovió una dinámica colectiva entre nosotros " (Torres, 2009).

Tiempo después de su renuncia, efectivizada por la Resolución del Jefe de Gabinete de Ministros 358/2009[58] que acepta la dimisión de la Dra. Oyhanarte, esa opinión cambiaría. En una carta que publicara en su blog personal entonces afirmaba: “"He trabajado durante seis años con libertad, pero desde hace un par de meses se nos imponen restricciones de manera cotidiana: suspensión de actividades y de publicaciones ya programadas, pedido de renuncia a profesionales de alta capacitación técnica y designación de otros que no cumplen con el perfil requerido para el cargo, levantamiento de sitios web que dan cuenta de nuestro trabajo, prohibición de viajes"[59].

Para cubrir el cargo vacante, el Decreto 2150/09[60] del Poder Ejecutivo designó a la Doctora María Cristina Perceval que permaneció en el puesto por unos pocos meses hasta que, en mayo de 2010, Andrés Larroque fue designado como Subsecretario mediante el Decreto 698/2010[61]. Larroque fue elegido Diputado Nacional por el Frente para la Victoria en 2011[62], razón por la cual abandonó su puesto al frente de la Subsecretaría aunque no el equipo de investigación no encontró registro de su renuncia en las bases de datos públicos.

En julio de 2010, el Decreto 1099/10[63] designa de manera transitoria y por el lapso de 180 días como Director de Fortalecimiento de la Democracia a Franco Vitali. Esta designación se prorroga primero mediante el Decreto 784/11[64] –emitido en junio de 2011- y luego por el Decreto 1029/12[65]. En paralelo, y coincidente con la asunción de Andrés Larroque a su cargo de Diputado de la Nación, el Decreto 24/2011[66] designa como Subsecretario para la Reforma Institucional y el Fortalecimiento de la Democracia a Franco Vitali.

2.2 Diseño institucional para la implementación de la regulación de datos personales: Dirección Nacional de Protección de Datos Personales

En esta sección analizaremos los principales aspectos de la Dirección Nacional de Protección de Datos Personales, organismo establecido en la órbita del Ministerio de Justicia de la Nación para la implementación de la Ley 25326.

2.2.2 Aspectos externos

Tipo de legislación que crea la agencia
Como mencionamos anteriormente, el diseño institucional para la protección de los datos personales ha estado en el centro de la discusión desde el primer debate parlamentario. Tal como recordábamos oportunamente, en 1996 el Decreto 1616/1996 vetó la ley aprobada por el Congreso Nacional por entender que la Comisión Bicameral de Seguimiento de Protección Legislativa de Datos vulneraba “…la distribución constitucional de incumbencias estatales”. Ese desacuerdo entre el Poder Ejecutivo y el Legislativo llevó a que no sea 1996 el año en el que la Argentina se suma a la lista de países que cuentan con regulaciones en la materia, sino que deba esperar su turno hasta 1998.

[57] http://www.infoleg.gov.ar/infolegInternet/anexos/85000-89999/86455/norma.htm
[58] http://www.infoleg.gov.ar/infolegInternet/anexos/160000-164999/161054/norma.htm
[59] http://www.lanacion.com.ar/1206648-transparencia-por-falta-de-apoyo-renuncio-oyhanarte
[60] http://www.infoleg.gov.ar/infolegInternet/anexos/160000-164999/162397/norma.htm
[61] http://www.infoleg.gov.ar/infolegInternet/anexos/165000-169999/167394/norma.htm
[62] http://www.hcdn.gov.ar/diputados/alarroque/
[63] http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=170096
[64] http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=183375
[65] http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=199402
[66] http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=191065

El debate parlamentario que se da en el Senado de la Nación en 1998 encuentra a la constitución del órgano de control como uno de sus principales ejes. Veamos algunas de las posturas en el debate. El senador Berhongaray consideraba: "Un tema de consideración especial es el órgano de control. Se ha previsto que sea un organismo con independencia funcional y descentralizada, dentro del ámbito del Ministerio de Justicia de la Nación. Aquí se han propuesto distintas soluciones y alternativas. Se ha propuesto como órgano de control al defensor del pueblo. En fin, se ha propuesto que sea al margen del Poder Ejecutivo, pero nosotros entendemos que debe estar en la competencia del Poder Ejecutivo, ya que a éste le corresponde la administración general del país. En este caso se trata de desarrollar una eminente función administrativa de regulación y control. Esto es así porque no sólo le corresponde ejercer sus funciones respecto de los bancos de datos privados destinados a dar informes, sino también respecto de los bancos de datos públicos. Ello planteaba la necesidad de otorgar un grado de independencia funcional a ese organismo de control. Considerando las inquietudes planteadas en el dictamen en disidencia por parte de los señores senadores Branda y Berhongaray, hemos entendido que se debe reforzar la independencia técnica y funcional, teniendo en cuenta que al órgano de control también le corresponderá ejercer sus atribuciones respecto del Poder Ejecutivo, y que la designación de su director -ésa es nuestra propuesta- sea efectuada por el Poder Ejecutivo con acuerdo del Senado, estableciendo legalmente el período de duración en el cargo y su inamovilidad. Por lo demás, se dejan al Poder Ejecutivo los detalles respecto de la organización burocrática que corresponda, teniendo en cuenta la reforma administrativa en marcha. La articulación del control parlamentario de entes se da a través de las comisiones existentes y de las funciones que son propias del defensor del pueblo. Esto no excluye la participación del defensor del pueblo que, como es sabido, es un órgano del Congreso de la Nación que actúa con independencia funcional y autarquía financiera"[67].

Como vemos en esta exposición, hay una serie de argumentos que resultan de relevancia para la discusión: en primer lugar, que el tratamiento en comisión consideró diferentes diseños institucionales que podrían desempeñar la función de control; luego, que el órgano de control creado no sólo debe verificar el cumplimiento de la normativa sino también encargarse de la aplicación de la ley en los bancos públicos y es por eso que –argumenta Berhongaray- el órgano de aplicación debe estar en la órbita del Poder Ejecutivo Nacional; y tercero, considerando que el órgano debe estar en esa órbita, resulta de vital importancia asegurar la autonomía técnica y funcional del órgano para que, aun estando dentro del Ejecutivo, pueda actuar de manera independiente.

Diferente era la postura del Senador López que insistió con que el órgano de control quedara por fuera del Poder Ejecutivo Nacional en una conformación colegiada por diferentes instituciones: "Si a esto le agregamos, por ejemplo, el tema de la regulación del órgano de control, respecto del cual se dice que va a tener autonomía o independencia pero, en definitiva, va a estar girando en la órbita del Poder Ejecutivo, y no se garantiza independencia y autonomía -creando en la propia ley un órgano independiente del Poder Ejecutivo-, evidentemente estamos ante una posibilidad de que no funcione como un organismo de protección de los datos personales o de control eficiente, porque tendrá que controlar los propios bancos de datos que tiene el Poder Ejecutivo. Y es difícil que lo pueda hacer con imparcialidad girando en la propia órbita del Poder Ejecutivo. Observen, en una acotación más particularizada, que el órgano de control que crearía el dictamen de la mayoría, según el artículo 29 inciso e), está facultado para 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 de carácter personal que se le requieran. De tal manera que si se le ocurriese a un determinado Estado controlar la totalidad de los datos de las personas de ese país, podría obtener la información completa obrante en todos los bancos de datos públicos o privados de ese país. Es decir que tendría la totalidad del poder informático en sus manos y, con esto, dispondría de facultades exorbitantes en materia de identidad de las personas. Por eso preferiríamos que este órgano de control, tal como lo proponemos en el proyecto de ley que presenté oportunamente en este Senado, sea independiente y autónomo, que esté formado por un representante de la Cámara de Diputados, uno del Senado, uno del Poder Ejecutivo y uno de la Corte Suprema con jerarquía no inferior a juez de Cámara y un representante de la Fiscalía Nacional de Investigaciones Administrativas. (…) Es necesario establecer esta protección a los cinco intereses fundamentales sobre el registro de datos. Ellos son: el interés referido a la confidencialidad, el interés en que los datos sean completos y actualizados, el interés en saber el uso que se les dará, el interés en cuanto a contar con una administración eficiente, y el interés de que los datos no sean usados de manera ilícita. Para ello es necesario un órgano de control totalmente independiente, como los que han sido establecidos por leyes de otros países avanzados. No es una razón el principio de que por la reforma del Estado podríamos incurrir en un gasto elevado al crear un organismo de control independiente y autónomo del Poder Ejecutivo. No nos parece suficiente esta razón, porque se trata nada más y nada menos que de proteger el derecho a la intimidad de la persona, al manejo de sus datos para que no quede desnuda ante el poder informático y el entrecruzamiento de datos entre diversos registros, su cesión o su transferencia en determinado momento"[68].

[67] Para consultar la versión taquigráfica del debate en el Senado de la Nación puede accederse a este sitio http://www.senado.gov.ar/web/taqui/taqui_op_adjunto.php?clave=F31013/041000.htm#6

[68] Para consultar la versión taquigráfica del debate en el Senado de la Nación puede accederse a este sitio http://www.senado.gov.ar/web/taqui/taqui_op_adjunto.php?clave=F31013/041000.htm#6

El Senador Menem insiste con la ubicación del órgano de control en el ámbito del Poder Ejecutivo Nacional y apunta a la despolitización de la discusión considerando el blindaje que tendrá la designación de sus autoridades: "A través del tratamiento de distintos proyectos de ley, advierto que existe como una especie de cierta desconfianza sobre las facultades de control del Poder Ejecutivo. Parecería que para que el control sea legítimo debe ser ejercido únicamente por el Poder Legislativo y que todo lo que en esta materia se refiere al Poder Ejecutivo estuviera contaminado de algún virus que hace que bajo ningún punto de vista pueda tener algún tipo de órgano de control porque carecería de imparcialidad. Cuando tratamos este tipo de temas debemos dejar de lado quién es el que está gobernando, o sea el partido político al que le toca ejercer el gobierno. Al respecto, debe analizarse la forma que le hemos dado a este artículo: se han introducido una serie de reformas que dan una independencia y una autonomía funcional que realmente otorga una serie de garantías que, de ningún modo, pueden hacer pensar que ese órgano estará sometido a la influencia del Poder Ejecutivo. Además de decir que tendrá autonomía funcional y que actuará como órgano descentralizado, se establece que será dirigido y administrado por un director designado por el término de cuatro años por el Poder Ejecutivo, con acuerdo del Senado de la Nación. Es decir, le estamos dando a esto el tratamiento que hasta hace poco tiempo teníamos para la designación de jueces y que ahora tenemos para la designación de embajadores y de miembros del Banco Central. Esto, sin perjuicio de las facultades que también tiene el defensor del pueblo para intervenir por la naturaleza de las funciones que se le atribuyen por la ley de su creación y por la Constitución Nacional. Sobre el particular hubo muchas propuestas, inclusive una para que se le dé la función de órgano de contralor al Defensor del Pueblo. Consideramos que el Defensor del Pueblo puede actuar de manera coadyuvante, porque está dentro de sus funciones, pero pienso que en la forma en que hemos diseñado el órgano de control, reúne todas las garantías suficientes, porque inclusive en su designación interviene el Senado a través del acuerdo, como para que lo aceptemos en la forma en que está establecido. Además, no nos olvidemos de que aquí también tienen que ver los archivos públicos. De modo que es lógico que esté en la órbita del Poder Ejecutivo, por las funciones de administrador general del país que tiene, de acuerdo con la Constitución Nacional. Así que nosotros vamos a insistir en que lo referente al órgano de control quede tal como está redactado en la propuesta del artículo 29"[69].

El espacio dedicado en el debate del Senado para la determinación del órgano de control no se replicó en diputados: el tema no fue ni siquiera analizado por la Cámara Baja. El proyecto fue finalmente aprobado y la Ley 25326 dispone la creación de un órgano de control en el ámbito del Poder Ejecutivo con autonomía funcional. El organismo establecido por la ley tenía un formato de entidad descentralizada en la órbita del Ministerio de Justicia y Derechos Humanos de la Nación. Sin embargo, el Decreto 995/2000 emitido por el Presidente De la Rúa veta dos incisos fundamentales del artículo 29 de la ley:

"2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.
3.El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia" (Decreto 995/200).
Así, con una argumentación bastante pobre, De la Rúa borra de un plumazo toda la discusión parlamentaria:

"Que el artículo 29 del Proyecto de Ley establece la constitución de un Órgano de Control que deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y disposiciones emanados del referido Proyecto.
Que en el punto 2 del citado artículo se establece que el Órgano de Control gozará de autonomía funcional y actuará como organismo descentralizado en el ámbito del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.
Que el punto 3 del artículo 29 del Proyecto de Ley norma sobre la conducción y administración del Órgano de Control.
Que la constitución del Órgano de Control como organismo descentralizado habrá de implicar, como toda incorporación de una estructura organizativa de este tipo, un incremento en las erogaciones del ESTADO NACIONAL para atender su funcionamiento.
Que el presente Proyecto de Ley no prevé el financiamiento del Órgano de Control y la Ley N° 25.237 de Presupuesto de la Administración Nacional para el ejercicio 2000 y el Proyecto de Ley de Presupuesto Nacional para el ejercicio 2001 no contiene previsiones crediticias para su atención.
Que la legislación vigente en materia de Administración Financiera Pública determina que todo incremento de gastos debe prever el financiamiento respectivo.
Que sin perjuicio de lo indicado, se considera pertinente la constitución de un órgano de control, pero que reúna las características organizativas que determine el PODER EJECUTIVO NACIONAL de conformidad con la autorización conferida por el artículo 45 del presente Proyecto de Ley."

Es decir, el veto considera que la constitución de un órgano de control que no se encuentre financiado altera lo establecido por la doctrina de la administración financiera. Sin embargo, no cuestiona, modifica, ni pone en discusión las tareas que debe realizarse para implementar la ley. Es decir, cuestiona la constitución del organismo –o mejor dicho, un aspecto del mismo, su autonomía- por las erogaciones presupuestarias que implica, pero

[69] Para consultar la versión taquigráfica del debate en el Senado de la Nación puede accederse a este sitio http://www.senado.gov.ar/web/taqui/taqui_op_adjunto.php?clave=F31013/041000.htm#6

básicamente las erogaciones se vinculan con el desarrollo de las funciones que le son encargadas por la ley. Paradójicamente, el veto no reduce ninguna de sus funciones. “Con el veto presidencial, el órgano quedó desvirtuado en su fortaleza por varios motivos que exceden su dependencia funcional y se vinculan con otros aspectos como la forma de elección, requisitos para el cargo, duración y estabilidad de su titular…(…) Las razones expresadas en el veto parcial a ese apartado, si bien preminentemente formales y fundadas, llevaron prácticamente a vaciar de contenido las pocas garantías que la norma había establecido en pos de lograr una mínima independencia de criterio y la necesaria estabilidad de su director” (Pucinelli, 2004: 434-444).

La historia se cierra con otro decreto, el 1558/2001 en cuyo artículo 29 dispone la creación de la Dirección Nacional de Protección de Datos Personales (DNPDP) en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES contará con un Consejo Consultivo, que se desempeñará "ad honorem", encargado de asesorar al Director Nacional en los asuntos de importancia, integrado por:

a) un representante del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS;
b) un magistrado del MINISTERIO PUBLICO FISCAL con especialidad en la materia;
c) un representante de los archivos privados destinados a dar información designado por la Cámara que agrupe a las entidades nacionales de información crediticia;
d) un representante de la FEDERACION DE ENTIDADES EMPRESARIAS DE INFORMACIONES COMERCIALES DE LA REPUBLICA ARGENTINA;
e) un representante del BANCO CENTRAL DE LA REPUBLICA ARGENTINA;
f) un representante de las empresas dedicadas al objeto previsto en el artículo 27 de la Ley Nº 25.326, designado por las Cámaras respectivas de común acuerdo, unificando en una persona la representación;
g) un representante del CONSEJO FEDERAL DEL CONSUMO;
h) un representante del IRAM, Instituto Argentino de Normalización, con especialización en el campo de la seguridad informática;
i) un representante de la SUPERINTENDENCIA DE SEGUROS DE LA NACION;
j) un representante de la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del HONORABLE CONGRESO DE LA NACION.
Invitase a las entidades mencionadas en el presente inciso a que designen los representantes que integrarán el Consejo Consultivo.

En relación a la conformación del Consejo Consultivo, las autoridades de la Dirección entrevistadas informaron que en los últimos años no ha tenido actividad y que el rol del consejo mayor protagonismo en los momentos fundacionales de la Dirección en los que se necesitaba contar con mayor apoyo para el desarrollo del organismo y definir su estructura interna y áreas de trabajo.

Posición de la agencia en el organigrama/cobertura territorial

Tal como lo relatamos en el apartado anterior, el órgano de control quedó en la esfera del Poder Ejecutivo Nacional, pero subordinado como una agencia de cuarto nivel, bajo la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos de la Nación. La DNPDP tiene competencia a nivel nacional, de la mano a lo establecido por la Ley 25326.

Atribuciones

De acuerdo a la Ley 25326 la DNPDP tiene la responsabilidad de:

“a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;
b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;
c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;
d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;
e) 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;
f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;
g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley".

Además, la reglamentación de la legislación mediante al Decreto 1558/01 establece que la DNPDP debe:

"a) dictar normas administrativas y de procedimiento relativas a los trámites registrales y demás funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados;
b) atender las denuncias y reclamos interpuestos en relación al tratamiento de datos personales en los términos de la Ley Nº 25.326;
c) percibir las tasas que se fijen por los servicios de inscripción y otros que preste;
d) organizar y proveer lo necesario para el adecuado funcionamiento del Registro de archivos, registros, bases o bancos de datos públicos y privados previstos en el artículo 21 de la Ley Nº 25.326;
e) diseñar los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el mejor cumplimiento de la legislación de aplicación;
f) Homologar los códigos de conducta que se presenten de acuerdo a lo establecido por el artículo 30 de la Ley Nº 25.326, previo dictamen del Consejo Consultivo, teniendo en cuenta su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y organismo que elabora el código y su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados".

Como puede verse, las atribuciones y funciones establecidas por la ley y su decreto reglamentario son amplias y requieren la implementación sistemática de políticas públicas para garantizar la protección de datos personales. Nuevamente, llama la atención que el veto presidencial del Dr. De la Rúa objetara las características del órgano de control por las erogaciones presupuestarias y no modificara las actividades que debían realizarse para implementar la normativa. Consideremos solamente dos de sus funciones, las de "...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" y la de "Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley". Estas funciones suponen actividades de seguimiento sistemático sobre un universo muy extenso de entidades públicas y privadas para lo que resulta imprescindible un alto número de funcionarios a disposición de la dirección.

2.2.2 Aspectos internos

Capacidad organizativa

Presupuesto

Tal como lo mencionamos con anterioridad, el financiamiento de las actividades del órgano de control estuvo en la base de las discusiones en tanto dio pie al veto presidencial del Presidente De la Rúa. El Decreto reglamentario 1558/01 trabaja para subsanar esas objeciones y establece que la DNPDP "…se financiará a través de: a) lo que recaude en concepto de tasas por los servicios que preste; b) el producido de las multas previstas en el artículo 31 de la Ley Nº 25.326;29 c) las asignaciones presupuestarias que se incluyan en la Ley de Presupuesto de la Administración Nacional a partir del año 2002. Transitoriamente, desde la entrada en vigencia de la presente reglamentación y hasta el 31 de diciembre de 2001, el costo de la estructura será afrontado con el crédito presupuestario correspondiente al MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS para el año 2001, sin perjuicio de lo dispuesto en los su incisos a) y c) b) del párrafo anterior" (Decreto 1558/01). El Decreto 17/02 muestra la precariedad del organismo: "Que la emergencia económica y la crisis que afecta al país ha repercutido en forma significativa en el presupuesto asignado al Ministerio de Justicia y Derechos Humanos, que en este momento no cuenta con las partidas necesarias para la creación del cargo del Director en cuestión".

En la entrevista realizada con las autoridades de la Dirección se nos informó que el organismo no cuenta con SAF propio pero que el presupuesto asignado resulta suficiente para el desarrollo de las tareas a su cargo y para cubrir las erogaciones presupuestarias considerando que cuentan con un staff modesto de empleados.

Personal

De acuerdo al decreto reglamentario, la DNPDP "…contará con el personal jerárquico y administrativo que designe el Ministro de Justicia y Derechos Humanos aprovechando los recursos humanos existentes en la

ADMINISTRACIÓN PUBLICA NACIONAL. El personal estará obligado a guardar secreto respecto de los datos de carácter personal de los que tome conocimiento en el desarrollo de sus funciones".

De acuerdo a la información proporcionada por las autoridades del organismo, la Dirección cuenta con un plantel aproximado de 30 empleados. De acuerdo a la descripción de las autoridades, el personal es altamente calificado algo que se va reforzando a medida que su permanencia en el organismo se ratifica.

Diferenciación política
Reglas para la designación y remoción y duración del mandato

En este punto es donde vemos una de las mayores implicancias del veto presidencial. Recordemos que la ley aprobada por el Congreso de la Nación, estipulaba que el nombramiento del Director era realizado por propuesta del Poder Ejecutivo Nacional con acuerdo del Senado de la Nación, lo que apuntaba a garantizar cierta independencia de la autoridad designada. Al eliminar esta condición –que no se condice con el argumento de reducir las erogaciones asociadas a la creación de un organismo-, debilita el blindaje del organismo de la influencia partidaria o de la dependencia del Ejecutivo.

Luego, el decreto reglamentario, establece algunas condiciones extras para designación de su autoridad de la DNPDP y su mandato. De acuerdo a esta normativa, la dirección "…se integrará con un Director Nacional, Nivel "A" con Función Ejecutiva I, designado por el Poder Ejecutivo Nacional, por el plazo de cuatro (4) años, debiendo ser seleccionado entre personas con antecedentes en la materia, a cuyo fin facultase al Ministro de Justicia y Derechos Humanos, o a quien lo sustituya en sus funciones, a efectuar la designación correspondiente, como excepción a lo dispuesto por el Anexo I del Decreto Nº 993/91 y sus modificatorios".

Hay que destacar la Resolución 325/2002 por la que el Ministerio de Justicia desarrolla un mecanismo para la selección de candidatos a cubrir el puesto de Director Nacional. Esta resolución surge frente a la observación realizada por la Oficina Anticorrupción frente a la designación del primer director que fue realizada sin concurso público. De acuerdo a esta normativa, y con la finalidad de "…garantizar la transparencia en la designación de referencia y asegurar que la misma recaerá en una persona con probados antecedentes en la materia", el Ministerio dispuso un mecanismo en el que se realiza una convocatoria abierta a cubrir el cargo y en el que los candidatos que se postulen son evaluados por un Comité de Evaluación. El Comité propone una terna al Ministro de Justicia, y él determina cuál de los candidatos será finalmente propuesto al Presidente de la Nación para su designación.

Sin embargo, esa resolución se emitió con posterioridad al nombramiento del primer director, y, de acuerdo a las investigaciones desarrolladas en el presente estudio, fue aplicada tan solo una vez. El 18 de enero del 2002, la Resolución 17/2002 designó como Director Nacional para la Protección de Datos Personales al Dr. Juan Antonio Travieso. El Dr. Travieso es un profesional con probada trayectoria en el tema, que se desempeñaba como Jefe de Gabinete en el Ministerio de Justicia al momento de ser designado, cargo que mantuvo al principio y por lo que su designación es "ad honorem" en razón a los honorarios que percibía en su otro cargo. Cabe preguntarse si esta situación no alteró en su momento lo establecido en la Ley 25326 por su artículo 29: "El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones". Recién en septiembre de 2002, el Poder Ejecutivo formaliza en el Decreto 1898/02 la designación del Director, dejando sin efecto la situación "ad honorem", por lo que se entiende que para entonces la falta en la dedicación exclusiva se había resuelto. Recordemos que el cargo de Director tiene un mandato establecido de cuatro años. Si consideramos que el decreto de designación fue emitido en 2002, el primer término del mandato del Director caducó en 2006. Recién en junio de 2007, el Dr. Travieso es designado nuevamente. Llama la atención que, de acuerdo al Decreto 704/07, la designación tiene carácter de transitoria. Cuesta un poco seguir la historia de las designaciones en tanto hay una serie de actos normativos que parecen superponerse. Por ejemplo, un nuevo decreto, el 194/08, designa nuevamente de manera transitoria al Dr. Travieso al frente de la Dirección Nacional. También encontramos otro decreto (779/07) que designa de manera transitoria al Dr. Francisco José Orué como responsable de la DNPDP. Entre todos estos actos, no se han encontrado referencias a la utilización del mecanismo de selección de candidatos establecidos por la Resolución ministerial 325/02 lo cual podría explicar el por qué de la designación transitoria, aunque esto no es ni explicitado ni inferido del texto normativo. Finalmente, si consideramos que la última designación transitoria fue realizada en febrero del 2008, el mandato del actual Director Nacional habría vencido en febrero del 2012. Al momento en el que este informe era redactado, no consta en las bases de datos de legislación nacional, ni la designación de un nuevo Director, ni la convocatoria a cubrir el cargo de acuerdo a la Resolución 325/02[70].

[70] Para conocer los textos de las designaciones puede consultarse
http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=78107
http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=128991
http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=137316

En relación a las condiciones establecidas para la remoción del Director Nacional, de acuerdo al artículo 29 de la Ley 25326, el director del órgano de control "…podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones".

2.3 Mecanismos para resolución de controversias
Articulación entre las dos normativas

El Decreto 1172/03 considera la gestión de los datos personales de carácter sensible dentro del área de excepciones de la normativa, en su artículo 16: "Los sujetos comprendidos en el artículo 2º sólo pueden exceptuarse de proveer la información requerida cuando una Ley o Decreto así lo establezca o cuando se configure alguno de los siguientes supuestos:
I) información referida a datos personales de carácter sensible —en los términos de la Ley Nº 25.326— cuya publicidad constituya una vulneración del derecho a la intimidad y al honor, salvo que se cuente con el consentimiento expreso de la persona a que refiere la información solicitada"

El artículo 17 del decreto establece de qué manera debe actuarse frente a documentos que pueda contener información que debe ser preservado, es decir, en el caso de nuestro interés, qué hacer con aquellos documentos que puedan contener datos personales de carácter sensible: "En el caso que existiere un documento que contenga información parcialmente reservada, los sujetos enumerados en el artículo 2º deben permitir el acceso a la parte de aquella que no se encuentre contenida entre las excepciones detalladas en el artículo 16". Es decir, la normativa establece la necesidad de desarrollar mecanismos de disociación de datos para poder garantizar tanto el acceso a la información como la protección de datos personales. Para esto resulta fundamental articular la labor de los funcionarios encargados de implementar políticas de información con la de los archivistas o encargados de la gestión documental en el ámbito administrativos. Si los archivos o series documentales no cuentan con descriptores que sean capaces de dar cuenta del tipo de información que se conserva en las instituciones públicas difícilmente podrán ponerse en práctica mecanismos de disociación de manera eficiente.

Hemos analizado el modo en que la gestión de los datos personales es considerada por la normativa de acceso a la información. Veamos ahora el modo en que la accesibilidad a la información es considerada por la Ley 25326. En primer lugar, vale la pena recordar que la ley nacional de protección de datos personales aparece con anterioridad al debate local sobre el derecho a saber. Si bien ambos temas, como vimos, fueron tematizados –en diferente grado, claro está- en la reforma constitucional de 1994, el debate parlamentario por la regulación de la protección de los datos personales antecede al del acceso a la información. En las versiones taquigráficas se ve claramente que los legisladores no consideran el tema, lo rozan, en algunas ocasiones al mencionar los datos vinculados a la seguridad y defensa nacional pero no los tratan. Como consecuencia, la idea de accesibilidad que se encuentra presente en la normativa es aquella que se vincula con el ejercicio de la acción de habeas data, con la potestad que tiene un individuo de conocer –y corregir si fuera necesario- los datos de él/ella que poseen otros.

Siguiendo la argumentación anterior, la ley no estipula un mecanismo específico para solicitar y acceder información sino que establece el modo en que los datos personales pueden ser cedidos pero sin contemplar el eventual conflicto con el derecho fundamental de saber que los ciudadanos tenemos en una democracia representativa. El artículo 11 de la Ley 25326 establece así los requisitos que deben ser cumplidos para poder ceder documentos que contengan datos personales. Los requisitos son los siguientes:

> "1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
> 2. El consentimiento para la cesión es revocable.
> 3. El consentimiento no es exigido cuando:
> a) Así lo disponga una ley;
> b) En los supuestos previstos en el artículo 5° inciso 2;
> c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
> d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
> e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.
> 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".

Este artículo se complementa por lo establecido en el 5 inciso 2:

"1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

El modo en que estos artículos se armonizan o se han armonizado con las excepciones del decreto 1172/03 constituye el nudo de la tensión entre el derecho a saber y la protección de datos personales. Recordemos que este trabajo no apunta a brindar una interpretación de esta tensión sino a describir las instancias de resolución de controversias y las posibilidades que los diseños institucionales brindan para llegar a interpretaciones armónicas de ambas legislaciones.

Instancias de apelación para que los ciudadanos planteen controversias
Decreto 1172/03

Como detallábamos con anterioridad, la Subsecretaría para Reforma Institucional y la Oficina Anticorrupción desarrollaron un mecanismo para recepción y resolución de denuncias frente al incumplimiento de lo establecido por el Decreto 1172/03. Este mecanismo fue consagrado en la Resolución Conjunta 1/2008 y 3/2008 de ambos organismos[71].

El mecanismo se apoya en los artículos 18 y 18 del Decreto 1172/03 que las denuncias que se efectúen por incumplimientos al Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional deberán ser recibidas por la Oficina Anticorrupción y que la subsecretaría como Autoridad de Aplicación del Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional debe resolverlas.

El mecanismo dispone que los reclamos deban presentarse en la Oficina Anticorrupción, pero prevé que en caso de que un solicitante presente un requerimiento en otro organismo, éste debe remitirlo a la OA. El mecanismo establece una serie de requisitos y formales y un trámite especial para las denuncias. Una vez recibida la denuncia, la OA efectúa una actuación administrativa que habilita el descargo del organismo denunciado. Tanto la actuación administrativa como el descargo son incluidos en un informe preliminar que la OA debe entonces enviar a la Subsecretaría quien "analizará y merituará las constancias obrantes en las actuaciones y resolverá respecto de los hechos denunciados dentro de los VEINTE (20) días hábiles de recibida la actuación administrativa con el Informe Preliminar de la Oficina Anticorrupción. En su caso, recomendará a las autoridades competentes la adopción de las medidas de carácter particular o general que considere adecuadas para garantizar el derecho de acceso a la información del denunciante y el óptimo funcionamiento del Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional".

Como puede leerse, la Subsecretaría tiene solo capacidad para emitir recomendaciones sobre el modo en que debe resolverse la controversia. Si consideramos que estas resoluciones son emitidas por una subsecretaría y que muchas veces generan recomendaciones para organismos con mayor jerarquía organizacional (ministerios, secretarías) podemos conjeturar sobre la debilidad que enfrentan tales medidas para hacerse efectivas.

Las actuaciones de la subsecretaría generan en algunos casos "criterios orientadores". Estos criterios permiten ir estableciendo sentidos compartidos acerca de lo que debe entenderse por información pública y que resultan de utilidad para la interpretación de la normativa en otros casos. Estos criterios orientadores se encuentran disponibles en el sitio web del organismo aunque solo actualizados hasta 2009[72].

Ley 25326

En el caso de la ley de protección de datos personales, las instancias para que los se planteen controversias no resultan tan claras.

[71] http://www.anticorrupcion.gov.ar/documentos_relacionados/SGRP%201-08%20y%20FCA%203-08.pdf
[72] http://www.jgm.gov.ar/paginas.dhtml?pagina=115

Una primera forma de encarar la descripción de estos mecanismos es la intervención de la DNPDP frente a las consultas que provienen de otros organismos. Recordemos que en este trabajo estamos analizando exclusivamente los procedimientos que pueden aplicarse para resolver las controversias en relación a la provisión de información toda vez que esta contenga datos personales. Así, encontramos situaciones en las que particulares –ciudadanos u organizaciones- realizaron solicitudes de información a organismos del Poder Ejecutivo nacional y estos organismos consultaron a la DNPDP sobre si correspondía brindar o no información. En estos casos, la DNPDP dictamina y publica los criterios que deben seguirse en cada caso. Los dictámenes se encuentran online en su sitio web organizacional[73].

En segundo lugar, si consideramos las decisiones que adopta la Dirección Nacional de Protección de Datos Personales se encuentra con otras dificultades. Según Gils Carbó "…la norma, en líneas generales, atiende a la exigencia de brindar un marco legal adecuado al tratamiento de datos personales para el sector público y privado, pero falla en cuanto: 1) no prevé un recurso judicial directo contra las decisiones del órgano de control" (Pucinelli, 2004: 50). La Ley nacional establece un universo de decisiones que puede adoptar la DNPDP para cumplir y hacer cumplir la ley –decisiones sobre el carácter sensible de los datos, la extensión del deber de confidencialidad, la accesibilidad de los datos, entre otras. El punto es cómo pueden ser revisadas estas decisiones. Siguiendo el argumento de Pucinelli (2004), las decisiones adoptadas por la dirección podrían ser revisables gracias al recurso de reconsideración garantizado en la Ley de Procedimientos Administrativos y, frente a su negativa, por vía del recurso jerárquico ante el Ministro de Justicia. Finalmente podrían ser cuestionados en el ámbito contencioso administrativo en vistas a lo establecido en la misma ley para el espacio de competencia. Sin embargo, esta situación no pareciera resultar tan sencilla, de acuerdo a lo argumentado por Pucianelli: "…la Dirección Nacional de protección de Datos Personales no es una dirección cualquiera, ya que se destaca en ella el carácter autónomo como condición mínima esencial para una efectiva independencia de criterio y una eficaz labor de control, máxime si se considera que los bancos de datos de carácter público de mayor envergadura están en la mayoría en la órbita del Poder Ejecutivo nacional y la posibilidad de que las decisiones del órgano sean revocadas por la vía jerárquica desnaturaliza ese control. En este sentido, el art. 29 ap. 2 de la versión original de la ley 25326 –tal como fue sancionada por el Congreso- establecía que el órgano de control gozaría de autonomía funcional y actuaría como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación" (Pucinelli, 2004: 448).

Como hemos detallado anteriormente, este aspecto fue eliminado en el veto parcial, algo que intentó ser corregido luego por el decreto reglamentario 1558/01 que establece que el director de la DNPDP "ejercerá sus funciones con plena independencia y no estará sujeta a instrucciones". Un parche precario e insuficiente que no resuelve la desprolijidad del veto efectuado por el Dr. De la Rúa: "…si bien puede que esa plena independencia y la no sujeción a instrucciones debieran inhibir la revocación de las decisiones del director del órgano por la vía del recurso jerárquico –tanto por la naturaleza misma de este tipo de órganos de control como por la previsión reglamentaria- con lo cual quedaría sólo expedita la vía judicial (…), la cuestión no quedará definitivamente resuelta hasta que no se realicen las modificaciones legales pertinentes o se expida sobre el particular la Corte nacional en algún caso que llegue a su juzgamiento" (Pucinelli, 2004: 449).

Rivalidades

Una solicitud de información particular, que luego analizaremos en profundidad, puso en escena lo que hoy constituye el centro de este estudio: la tensión entre el derecho a saber y la protección de datos personales. El Ministerio de Desarrollo Social (MSD) negó información sobre beneficiarios de subsidios, a una ONG basada en la Ley 25326. En esta ocasión, tanto el SRIyFD y DNPDP tenían la atribución de formular recomendaciones al ministerio. El caso reveló la inexistencia de un mecanismo que permita resolver la tensión entre derechos y que establezca cómo debe tomar finalmente su decisión un ministerio frente a recomendaciones no vinculantes de dos organismos diferentes que, como pasó en este caso, pueden ser contrapuestas.

Esta tensión aparece en varios casos. En algunos, la tensión se expresa de manera explícita en las resoluciones de la Subsecretaría: "Sobre este particular esta Subsecretaría considera pertinente advertir que si bien la DNPDP resulta el organismo con competencia técnica específica en relación a la determinación del alcance de lo que debe considerarse dato personal, puesto que el art 29 ap a) de la Ley 25326 le da esa atribución, esta Subsecretaría resulta el organismo con competencia técnica específica a efectos de expedirse sobre aquellas cuestiones que tienen que ver con el ejercicio del derecho de acceso a la información pública en el ámbito del Poder Ejecutivo nacional" (Nota 86/2007).

3. Organizaciones en acción

Esta sección apunta a analizar el modo en que tanto la DNPDP y la SRIyFD han resuelto, en la práctica, controversias y definen qué se entiende por información pública, datos personales y deciden su publicación o

[73] http://www.jus.gob.ar/datos-personales/dictamenes.aspx

resguardo. Para esto, relevaremos también los mecanismos y bases de datos mediante los cuales organismos públicos recolectan datos personales de manera masiva. Para realizar esta tarea tomaremos algunas políticas particulares para analizar el modo en el que se ha considerado la gestión de datos personales en la documentación pública. Para esto analizaremos dos casos: en primer lugar, el tratamiento de los datos personales en las historias clínicas; y en segundo lugar, la gestión de las declaraciones juradas patrimoniales. Estos temas se han seleccionado en función a dos temas: el primero porque permite ejemplificar el modo en que se gestionan los datos personales de particulares contenidos en documentos públicos y el segundo, porque permite dar cuenta del modo en que se gestionan los datos personales de funcionarios públicos.

Historias clínicas

A nivel nacional aún no hay un método determinado para realizar esta tarea, sin embargo si hay una legislación que empieza a mostrar un lejano interés en esta temática. La ley 26.529 de Derechos del paciente define la historia clínica como "el documento obligatorio cronológico, foliado y completo en el que conste toda actuación realizada al paciente por profesionales y auxiliares de la salud". Asimismo ordena la conservación de la misma por un plazo mínimo de 10 años desde la última actuación registrada en la misma, aunque nada dice sobre como deberá ser conservada ni tampoco como se destruirá pasados esos 10 años. Sí contempla la posibilidad de almacenamiento en soporte magnético (siempre que se tomen en cuenta ciertos recaudos como el uso de acceso restringido con claves o medios no reescribibles de almacenamiento) aunque esto no quita que quienes quieran puedan seguir registrándola en las fichas de papel que tiene generalmente los médicos. Finalmente establece el plazo máximo de 48 hs. que ante un pedido tendrá el establecimiento para entregarle al paciente su historia clínica.

Respetando los lineamientos de la ley, en Argentina lo que ocurre comúnmente es que cada paciente tiene tantas historias clínicas como médicos a los que consultó a lo largo de su vida y estas en su mayor porcentaje se encuentran en soporte papel. Esta multiplicidad de historias clínicas y la forma de almacenarlas genera diversas desventajas. Ya sea porque a la hora de elaborar un diagnóstico no se cuenta con todos los antecedentes del paciente, o porque el papel sufre de deterioro con el tiempo o incluso por que es más fácil de extraviar. Es debido a estas situaciones que se recomienda la implementación de una historia clínica única y digital. Un primer intento de avanzar en esa situación se dio en una iniciativa promovida desde el Ministerio de Salud de la Nación en 2009 cuyo avance fue trabado luego de cambios en la dirección del organismo. En San Luis comenzará a implementarse la historia clínica digital sobre "todo tipo de asistencia a la salud que se preste en el Territorio Provincial ya sea privada o pública, cualquiera sea su jurisdicción". Así lo establece la Ley Acceso del paciente a su historia clínica crea un sistema de Historia Clínica Digital (HCD), y una Base de Datos Única de Salud, la cual "permitirá el almacenamiento y gestión de todas las Historias Clínicas Digitales (HCD)" .

Otro modo de indagar el modo en que se gestionan masivamente los datos personales contenidos en documentos públicos es el modo en que ha resuelto La segunda situación a la que se hace referencia al comienzo de este caso está relacionada con el acceso a la información de las historias clínicas. Este caso surge ante una consulta del Archivo General de la Nacional a la Dirección Nacional de Protección de Datos Personales, la cual en respuesta emite el Dictamen 01/04donde analiza la posibilidad de ceder o no determinadas historias clínicas ante un pedido de acceso a la información. Las historias clínicas en cuestión refieren a personas fallecidas entre 1947 y 1987. Estas al tener datos de salud requieren un tratamiento especial porque "pueden causar perjuicios tanto en la vida social de los afectados como de los parientes, tanto en el mercado laboral como en el de los seguros". Es por esto que la dirección dice que tan solo podrán ser cedidas a los sucesores universales del titular previa acreditación de identidad y por el plazo de 10 días, y a los profesionales que intervinieron en el tratamiento o los titulares del centro de salud del cual derivaron las historias clínicas. Asimismo contempla ciertos casos excepcionales en los cuales se podrán ceder estos datos a sujetos que no estén contemplados anteriormente. Estos casos se darán cuando "medien razones de interés general autorizadas por una ley", "cuando la finalidad de su recolección y tratamiento sea estadística o científica y los titulares de los datos recabados no puedan ser identificados, por lo que deben disociarse los datos" y ante una resolución judicial, cuando medien razones fundadas relativas a la seguridad pública, defensa nacional o la salud pública.

Como se puede ver, a nivel nacional aún no hay mucho dicho sobre esta cuestión. Sin embargo hay ciertos puntos claros: los datos de salud deben estar especialmente protegidos, por lo tanto a la hora de instrumentar un sistema general de almacenamiento de estos habrá que ser muy cuidadosos con las medidas de seguridad que se implementen, de forma tal que el acceso quede restringido únicamente al paciente y a los profesionales e instituciones que intervengan en su tratamiento. Pudiendo otorgarse a terceros solo en unos pocos casos de excepción.

Declaraciones juradas patrimoniales

"Quizás, obviamente, usted no lo ignora, señor senador, pero la ley de ética pública que hemos sancionado permite el acceso a cualquier ciudadano a las declaraciones de bienes que hacemos todos los funcionarios públicos, parlamentarios y demás personas vinculadas con el quehacer público. Hago esta reflexión simplemente para señalar

que el secreto que podría rodear al patrimonio de los hombres públicos está hoy relativizado, casi -diría yo- suprimido por esta decisión que hemos tomado al legislar sobre ética pública"
Senador Cafiero, debate por la Ley 25326.

La Ley Nacional de Ética en la Función Pública (25188) aprobada en 1999 es clara: las declaraciones juradas patrimoniales de los funcionarios son públicas. El Capítulo II de la ley establece el modo en que los funcionarios determinados en el artículo 5[74] deben presentar sus declaraciones juradas patrimoniales y los mecanismos establecidos para la consulta pública. Los funcionarios deben presentar sus DDJJ al asumir el cargo, anualmente y al dejar sus funciones.
La ley garantiza el derecho de acceder a la información patrimonial de los funcionarios aunque establece ciertos requisitos y formalidades que van más allá de los establecidos posteriormente por el Decreto 1172/03:

"ARTICULO 10. — El listado de las declaraciones juradas de las personas señaladas en el artículo 5º deberá ser publicado en el plazo de noventa días en el Boletín Oficial.
En cualquier tiempo toda persona podrá consultar y obtener copia de las declaraciones juradas presentadas con la debida intervención del organismo que las haya registrado y depositado, previa presentación de una solicitud escrita en la que se indique: a) Nombre y apellido, documento, ocupación y domicilio del solicitante; b) Nombre y domicilio de cualquier otra persona u organización en nombre de la cual se solicita la declaración; c) El objeto que motiva la petición y el destino que se dará al informe; y d) La declaración de que el solicitante tiene conocimiento del contenido del artículo 11 de esta ley referente al uso indebido de la declaración jurada y la sanción prevista para quien la solicite y le dé un uso ilegal.
Las solicitudes presentadas también quedarán a disposición del público en el período durante el cual las declaraciones juradas deban ser conservadas.

ARTICULO 11. — La persona que acceda a una declaración jurada mediante el procedimiento previsto en esta ley, no podrá utilizarla para:
a) Cualquier propósito ilegal;
b) Cualquier propósito comercial, exceptuando a los medios de comunicación y noticias para la difusión al público en general;
c) Determinar o establecer la clasificación crediticia de cualquier individuo; o
d) Efectuar en forma directa o indirecta, una solicitud de dinero con fines políticos, benéficos o de otra índole.

[74] ARTICULO 5º — Quedan comprendidos en obligación de presentar la declaración jurada:
a) El presidente y vicepresidente de la Nación;
b) Los senadores y diputados de la Nación;
c) Los magistrados del Poder Judicial de la Nación;
d) Los magistrados del Ministerio Público de Nación;
e) El defensor del pueblo de la Nación y los adjuntos del defensor del pueblo;
f) El jefe de gabinete de ministros, los ministros, secretarios y subsecretarios del Poder Ejecutivo;
g) Los interventores federales;
h) El síndico general de la Nación y los síndicos generales adjuntos de la Sindicatura General de la Nación, el presidente y los auditores generales de la Auditoría General de la Nación, las autoridades superiores de los entes reguladores y los demás órganos que integran los sistemas de control del sector público nacional, y los miembros de organismos jurisdiccionales administrativos;
i) Los miembros del Consejo de la Magistratura y del Jurado de Enjuiciamiento;
j) Los embajadores, cónsules y funcionarios destacados en misión oficial permanente en exterior;
k) El personal en actividad de las Fuerzas Armadas, de la Policía Federal Argentina, de Gendarmería Nacional, de la Prefectura Naval Argentina y del Servicio Penitenciario Federal, con jerarquía no menor de coronel o equivalente;
l) Los rectores, decanos y secretarios de las universidades nacionales;
m) Los funcionarios o empleados con categoría o función no inferior a la de director o equivalente, que presten servicio en la Administración Pública Nacional, centralizada o descentralizada, las entidades autárquicas, los bancos y entidades financieras del sistema oficial, las obras sociales administradas por el Estado, las empresas del Estado, las sociedades del Estado y el personal con similar categoría o función, designado a propuesta del Estado en las sociedades de economía mixta, en las sociedades anónimas con participación estatal y en otros entes del sector público;
n) Los funcionarios colaboradores de interventores federales, con categoría o función no inferior a la de director o equivalente;
o) El personal de los organismos indicados en el inciso h) del presente artículo, con categoría no inferior a la director o equivalente;
p) Todo funcionario o empleado público encargado de otorgar habilitaciones administrativas para el ejercicio de cualquier actividad, como también todo funcionario o empleado público encargado de controlar el funcionamiento de dichas actividades o de ejercer cualquier otro control en virtud de un poder de policía;
q) Los funcionarios que integran los organismos de control de los servicios públicos privatizados, con categoría no inferior a la de director;
r) El personal que se desempeña en el Poder Legislativo, con categoría no inferior a la de director;
s) El personal que cumpla servicios en el Poder Judicial de la Nación y en el Ministerio Público de la Nación, con categoría no inferior a secretario o equivalente;
t) Todo funcionario o empleado público que integre comisiones de adjudicación de licitaciones, de compra o de recepción de bienes, o participe en la toma de decisiones de licitaciones o compras;
u) Todo funcionario público que tenga por función administrar un patrimonio público o privado, o controlar o fiscalizar los ingresos públicos cualquiera fuera su naturaleza;
v) Los directores y administradores de las entidades sometidas al control externo del Congreso de la Nación, de conformidad con lo dispuesto en el artículo 120 de la ley 24.156, en los casos en que la Comisión Nacional de Ética Pública se las requiera.

Todo uso ilegal de una declaración jurada será pasible de la sanción de multa de quinientos pesos ($ 500) hasta diez mil pesos ($ 10.000). El órgano facultado para aplicar esta sanción será exclusivamente la Comisión Nacional de ética Pública creada por esta ley. Las sanciones que se impongan por violaciones a lo dispuesto en este artículo serán recurribles judicialmente ante los juzgados de primera instancia en lo Contencioso Administrativo Federal".

Si bien la ley fue un paso fundamental en la publicidad de la información patrimonial de los funcionarios, la implementación se encontró con muchos obstáculos. Gran parte de los obstáculos se vincularon al diseño institucional creado por la ley para recibir, preservar y analizar las declaraciones juradas. La ley establecía que estas funciones debería desarrollarlas la Comisión Nacional de Ética Pública que jamás fue constituida. Frente a esa situación, la división de poderes garantizada en el ordenamiento republicano dio lugar a la implementación no uniforme del contenido de la ley. Mientras que el Ejecutivo avanzó en la creación de un mecanismo para recibir y controlar las DDJJ[75], tanto el Poder Judicial como el Poder Legislativo se resistieron a la aplicación de la normativa. El Poder Judicial lo hizo al establecer su propio régimen de recepción de DDJJ mediante la Acordada 1/2000[76], un régimen en el que la Corte Suprema de Justicia de la Nación determinaba si brindaba acceso o no las declaraciones suprimiendo de este modo su carácter público. En el caso del Poder Legislativo, cada una de las cámaras enfrentó acciones legales para que se permitiera el acceso a las declaraciones juradas[77]. El Comité de Expertos del Mecanismo de Seguimiento de la Convención Interamericana contra la Corrupción llamó la atención de estas irregularidades en la implementación de la Ley de Ética Pública en diferentes informes[78]. Al momento de cerrar el presente informe la Presidente de la Nación Cristina Fernández de Kirchner había anunciado una reforma integral al régimen de presentación de las declaraciones juradas patrimoniales de modo tal que se corrijan las deficiencias en la implementación de la ley nacional de ética en la Función Pública. Este anuncio se hizo con motivo a la apertura de sesiones ordinarias del Poder Legislativo en el que anunció la agenda legislativa del 2013[79].

Casos resueltos por las autoridades de aplicación sobre las tensiones entre el derecho a saber y la protección de los datos personales.

De acuerdo al último informe publica por la Oficina Anticorrupción que releva las actividades realizadas en el organismo desde su creación hasta junio de 2012, son pocas las presentaciones recibidas por incumplimiento del Decreto 1172/03 en relación al reglamento de Acceso a la Información: "Hasta el momento de cierre del presente informe y desde la entrada en vigencia del Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional, el 22 de abril de 2004, la OA ha recibido un total de ciento noventa y siete (197) denuncias por incumplimiento de dicho régimen, de las cuales dos (2) corresponden al año 2004, veintiocho (28) al año 2005, veintinueve (29) al año 2006, treinta y seis (36) al año 2007, veinticuatro (24) al año 2008, treinta y tres (33) al 2009, veinticuatro (24) al 2010, diecisiete (17) al 2011 y cuatro (4) en el primer semestre del 2012. (…) estas denuncias fueron tramitadas inicialmente por la DPPT y luego remitidas a la Subsecretaría para la Reforma Institucional y Fortalecimiento de la Democracia, para que este organismo actúe en ejercicio de sus competencias específicas como Autoridad de Aplicación. Actualmente no se registran denuncias en trámite ante esta Oficina" (OA, 2012: 54-55).

Como puede verse, nada de la información brindada en el informe oficial da cuenta del contenido de los reclamos por lo que no puede determinarse cuántas de estas denuncias se han vinculado a la resolución de controversias entre el derecho a saber y la protección de datos personales.

Si analizamos las resoluciones de la Subsecretaría para la Reforma Institucional y Fortalecimiento de la Democracia que figuran en su sitio web institucional encontramos que desde la entrada en vigencia del Decreto 1172/02 hasta el 2009 –último año sobre el que encontramos información disponible online- se emitieron 106 recomendaciones[80]. De esas, solo 8[81] se vinculan con la resolución de controversias entre el derecho a saber y la protección de datos personales.

[75] http://www.ddjjonline.gov.ar/
[76] http://www.foresjusticia.org.ar/FORES3/ETICA/Normas.htm#acordada
[77] Poder Ciudadano inició una acción judicial de amparo por mora contra la Presidencia de la Cámara de Diputados para que la justicia estableciera el plazo en el que la cámara debía entregar copia de las de las declaraciones juradas patrimoniales y financieras de los legisladores. En el caso del Senado, Poder Ciudadano inició una acción judicial de amparo contra la Secretaría Administrativa del Senado para que la justicia declare ilegítima la falta de presentación de las ddjj. En ambos casos la justicia dictaminó a favor de la organización no gubernamental exigiendo a las cámaras que arbitren los modos en que se publique la información.
[78] http://www.oas.org/juridico/spanish/arg.htm
[79] http://www.presidencia.gob.ar/discursos/25724-apertura-del-130o-periodo-de-sesiones-ordinarias-del-congreso-nacional-discurso-de-la-presidenta-de-la-nacion
[80] Este dato surge utilizando los criterios de búsqueda del sitio web organizacional http://www.jgm.gov.ar/paginas.dhtml?pagina=115
[81] Las notas que contienen el criterio "datos personales" de acuerdo al sitio web institucional de la Subsecretaría son las 09/2009, 214/2008, 92/2008, 60/2008, 45/2008, 40/2008, 79/2007 y 80/2007.

En el caso de la Dirección Nacional de Protección de Datos Personales, desde su creación hasta el momento en el que este informe fue elaborado realizó un total de 296[82]. Del total de estos dictámenes, 96 refieren en su descripción a controversias planteadas en relación a la armonización entre el Decreto 1172/03 y la Ley 25326.

Hasta podemos hacer una conjetura, que puede ser errónea en vistas a la falta de información sobre la Subsecretaría: la Dirección Nacional de Protección de Datos Personales desempeña hoy un rol más activo que la Subsecretaría en la definición de lo que se considera información pública. Esto es algo que no debiera sorprendernos, especialmente si consideramos el diseño institucional del Decreto 1172/03. La DNPDP definió qué se considera información pública de manera independiente a lo que establece el decreto y lo hizo de la siguiente manera en distintos dictámenes. En primer lugar considera que: "La Ley Nº 25.326 define a una base como "pública" no por la posibilidad de acceso del público a la información contenida en ella, sino por su titularidad por parte de un organismo público". Y que sea pública no se vincula necesariamente con el acceso o la publicación de información y es por eso que distingue entre tres tipos de información: "De esta manera, como ya ha tenido oportunidad de señalar este Órgano de Control, la información registrada en una base de datos pública puede ser clasificada en tres niveles de intensidad de la publicidad de los datos que registra: a) Información confidencial: Es aquella afectada por un secreto o confidencialidad legal (Ej. Secreto profesional, bancario, fiscal, datos sensibles, etc.), derechos de terceros (ej. intimidad), etc. b) Información de acceso público: Es la información en poder de la Administración que no está sujeta a confidencialidad ni tampoco está destinada a ser difundida irrestrictamente al público, y que generalmente su acceso por parte de terceros resulta condicionado al cumplimiento de ciertos requisitos. c) Información de acceso público irrestricto: Es aquella información destinada a ser difundida al público en general"[83].

Más allá de esta postura, el análisis de los dictámenes muestra cierta coherencia interpretativa de la Dirección. En todos los dictámenes en donde estaba en juego la disputa normativa, la Dirección siguió al pie de la letra la Ley 25326 sin considerar armonización alguna con el decreto ni con los avances locales, regionales o internacionales en el reconocimiento del derecho a saber cómo derecho fundamental. La clave interpretativa, en breve, se apoya en 3 puntos:

- El artículo 11 de la Ley Nº 25.326 dispone que los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
- El requisito del consentimiento puede ser relevado en el caso que se presente alguna de las situaciones establecidas en el artículo 5°, inciso 2[84]
- Pero incluso cuando se pudiera exceptuar del consentimiento, la Dirección se apoya en el requerimiento establecido por el artículo 11 de existencia de interés legítimo.
- Adicionalmente la dirección recurre al artículo 28 inciso 2 que prescribe que si no fuera posible mantener el anonimato se deberá utilizar una técnica de disociación de modo que no permita identificar a persona alguna.

Veamos dos casos que resultan paradigmáticos para el análisis de la tensión entre el derecho a saber y la protección de datos personales: el acceso al listado de beneficiarios de planes sociales y el acceso a la información sobre sociedades comerciales que se encuentra en manos de la Inspección General de Justicia (IGJ).

Caso CIPPEC vs Ministerio de Desarrollo Social

En 2007, el Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC) presentó un pedido de información al Ministerio de Desarrollo Social (MDS) solicitando información relativa a las transferencias en gastos corrientes realizadas al sector privado en diferentes conceptos. Entre la información solicitada, la organización requirió información sobre las transferencia tramitadas y subsidios otorgados en el rubro presupuestario "ayuda social a personas,

[82] Este es el total de los dictámenes disponibles en el sitio web del organismo. En algunos años la numeración de los dictámenes no es consecutiva. Este aspecto no es explicado en el sitio razón por la cual no puede afirmarse que el listado publicado sea exhaustivo de los dictámenes emitidos. Para consultar el listado puede accederse a http://www.jus.gob.ar/datos-personales/dictamenes/

[83] Esta definición está contenida en el primer dictamen que emitió el organismo en razón de una controversia con la implementación del Decreto 1172/03 y que se encuentra disponible en http://www.jus.gob.ar/media/41510/D2004_009.pdf

[84] "2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526".

copia de los padrones de beneficiarios en el ejercicio presupuestario 2006. El MDS respondió en julio de 2007 con una negativa explicando que no podían suministrar dicha información en tanto la información contenía datos personales. Esta respuesta impulsó a la ONG a presentar una denuncia en la Oficina Anticorrupción. La OA elaboró un informe técnico concluyendo que "las constancias agregadas en las presentes actuaciones me llevan a opinar que la respuesta brindada por el MDS a la solicitud de información presentada por CIPPEC, se aparta del debido cumplimiento del Reglamento General de Acceso a la Información y vulnera el derecho de acceso a la información pública". El informe fue remitido a la Subsecretaría, como autoridad de aplicación del decreto, quien para resolver la controversia pidió consulta a la DNPDP.

En febrero de 2008, la DNPDP emitió un dictamen en respuesta a esta consulta. Allí interpreta que el pedido efectuado por CIPPEC reclama una cesión de datos personales y, por lo tanto, deben aplicarse los requisitos establecidos por la Ley 25326: "En consecuencia, exigiendo la Ley Nº 25.326, la existencia de "interés legítimo", los datos personales no podrían cederse frente a la ausencia, en el caso concreto, de ese interés, no obstante que el Decreto Nº 1172/03 no lo exija. En materia de datos personales –como ya se dijo- rige lo dispuesto en la citada ley". El dictamen obliga al Ministerio a obligar un eventual daño a terceros pero exime la obligación del consentimiento: "En efecto, la información identificadora de los listados de beneficiarios de ayuda social, se le agrega una información adicional, que es precisamente, la de integrar un grupo de personas que reciben ayuda social, circunstancia que excluye la excepción al consentimiento prevista en el artículo 11, inciso 3, apartado b, de la Ley Nº 25.326". A los argumentos que mencionábamos anteriormente, la DNPDP agrega la consideración del carácter de los datos personales solicitados. La Dirección entiende que los datos solicitados pueden poseer carácter sensible: "Si bien el hecho de integrar una lista de beneficiarios de un plan de ayuda social no es, en principio, información de carácter sensible per se, si el subsidio tiene su origen o fundamento en una enfermedad (dato relativo a la salud) podría revelar un dato sensible, circunstancia que configuraría en ese caso la excepción prevista en el citado artículo 16 del Reglamento de Acceso a la Información Pública"[85].

La Subsecretaría toma lo dictaminado por la DNPDP en su Nota 40 del 2008[86] y sigue su interpretación en relación a la eximición de la obligación del consentimiento pero disputa la interpretación del requisito de interés legítimo en tanto la misión organizacional de la Fundación permitiría acreditarlo. Y agrega que la evaluación del daño sobre la intimidad de los beneficiarios debe ser contemplada en concreto y junto al contexto de la información de cada uno de los planes y debe tenderse a proveer la mayor cantidad de datos posibles recurriendo, en última instancia a técnicas de disociación.

Como podemos ver, esta respuesta de la Subsecretaría entra en disputa con lo dictaminado por la DNPDP. Frente a esta contradicción, ¿cómo debía actuar el Ministerio? ¿Qué recomendación debía seguir? El Ministerio optó por cerrar su información y la organización terminó apelando a la justicia. El caso muestra entonces el fracaso de las autoridades de aplicación para resolver una controversia y demuestra que en esta tensión ninguna de las dos entidades posee la última ratio para definir el tema. El caso aguarda su resolución por parte de la Corte Suprema de Justicia de la Nación desde 2010.

Caso Ricardo Gil Lavedra vs Inspección General de Justicia (IGJ)

La Asociación por los Derechos Civiles presentó una acción de amparo contra la IGJ por la falta de respuestas a los pedidos de información remitidos por el Diputado Nacional por la Unión Cívica Radical sobre las sociedades comerciales registradas en dicho organismo, especialmente aquellas vinculadas con el llamado caso Ciccone[87]. El diputado había presentado dos solicitudes "…sobre la composición accionaria de diversas sociedades vinculadas al llamado caso Ciccone y sobre el accionar de la propia IGJ en relación a diversas irregularidades denunciadas en relación a esas personas jurídicas. En particular, se solicitó acceder al estatuto de diversas sociedades comerciales inscriptas en el Registro Público de Comercio, así como a datos sobre su integración accionaria, de sus órganos de gobierno, entre otros".

A la falta de respuesta se agrega la determinación de la IGJ de una nueva política para acceder a la información en sus registros que requería la acreditación de parte interesada o demostración de interés legítimo. Esta decisión fue adoptada por la IGJ siguiendo los lineamientos establecidos por la Dirección Nacional de Datos Personales (DNPDP) en el dictamen 7/2012.

---

[85] http://www.jus.gob.ar/media/43433/d2008_002.pdf
[86] http://tmp.jgm.gov.ar/Paginas/AccesoDescargaCriterios.php?id=37
[87] El caso Ciccone se refiere a la quiebra de la empresa Ciccone Calcográfica, una imprenta privada a la que se le otorgó en diferentes ocasiones la impresión de moneda. Frente a la quiebra, una sociedad llamada The Old Fund realizó un salvataje y una moratoria excepcional eximió a la compañía de la bancarrota. El caso tuvo repercusión por la falta de información sobre la composición de The Old Fund y por la supuesta vinculación del fondo con el Vicepresidente de la Nación. El caso se encuentra en estudio por la justicia.

Sobre este dictamen opinaba la ADC: "En efecto, allí la DNPDP postula una interpretación del régimen de acceso a la información pública que no analiza adecuadamente los intereses constitucionales en juego, no valora el rol que el acceso a la información cumple en una sociedad democrática y resulta en una restricción ilegítima de ese derecho constitucional"[88].

Llama la atención, en este dictamen, la consideración de la información sobre sociedades comerciales como dato personal. No podemos olvidar que el artículo 1 de la Ley 25326 incluye en el alcance de las normativas no sólo a las personas físicas sino también a las personas jurídicas, pero lo hace con una advertencia: "Las disposiciones de la presente ley también serán aplicables, *en cuanto resulte pertinente*, a los datos relativos a personas de existencia ideal"[89]. Nada hay en el dictamen sobre el análisis de la pertinencia de esa interpretación extensa de la normativa. Este tema había sedo mencionado por el legislador Berhongaray cuando se debatió en el Congreso: "El régimen se hace extensivo a la protección de los datos de las personas de existencia ideal, inclusión que se efectuó no sólo porque existen antecedentes en ese sentido en el derecho comparado, sino porque además el artículo 43 se refiere a toda persona, sin distinguir entre personas de existencia física e ideal. Y recordemos, además, que hay un precepto jurídico según el cual donde la ley no distingue no debemos distinguir. Es cierto que alguien podría preguntar, válidamente, cómo se puede proteger el derecho a la intimidad de una persona de existencia ideal. Sin embargo, no es que se trate de proteger la intimidad de ese tipo de personas sino de su derecho a que se tenga de ellas un conocimiento adecuado y real; que no sean objeto de discriminación ni de información que las pueda colocar en una situación difícil. Además, no cabe duda de que las personas de existencia ideal están integradas por personas de existencia física. Y muchas veces, la información que afecta a una persona de existencia ideal puede afectar, indirectamente, a las personas de existencia física que la integran. Sería el caso de una sociedad de la cual se diga que ejerce actividades ilícitas o de contrabando. Indudablemente, quienes integren dicha sociedad se verán afectados por ese dato falso. Por eso, también hemos incluido la protección de las personas de existencia ideal". Sin embargo, este punto no fue objeto de mayor debate.

4. Conclusiones

Hemos analizado en este documento el diseño de las dos instituciones establecidas para garantizar el derecho a saber y la protección de datos personales. En el caso de Subsecretaría para la Reforma Institucional y el Fortalecimiento de la Democracia nos encontramos con una organización que fue creada para funciones un tanto distantes a la promoción al acceso a la información. El Decreto 1172/03 fue un paso fundamental en el reconocimiento del derecho a saber porque permitió avanzar en una agenda que no hallaba su lugar en el ámbito parlamentario. Con sus traspiés y sus obstáculos, el Poder Ejecutivo Nacional ha recorrido un camino que otros poderes no han transitado aún.

El decreto fue una política muy valiosa en un contexto de recomposición del vínculo con la ciudadanía y colaboró, en sus primeros pasos, a establecer diálogos entre estado y sociedad, entre funcionarios y ciudadanos, entre responsables de la información y organizaciones comunitarias. Sin embargo, el déficit en diseño institucional del decreto frenó la reforma buscada. 10 años después de su emisión, el Reglamento General de Acceso a la Información muestra sus limitaciones, especialmente en relación a su diseño.

El haber establecido a la Subsecretaría de Reforma Institucional y Fortalecimiento de la Democracia como autoridad de aplicación se visualiza hoy como un desacierto. Su ubicación en el organigrama del ejecutivo como agencia de cuarto nivel, sin presupuesto propio, sin capacidades para designar a su propio personal y sin requisitos para la designación y remoción de funcionarios genera condiciones adversas para garantizar el derecho de toda persona a acceder a información pública. Estas limitaciones se refuerzan por el hecho de que la misión por la que fue constituida la Subsecretaría difiere a las atribuciones establecidas por el decreto.

Por otro lado, la Dirección Nacional de Protección de Datos Personales presenta tus propias debilidades de origen. La intención del legislador de contar con un organismo autónomo para proteger los datos de las personas naufragó con el veto presidencial del Dr. De La Rúa. Ese veto limitó de una vez y para siempre la entidad del organismo, su capacidad de financiamiento y los requisitos para la designación y remoción de las autoridades. Un tema que no ha sido objeto de este estudio, pero que debería ser indagado es hasta qué punto el veto presidencial limitó el pleno desarrollo de las actividades establecidas en la letra de la ley. Sin autonomía, sin SAF, puede la Dirección desarrollar ampliamente sus actividades de fiscalización del sector privado?

Nuestro objetivo ha sido el de determinar si el presente diseño institucional resulta adecuado para resolver controversias entre el derecho a saber y la protección de los datos personales. Difícil es tener opinión acerca de cuál es el mejor ordenamiento para la resolución de controversias. Lo que aparece aquí, como lo mostramos en el caso CIPPEC vs MDS, es que contamos con dos organismos que pueden brindar recomendaciones contrapuestas sobre el mismo caso. Consultado sobre el tema, Puccinelli afirmaba: "dado que existen similares causales de negativa de

[88] La posición completa y el amparo presentado por la Asociación por los Derechos Civiles se encuentra disponible en http://www.adc.org.ar/sw_contenido.php?id=915
[89] El subrayado es nuestro.

acceso a la información pública de las de negativa de acceso a los datos personales, es aconsejable que no haya dos órganos de control separado sino uno solo que unifique ambas cuestiones porque de lo contrario habría choques permanentemente, por ejemplo, entre los criterios de protección de datos de uno y de otro órgano, generando una suerte de respuesta bipolar por parte del Estado que no resulta compatible con el sistema de derechos humanos vigente en nuestros países".

Está claro que estas son las cuestiones que deberán abordar los legisladores cuando vuelva a darse el debate por la Ley Nacional de Acceso a la Información Pública. Nuestro país necesita un marco normativo que alcance a todos los poderes y que establezca una instancia clara para la resolución de controversias. Hoy, el decreto se muestra como insuficiente. Y la información sigue desempeñando su lugar clave para el ejercicio no solo del derecho a saber sino también de otros derechos.

Anexo I

Dictámenes Dirección Nacional Protección de Datos personales vinculados con el Decreto 1172/03

2004

009: Acceso a la Información Pública (Decreto Nº 1172/03) - Ministerio del Interior - destinatarios de subsidios y subvenciones.
019: Acceso a la información pública (Decreto Nº 1172/03) - nómina de contratados del Ministerio de Trabajo.
028: Acceso a la Información Pública(Decreto Nº 1172/03) - Ministerio del Interior - subsidios y subvenciones (Decreto Nº 1192/03 y en la Resolución MI Nº 235/04).
034: Acceso a la Información Pública (Decreto Nº 1172/03) - Ministerio del Interior - organigrama de empleados del Ministerio del Interior y sus dependencias.

2005

158: Acceso a la Información Pública (Decreto 1172/03), frente a las consultas que recibe Gendarmería Nacional sobre la entrada y salida de vehículos del país.
249: Acceso a la Información Pública Decreto 1172/03Ministerio del Interior -Listado de Asilados.

2006

018: Acceso a la Información Pública(Decreto 1172/03) - ADMINISTRACIÓN FEDERAL DE INGRESOS PUBLICOS (AFIP) por parte de la Unión Personal Civil de las Fuerzas Armadas (PECIFA).
043: Acceso a la Información Pública(Decreto 1172/03) - entradas y salidas de personas del edificio del Ministerio de Economía de la Nación (MECON).
082: Acceso a la Información Pública(Decreto 1172/03) - Gendarmería Nacional Argentina
118: Acceso a la Información Pública(Decreto 1172/03); Ministerio del Interior (Fundación Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento -CIPPEC-).
134: Acceso a la Información Pública (Decreto 1172/03); Ministerio del Interior; funcionarios, remuneraciones y subsidios.
216: Acceso a la Información Pública(Decreto Nº 1172/03) - Secretaría de Asuntos Municipales del Ministerio del Interior (datos de auditores y plan de auditoria 2006).
254: Acceso a la información pública (Decreto Nº 1172/03); Ministerio del Interior; subsidios (Decreto Nº 1193/03)
274: Acceso a la información pública (Decreto Nº 1172/03); Ministerio del Interior; datos penales y contravencionales de personas fallecidas
285: Acceso a la información pública (Decreto Nº 1172/03); Ministerio del Interior; denuncia de Poder Ciudadano ante la Oficina Anticorrupción

2007

140: Acceso a la Información Pública (Decreto Nº 1172/03) - reingreso relacionado con Dictamen Nº 118/06 - Ministerio del Interior -(Fundación Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento - CIPPEC-).
141: Acceso a la Información Pública (Decreto Nº 1172/03) - Secretaría General de la Presidencia de la nación - Comisión Nacional Asesora para la Integración de Personas Discapacitadas (cargos y funciones del personal)
142: Acceso a la Información Pública (Decreto Nº 1172/03) - reingreso relacionado con Dictamen Nº 285/06 - Ministerio del Interior (Poder Ciudadano).
144: Acceso a la Información Pública (Decreto Nº 1172/03) - Ministerio del Interior (designación de personal).
145: Acceso a la Información Pública (Decreto Nº 1172/03) - Comité Federal de Radiodifusión (empleados, resoluciones, etc.)
153: Acceso a la Información Pública(Decreto N° 1172/03) – Comisión Nacional sobre la Desaparición de Personas (CONADEP)

2008

002: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de informes formulado por el Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (CIPPEC) al Ministerio de Desarrollo Social.
003: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de datos relativos a personal superior de la Policía Federal Argentina.
004: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de datos relativos a personal contratado del Ministerio de Justicia, Seguridad y Derechos Humanos.
005: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al Ministerio de Justicia, Seguridad y Derechos Humanos relativa a hechos relacionados con el paro agropecuario.
006: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de
información al Ministerio de Economía y Producción relativa a los
receptores/beneficiarios finales de diversos programas.
011: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al Ministerio de Justicia, Seguridad y Derechos Humanos sobre el monto asignado al señor Ministro y el listado de gastos efectuado.

014: Acceso a la Información Pública (Decreto Nº 1172/03); Solictud del listado completo de todos los registros otorgados en los últimos 12 meses por tenencia simple y portación de armas en todo el país, con el detalle de nombre, DNI y tipo de arma utilizada.
015: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información formulada al SERVICIO PENITENCIARIO NACIONAL relativa al número de personas nacionales o extranjeras privadas de la libertad.
018: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información relativa a actuaciones, sumarios, órdenes del día y dictámenes de la POLICÍA FEDERAL ARGENTINA.
019: Acceso a la Información Pública (Decreto Nº 1172/03) ; Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS relativa a investigaciones sobre estupefacientes.
021: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS relativa al número de solicitudes de conmutación de pena e indultos presentados a partir del 25.05.03, así como de los concedidos, en trámite, rechazados, devenidos abstractos y archivados.
024: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información a la SECRETARIA GENERAL de la PRESIDENCIA DE LA NACIÓN respecto del otorgamiento de subsidios.
029: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS respecto de transferencias a organizaciones sin fines de lucro y ayudas sociales a personas.
033: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS respecto de datos de un concurso de admisión para personal superior y subalterno de Gendarmería Nacional.
034: Acceso a la Información Pública (Decreto Nº 1172/03) – Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS; SERVICIO PENITENCIARIO FEDERAL, respecto de personas fallecidas en entre enero de 1990 y mayo de 2008 en Unidades penitenciarias de todo el territorio nacional.
035: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información formulada a la SECRETARÍA GENERAL de la PRESIDENCIA DE LA NACION - Inaplicabilidad de la Ley Nº 25.326.
037: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información formulada a la SECRETARÍA GENERAL de la PRESIDENCIA DE LA NACION relativa al sueldo de la Presidenta de la Nación.
038: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información al MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS; POLICIA FEDERAL ARGENTINA, requiriendo información sobre el eventual desembarco de submarinos alemanes en nuestro país al finalizar la
Segunda Guerra Mundial.

2009
003: Acceso a la Información Pública (Decreto Nº 1172/03) - solicitud de información respecto del secuestro del criminal de guerra nazi Adolf EICHMAN
004: Acceso a la Información Pública (Decreto Nº 1172/03) - solicitud de información respecto de personas que habrían sido detenidas por la Coordinación Federal en el año 1960, en razón de estar realizando investigaciones sobre los años 50 y 60 en la argentina.
005: Acceso a la Información Pública (Decreto Nº 1172/03) - solicitud de la nómina de los informes de auditorías emitidos por la Auditoría Interna del Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI) correspondientes a los años 2006, 2007 y 2008.
006: Acceso a la Información Pública (Decreto Nº 1172/03) - solicitud de la nómina del personal policial de la Policía Federal Argentina, con nombre y apellido y dependencia en la que prestara servicios, que hubieren sufrido un accidente durante los años 2007/2008.
007: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de la nómina y DNI de los estudiantes universitarios y de los cursos de extensión que se dictan en el Instituto de Detención Unidad Nº 2 Devoto que fueron trasladados a otras unidades durante 2008…".entre otros temas.
011: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información sobre la Licitación Pública Nº 9/2006 referida a la prestación de servicio de ambulancia para atención médica domiciliaria, de urgencias y emergencias para los afiliados a la obra social de la Policía Federal Argentina.
012: Acceso a la Información Pública (Decreto Nº 1172/03) - solicitud de información pública en relación a diversas organizaciones sociales.
014: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información acerca de la cantidad de denuncias recibidas y sumarios iniciados que involucren niños, niñas y adolescentes, ya sea desde su calidad de víctima o de imputado en relación a delitos sexuales o narcotráfico y denuncias de usurpaciones.
016: Acceso a la Información Pública (Decreto Nº 1172/03) Solicitud de información sobre el último concurso de oposición y antecedentes practicado en el Ministerio de Justicia, Seguridad y Derechos Humanos
023: Acceso a la Información Pública (Decreto Nº 1172/03) Solicitud de información formulada a la Oficina Anticorrupción.
025: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información requerida a la Jefatura de Gabinete de Ministros.
027: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de nómina del personal de la Administración Pública Nacional.

030: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información pública requerida al Ministerio de Defensa, respecto de la nómina de los ciudadanos militares, ex soldados conscriptos y civiles condecorados por el Congreso Nacional por haber luchado y combatido por la recuperación territorial de las Islas Malvinas, Georgias y Sandwich del sur.
032: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información pública respecto de todos los contratos celebrados entre dependencias, organismos descentralizados y empresas públicas dependientes de la Jefatura de Gabinete de Ministros y otras empresas.
033: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información a la Jefatura de Gabinete de Ministros acerca de la inversión publicitaria en pesos.
038: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información pública a la Jefatura de Gabinete de Ministros respecto de las transferencias en gastos corrientes realizadas a organizaciones sin fines de lucro.
039: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información pública a la Oficina Nacional de Contrataciones respecto de todas las contrataciones que celebró el Estado Nacional con un proveedor determinado.
040: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de información pública acerca de la distribución de la pauta oficial en medios gráficos locales requerida a la Secretaría de Medios de Comunicación.
041: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de acceso y extracción de copias certificadas de actuaciones administrativas que motivaron el dictado de la resolución del Comfer N° 763/09.
042: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de acceso a la información pública acerca de las campañas públicas realizadas durante el primer semestre del año 2009, requerida a la Secretaría de Medios de Comunicación.
046: Acceso a la Información Pública (Decreto Nº 1172/03); Solicitud de acceso a la información pública referida a las denuncias de recepción ilegal de radiofrecuencia audiovisual

2010
001: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Secretaría General de la Presidencia de la Nación.
003: Acceso a la Información Pública (Decreto Nº 1172/03) Solicitud de información efectuada a la Secretaría de Medios de Comunicación.
004: Acceso a la Información Pública (Decreto Nº 1172/03) Solicitud de información efectuada a la Jefatura de Gabinete de Ministros.
010: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información presentada ante la Oficina Anticorrupción.
013: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información presentada ante el Ministerio de Justicia, Seguridad y Derechos Humanos.
016: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Sistema Nacional de Medios Públicos.
019: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Oficina Nacional de Empleo Público.
023: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Jefatura de Gabinete de Ministros.
029: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Prefectura Naval Argentina.

2011
01: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Agricultura, Ganadería y Pesca.
004: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información presentada ante la Dirección Nacional de Protección de datos Personales.
009: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Desarrollo Social.
013: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información presentada ante el Ministerio de Justicia y Derechos Humanos.
014: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada ante el Ministerio de Justicia y Derechos Humanos.
015: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada ala Sra. Presidenta de la Nación.
020: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Secretaría General de la Presidencia de la Nación
021: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a RTA SE RADIO NACIONAL
022: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a CANAL 7
024: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a AEROLINEAS ARGENTINAS

025: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al BANCO CENTRAL DE LA REPÚBLICA ARGENTINA
026: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada Al MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

2012
001: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Economía y Finanzas Públicas
002: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Planificación Federal, Inversión Pública y Servicios
003: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio del Interior
004: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de la Jefatura de Gabinete de Ministros
005: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de la Jefatura de Gabinete de Ministros
006: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de la Jefatura de Gabinete de Ministros
007: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Inspección General de Justicia
010: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Educación
012: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Economía y Finanzas Públicas
014: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a Aerolíneas Argentinas
015: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Economía y Finanzas Públicas
016: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada al Ministerio de Economía y Finanzas Públicas

2013
001: Acceso a la Información Pública (Decreto Nº 1172/03) -
Solicitud de información efectuada a la Secretaría General de la Presidencia de la Nación.
003: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Jefatura de Gabinete de Ministros.
004: Acceso a la Información Pública (Decreto Nº 1172/03) - Solicitud de información efectuada a la Jefatura de Gabinete de Ministros.

Anexo II

Normativa y Marco normativo

La Ley de protección de datos personales cuenta con 14 reglamentaciones y 19 actualizaciones a saber:
-El Decreto 1558/2001, por medio de este se aprueba la reglamentación de la ley. “Sus principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.”
- La Disposición 1/2003, por medio de la cual se aprueba la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante las faltas que se comprueben.
- La Disposición 2/2003, por medio de la cual se habilita el Registro Nacional de Bases de Datos y se dispone la realización del primer censo nacional de bases de datos.
- La Disposición 1/2004, por medio de la cual se implementa con carácter obligatorio, el primer censo nacional de archivos, registros, bases o bancos de datos privados.
- La Disposición 2/2005, por medio de la cual se implementa el registro nacional de bases de datos alcanzadas por la ley 25326. Se establecen los plazos para la inscripción de los archivos, registros y bases de datos y los formularios para la inscripción.
- La Disposición 2/2005, por medio de la cual se aprueban los Formularios, Instructivos y Procedimientos que utilizará la Dirección Nacional de Protección de Datos Personales, en relación con la implementación del Registro Nacional de Bases de Datos.
- La Disposición 4/2005, por medio de la cual se prorroga la fecha de implementación del censo nacional de archivos, registros, bases o bancos de datos privados.
- La Disposición 4/2005, por medio de la cual se prorroga la fecha de implementación del registro nacional de bases de datos, y en consecuencia el vencimiento del plazo para la inscripción de los archivos, registros y bases de datos. 2/2005.
- La Disposición 7/2005, por medio de la cual se aprueban la "clasificación de infracciones" y la "graduación de las sanciones" a aplicar ante violaciones a las normas de la ley 25326 y de las reglamentaciones dictadas en su consecuencia. Asimismo, se deroga la disposición 1/2003 y se crea el registro de infractores a la ley 25326.
- La Disposición 1/2006, por medio de la cual se prorroga el plazo de vencimiento para la inscripción en el registro nacional de bases de datos, establecido en las disposiciones 2/2005 y 4/2005.
- La Disposición 1/2006, por medio de la cual se establece la publicación de los dictámenes de la Dirección Nacional en la página web de la dependencia
- La Disposición 10/2006, por medio de la cual se incorpora al registro, la inscripción de archivos, registros o bases o bancos públicos de datos personales pertenecientes a los entes públicos estatales no incluidos en la disposición 2/2006 y entes públicos no estatales, que se encuentren interconectados en redes de alcance interjurisdiccional, nacional o internacional.
- La Disposición 11/2006, por medio de la cual se aprueban medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicos no estatales y privados. Y se establece un plazo para la implementación de dichas medidas.
- La Disposición 6/2008, por medio de la cual se establece el Procedimiento de control en la ejecución de los formularios de consentimiento informado.
- La Disposición 7/2008, por medio de la cual se aprueban la guía de buenas prácticas en políticas de privacidad para las bases de datos del ámbito público y el texto modelo de convenio de confidencialidad.
- La Disposición 10/2008, por medio de la cual se establece que los responsables y usuarios de bancos de datos públicos o privados, deberán incluir en su página web y en toda comunicación o publicidad la leyenda que indique la facultad o la prohibición de ejercer el derecho de acceso a los mismos.
- La Disposición 9/2008, por medio de la cual se adoptan medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicos no estatales y privados. Asimismo se prorroga el plazo establecido por la disposición 11/2006.
- La Disposición 7/2010, por medio de la cual se crea el centro de asistencia a las víctimas de robo de identidad en el ámbito de la dirección nacional de protección de datos personales, el cual tendrá la función de asistir a las personas que hayan sido afectadas, desarrollar información sobre medidas de prevención y tomar las medidas necesarias para evitar que la acción fraudulenta continúe desarrollándose respecto de la misma persona.
- El Decreto 1160/2010, por medio de la cual se sustituye el inciso 3 del artículo 31 del decreto 1558/2001 sobre el procedimiento que se aplicará para aplicar las sanciones.

Actualizaciones:
- La Resolución 415/2003, por medio de la cual se crea el registro de huellas digitales genéticas, en el ámbito de la policía federal argentina.
- La Disposición 4/2004, por medio de la cual se homologa el código de ética de la asociación de marketing directo e interactivo de argentina (AMDIA). Esta atribución, de homologar códigos de conducta, se encuentra entre las asignadas a la Dirección.
- La Disposición 6/2005, por medio de la cual se aprueba el diseño del isologotipo que identificará a los responsables de bases de datos personales inscriptos en el Registro Nacional de Bases de Datos.
- La Disposición 2/2006, por medio de la cual se implementa el relevamiento integral de bases de datos personales del Estado Nacional.

- La Disposición 5/2006, por medio de la cual se implementa, el Registro Nacional de Protección de Datos Personales a los fines de la inscripción de los archivos, registros, bancos y bases de datos públicos alcanzados por la ley 25326.
- La Ley 26343, por medio de la cual se incorpora el artículo 47 que establece que los bancos de datos destinados a brindar servicios de de información crediticia deberán eliminar y omitir el asiento en el futuro de todo dato referido a obligaciones y calificaciones asociadas de las personas físicas y jurídicas cuyas obligaciones comerciales se hubieran constituido en mora, o cuyas obligaciones financieras hubieran sido clasificadas con categoría 2, 3, 4 ó 5, según normativas del Banco Central de la República Argentina, en ambos casos durante el período comprendido entre el 1º de enero del año 2000 y el 10 de diciembre de 2003, siempre y cuando esas deudas hubieran sido canceladas o regularizadas al momento de entrada en vigencia de dicha ley o lo sean dentro de los 180 días posteriores a la misma.
- La Disposición 1/2008, por medio de la cual se aprueba el diseño de los isologotipos que identificarán a los responsables de bases de datos inscriptos en el registro, que haya efectuado las renovaciones correspondientes a los años 2007 y 2008.
- La Disposición 2/2008, por medio de la cual se crea el Repertorio de Jurisprudencia sobre Habeas Data.
- La Disposición 3/2008, por medio de la cual se crea el Centro de Jurisprudencia, Investigación y Promoción de la Protección de los Datos Personales
- La Disposición 5/2008, por medio de la cual se aprueban las normas de inspección y control de la Dirección.
- La Disposición 12/2008, por medio de la cual se aprueba el diseño del isologotipo que identificará a los responsables de bases de datos personales inscriptos en el Registro que hayan efectuado la renovación correspondiente al año 2009.
- La Resolución 925/2008, por medio de la cual se aprueba la política de intercambio electrónico de información. Se adecua el suministro de los datos contenidos en las bases de la administración nacional de seguridad social (ANSES) a los términos y condiciones fijados en la ley 25326, y su reglamentación.
- La Disposición 4/2009, por medio de la cual se establece que la opción para el ejercicio del derecho de retiro o bloqueo contemplada en el artículo 27, inciso 3, de la ley 25326, deberá aparecer en toda comunicación que se efectué con fines publicitarios, junto con el mecanismo previsto para su ejercicio.
- La Resolución conjunta 627/2010, por medio de la cual se establece que los productores asesores de seguros deberán acreditar su inscripción como responsables de bases de datos personales ante el Registro Nacional de Bases de Datos Personales en cumplimiento de lo establecido por el artículo 1 de la ley 20091 y articulo 3 de la ley 25326.
- La Disposición 17/2010, por medio de la cual se establece el sistema informativo denominado "Base Informática para la Comunicación Electrónica Interjurisdiccional sobre Datos Personales en Información Crediticia" a través del cual se disponen las distintas novedades que afecten a los informes crediticios respecto de los derechos de rectificación, actualización, confidencialidad, supresión y/o bloqueo de datos personales.
- La Disposición 24/2010, por medio de la cual se crea el registro nacional de documentos de identidad cuestionados.
- El Decreto 1766/2011, por medio de la cual se crea el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS).
- La Resolución 13/2012, por medio de la cual se aprueban los Procedimientos Operativos Estándares (POE) del Comité de Ética de Investigación del Instituto Nacional Central Único Coordinador de Ablación e Implante (INCUCAI). Se encomienda al Comité de Ética en Investigación (CEI) del INCUCAI la implementación y actualización permanente de un registro de ensayos clínicos, con el objeto de sistematizar y poner en acceso público la información sobre los mismos.
- La Resolución 3/2012, por medio de la cual se aprueban el "formulario de inspección" y el "instructivo del formulario de inspección", con el fin de facilitar la determinación de los distintos tratamientos de datos que realizan los responsables y verificar si los mismos se ajustan a los principios y requisitos de licitud que establece la ley 25326, lo que permitirá a la Dirección Nacional de Protección De Datos personales efectuar las correcciones y recomendaciones que resulten necesarias para mejorar la gestión y la protección de los derechos del titular del dato. Se deroga la disposición 5/2008.

Caso de estudio chileno

Por Ximena Salazar

Introducción

El presente estudio apunta a describir el diseño institucional de las agencias encargadas de garantizar el derecho a saber y la protección de datos personales en el Chile. Para llevar a cabo esta tarea se trabajó con una metodología cualitativa que recogió información a partir de relevamiento bibliográfico y documental y a través de entrevistas a expertos en estos temas. El estudio fue realizado durante 2012.

1. Relevamiento de información

1.1 Breve referencia a la institucionalidad de acceso a la información pública en Chile.

Chile cuenta con una Ley específica y sistemática en materia de acceso a la información pública desde el año 2008. En efecto, mediante la Ley N° 20.285 o denominada "Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado"[90] (LAIP), nuestro país regula el derecho de acceso a la información pública. Esta ley, iniciativa de los Senadores Hernán Larraín y Jaime Gazmuri[91], apoyada por el Gobierno de la época, es el corolario de la política chilena en materia de acceso a la información pública. Varios hitos llevaron en la práctica la existencia de esta ley. Así, y como respuesta a una serie de hechos de corrupción, el año 1994 se crea la Comisión de Ética Pública, que realizó el "Informe sobre la Probidad y la Prevención de la Corrupción". Dentro de las recomendaciones, algunas de ellas se vieron plasmadas en la dictación y modificación de leyes, como la promulgación de la Ley N° 19.653 sobre Probidad Administrativa[92] que modifica la Ley N° 18.575, Ley Orgánica Constitucional de Bases Generales de la Administración del Estado (LOCBGAE), que – ente otra cosas – incorporó el principio de transparencia y la forma de acceder a la información poder de la Administración en su artículo 13. Sin embargo, pese a los esfuerzos y por la redacción del inciso final del artículo en comento, el año 2001 se dictó el Decreto Supremo N°26 desde el Ministerio Secretaría General de la Presidencia, que permitía que los Jefes de Servicios del Estado pudieran declarar por resoluciones exentas como secretos o reservados ciertos actos y documentos, con lo cual se creaban nuevas causales de reserva– reglamentarias y no legales- que permitían entorpecer el acceso a la información. Con esto los principios de transparencia y acceso a la información pública se transformaron en letra muerta.

Como consecuencia de las prácticas abusivas de la administración por mantener una cultura del secreto, fue considerado necesario incorporar un mandato constitucional de publicidad que fue plasmado mediante un reforma constitucional del año 2005[93], incorporando el artículo 8° de la Constitución Política de la República, en cuanto indica que "Son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquellos o de éstos, cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional".

Pero, será otro hito proveniente desde la jurisprudencia internacional, la que en la necesidad de incorporar medidas efectivas que permitan garantizar el acceso a la información en Chile, el que obligue al Estado de Chile a su regulación, como fue lo resuelto por la Corte Interamericana de Derechos Humanos en la histórica sentencia Claude Reyes y otros con Estado de Chile (2006), que condena al Estado de Chile precisamente por no garantizar este derecho. La sentencia es, además, una referencia interamericana e internacional del reconocimiento del derecho de acceso a la información pública.

Como consecuencia de lo anterior, y como indicara en lo resolutivo del fallo, Chile debía adoptar las medidas necesarias para garantizar el ejercicio del acceso a la información pública y para ello, el Gobierno de turno realizó indicaciones al proyecto en tramitación desde el año 2005, agilizándose la discusión de una política nacional sobre acceso a la información que se materializaría en la dictación de la Ley de Transparencia el año 2008 y la dictación de su Reglamento el año 2009[94].

[90] Publicada en el Diario Oficial el 20 de agosto de 2008. La ley entró en vigencia un año después, en agosto de 2009.
[91] boletín N° 3773-06, presentado el 4 de enero de 2005,
[92] Publicada en el Diario Oficial el 14 de diciembre de 1999.
[93] Ley N° 20.050, publicada en el Diario Oficial el 26 de agosto de 2005.
[94] Aprobado por el Decreto Supremo N° 1 del Ministerio Secretaría General de la Presidencia.

1.1.1 Contenido de la Ley N° 20.285 o "Ley de Transparencia"[95]

La Ley de Transparencia, se encuentra dividida en 7 Títulos o Capítulos. El Título I llamado "Normas Generales", indica los objetivos y algunas definiciones que tendrán que tenerse presente. En su artículo 1°, la Ley señala la finalidad esto es, *"La presente ley regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información"*. En breve, esto significa la regulación de la transparencia de la función pública en cumplimiento del mandato constitucional del artículo 8° de la Constitución, procedimientos para acceder a ella y las excepciones de publicidad o causales de reserva.

Luego, indica cuales son los sujetos obligados a las normas de Transparencia (artículo 2°), para luego precisar cuál es el sentido del ejercicio de la función pública, esto es en palabras de la ley *"La función pública se ejerce con transparencia, de modo que permita y promueva el conocimiento de los procedimientos, contenidos y decisiones que se adopten en ejercicio de ella".* En consonancia con lo anterior, la ley establece un mandato general de sujeción a la transparencia en todas sus actuaciones por parte de todas las autoridades y funcionarios de la Administración del Estado – independiente de su denominación-en ejercicio de funciones públicas (artículo 4°). Luego, la ley precisa qué entender por éste principio de transparencia de la función pública, indicando que "*consiste en respetar y cautelar la publicidad de los actos, resoluciones, procedimientos y documentos de la Administración, así como de sus fundamentos, y en facilitar el acceso de cualquier persona a esta información, a través de los medios y procedimientos que al efecto establezca la ley"* (Segunda parte artículo 4°).

En cuanto a los sujetos obligados que deben dar cumplimiento a las normas de la Ley N° 20.285, cabe precisar que existe un régimen diferenciado de aplicación de las disposiciones que estable la ley[96], puesto que no todos las organismos públicos que constituyen la "Administración del Estado" - de acuerdo a lo indicado en el artículo 1° inciso segundo de la LOCBGAE – resultan ser sujetos obligados por la Ley de Transparencia, o le son aplicables de manera diferenciada, siguiendo un criterio orgánico, por lo que cabe distinguir tres niveles[97], a saber:

a) <u>Régimen general de transparencia</u>

En este grupo se encuentran todos aquellos organismo del Estado que indica el artículo 2° de la Ley de Transparencia, esto es, Ministerios, Intendencias, Gobernaciones, Gobiernos Regionales, Municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios creados para el cumplimiento de la función administrativa, los cuales quedan sujetos a la mayoría de las disposiciones de la Ley 20.285, esto es, sujetos a las normas de derecho de acceso a la información, normas de transparencia activa y pasiva, régimen de sanciones, competencia del Consejo para la Transparencia, aplicación de las causales de reserva de la información.[98]

Con la enumeración anterior, quedan excluidos de éste régimen (aquellos indicados en el artículo 1° de la Ley N° 18.575 LOCBGAE), la Contraloría General de la República, el Banco Central y las empresas públicas creadas por Ley, las empresas del Estado, las sociedades con participación estatal de más del 50%.

Quedan, además, excluidos aquellos organismos que no forman parte de la Administración del Estado, como son el Congreso Nacional, Poder Judicial (tribunales ordinarios y especiales y los demás que ejercen jurisdicción), el Ministerio Público, el Tribunal Constitucional, el Tribunal Calificador de Elecciones y los Tribunales Electorales Regionales.

Respecto de cada uno de ellos, hay que distinguir distintos niveles de cumplimiento de obligaciones de Transparencia que se analizan a continuación.

b) <u>Régimen de aplicación restringida de las normas de Transparencia</u>

En este grupo se encuentran aquellos organismos denominados "Constitucionalmente Autónomos", como son la Contraloría General de la República, el Banco Central y el Ministerio Público.

---

[95] En adelante LAIP.

[96] Para un análisis más detallado de las razones del régimen diferenciado, véase FERRADA B. Juan Carlos. El ámbito de aplicación de la Ley de Transparencia, en LETELIER, Raúl y RAJEVIC, Enrique coordinadores. Transparencia en la Administración Pública. Chile. Editorial Abeledo Perrot. 2010. P. 347 y ss.

[97] Tello Cristóbal, Marcelo Cerna y Andrés Pavón." Acceso a la información pública: los desafíos del Consejo de la Transparencia". Disponible en http://www.anuariocdh.uchile.cl/index.php/ADH/article/viewFile/11528/11887 (Septiembre 2012).

[98] Ob. Cit.

Respecto de este grupo, solamente resultan aplicables aquellas disposiciones que la propia Ley de Transparencia expresamente indica. Se excluyen, además, de la competencia del Consejo para la Transparencia.

En la práctica, los artículos 5º, 7º y 9º de la LAIP hacen aplicables a estos órganos: el principio de transparencia (artículos 3º y 4º LT); "en lo que fuere pertinente", las normas que regulan el concepto de información pública (Título II LT); el deber de transparencia activa (artículos 7º y 9º LT); los principios del derecho de acceso a la información pública (artículo 11 LT), las causales legales de secreto o reserva de la información (artículo 21 LT), la duración de dicho secreto o reserva (artículo 22 LT) y el procedimiento para la solicitud de información (artículos 10 a 22 LT); pero les somete a un procedimiento especial para el reclamo por la denegación del acceso a la información ante las Cortes de Apelaciones, excluyéndolos de la competencia del Consejo para la Transparencia".[99]

c) Régimen especial de Transparencia Activa

Como se analizará más adelante, un "tipo" de ejercicio de Transparencia corresponde a las obligaciones de la denominada "Transparencia Activa", esto es, *"[mantener a disposición permanente del público, a través de sus sitios electrónicos...]"* (artículo 7°), indicando una serie de antecedentes.

A obligación quedarán sometidos el Poder judicial, el Congreso Nacional[100], las empresas estatales o en aquellas que el Estado sea accionario por más del 50%.

Además, luego del control de constitucionalidad de la Ley de Transparencia llevada a cabo por el Eximo. Tribunal Constitucional (Rol 1.051-08), son sujetos obligados en ésta materia el propio Tribunal Constitucional y los Tribunales que conforman la Justicia Electoral.

Siguiendo con la estructura de la Ley 20.285, en el Título II denominado "De la publicidad de la Información de los Órganos de la Administración del Estado" la ley en su artículo 5° indicará cuales son las distintas materias que se pueden solicitar, resultando clave para la extensión y alcance de las materias que deben entregar en virtud de una solicitud de acceso a la información o publicarse en los sitios web de los organismos. El criterio es amplio y es cita obligada en las decisiones del Consejo para la Transparencia, pero no es pacífico en la jurisprudencia constitucional puesto que en dos ocasiones recientes ha sido declarado inconstitucional el inciso segundo del artículo 5° por ser contrario a lo indicado en el artículo 19 N° 4° y 5° de la Constitución Chilena[101],que protege la vida privada y la inviolabilidad de las comunicaciones[102], a propósito de la decisión del Consejo sobre la entrega de antecedentes de los concursos de la Alta Dirección Pública regulados por la ley N° 19.882 y en un segundo caso sobre la publicidad de los correos electrónicos del Subsecretario del Interior.[103]

La norma en cuestión indica que "*En virtud del principio de transparencia de la función pública, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo o esencial, y los procedimientos que se utilice para su dictación, son públicos salvo las excepciones que establece esta ley y las previstas en otras leyes de quórum calificado.*

Asimismo, es pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, a menos que esté sujeta a las excepciones señaladas".

El Título III de la Ley N° 20.285, comienza con las hipótesis de las denominadas "Transparencia Activa y Transparencia Pasiva". Así, en su artículo 7°, indica la obligación de todos los órganos indicados en el artículo 2° de la Ley, de mantener a

[99] Ob. cit.
[100] Respecto del Congreso Nacional, siéndole aplicables las normas de Transparencia Activa y otras pertinentes que la Ley expresamente indique, por medio de la Ley N° 20.447, modificatoria de la Ley Orgánica Constitucional del Congreso Nacional N° 18.918, se estableció la posibilidad de realizar solicitudes de acceso a la información. Asimismo, el Senado modificó su Reglamento con lo que en un procedimiento distinto al consagrado en la Ley de Transparencia, se estableció el deber del Secretario General dar o no acceso a la información requerida, siendo la entidad de apelación de reclamación última, la Comisión de Ética y Transparencia del Senado. Las causales de reserva de información son las mismas a las del artículo 21 de la Ley de Transparencia, siendo agregada por la Ley N° 20.447 (artículo 5° inciso 8°), la reserva de los registros de Secretarías de las comisiones y comités parlamentarios (como apuntes, grabaciones, u otros), lo que no son públicos.
[101] Artículo 19° N° 4° CPR: "La Constitución asegura a todas las personas: Art. 4°: EL respeto y protección de la vida privada y a la honra de la persona y su familia. Art. 5°: La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.
[102] STC 1990-11 INA caratulada "Servicio Civil con Consejo para la Transparencia".
[103] STC 2153-11 INA caratulada "Subsecretaría del Interior con Consejo para la Transparencia".

disposición permanente del público una serie de antecedentes que indica. Tal obligación como se analizará posteriormente, es una de las primeras normas relacionadas con datos personales que contiene la Ley, puesto que en su enumeración letra d) indica la obligación de publicar *"La planta del personal y el personal a contrata y a honorarios, con las correspondientes remuneraciones"*, por lo tanto, se debe publicar tanto el nombre completo de la persona que presta servicios al Estado como sus remuneraciones mensuales. En el mismo sentido, la letra i) indica la obligación de publicar "*El diseño, montos asignados y criterio de acceso a los programas y subsidios que entregue el respectivo órgano, además de las nóminas de beneficiarios de los programas sociales en ejecución. No se incluirán en estos antecedentes los datos sensibles, esto es, los datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opciones políticas, las creencias o convicciones religiosa, los estados de salud físicos o psíquicos o la vida sexual.* [104]

El no dar cumplimiento de estas obligaciones, da derecho a cualquier persona interponer una reclamación ante el Consejo para la Transparencia (artículo 8°).

Luego, en el Título VI, denominado "Del derecho de Acceso a la Información de los Órganos de la Administración del Estado" entre los artículos 10° a 30° se regula el procedimiento de acceso a la información, complementado con las disposiciones reglamentarias de los artículo 10°a 37° así como de la Instrucción N° 10, de reciente entrada en vigencia (Marzo 2012) sobre "Procedimiento Administrativo de Acceso a la Información".

Principalmente se indica la posibilidad de solicitud de información por cualquier persona (artículo 10) sin expresión de causa o condicionada al uso posterior de la información y – en general- respecto del acceso a cualquier información con exclusión de las excepciones legales (que se traducen en la aplicación de las causales de reserva, documentos declarados como secretos o reservados, entre otros. A la vez, consagra una serie de principios, a saber: a) Principio de la relevancia, conforme al cual se presume relevante toda la información que posean los órganos de la Administración del Estado, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento, b) Principio de la libertad de información de acuerdo al que toda persona goza del derecho de acceder a la información que obre en poder de los órganos de la Administración del Estado, con las solas excepciones o limitaciones establecidas por leyes de quórum calificado, c) Principio de apertura o transparencia, conforme al cual toda la información en poder de los órganos de la Administración del Estado se presume pública, a menos que esté sujeta a las excepciones señaladas, d) Principio de máxima divulgación, de acuerdo al que los órganos de la Administración del Estado, deben proporcionar información en los términos más amplios posibles, excluyendo sólo aquellos que esté sujeto a las excepciones constitucionales o legales, e) Principio de divisibilidad, conforme al cual si un acto administrativo contiene información que puede ser conocida e información que debe denegarse en virtud de causa legal, se dará acceso a la primera y no a la segunda, f) Principio de la facilitación, conforme al cual los mecanismos y procedimientos para el acceso a la información de los órganos de la Administración del Estado deben facilitar el ejercicio del derecho, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo, g) Principio de la no discriminación, de acuerdo al que los órganos de la Administración del Estado, deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivo para la solicitud, h) Principio de la oportunidad, conforme al cual los órganos de la Administración del Estado, deben proporcionar respuesta a las solicitudes de información dentro de los plazos legales, con la máxima celeridad posible y evitando todo tipo de trámites dilatorios, i) Principio de control, de acuerdo al que el cumplimiento de las normas que regulan el derecho de acceso a la información será objeto de fiscalización permanente, y las resoluciones que recaigan en solicitudes de acceso a la información son reclamables ante un órgano externo, j) Principio de la responsabilidad, conforme al cual el incumplimiento de las obligaciones que esta ley impone a los órganos de la Administración del Estado, origina responsabilidades y da lugar a las sanciones que establece la ley y finalmente k) principio de gratuidad, de acuerdo al cual el acceso a la información de los órganos de la Administración es gratuito, sin perjuicio de lo establecido en esta ley.

A la vez, éste título indica los requisitos de toda solicitud de acceso a la información (artículo 12), plazos de entrega de información (20 días prorrogables por otros 10 excepcionalmente, artículo 14), obligación de entrega de la información (artículo 16), salvo que aplicación de las causales de reserva, forma de entrega de información que será de acuerdo a lo indicado por el solicitante (artículo 17), exigencia de pago por la entrega de la información que una ley haya indicado (artículo 18)[105], procedimiento especial de oposición de terceros eventualmente afectados por la entrega de la información (artículo 20)[106].

[104] Cabe destacar que ambas obligaciones de transparencia activa tienen un desarrollo mayor sobre el qué publicar en la Instrucción N° 4° del Consejo para la Transparencia sobre Transparencia Activa en ejercicio de la atribución que le confiere el artículo 33 letra d) de la Ley de Transparencia.

[105] Tener presente que el Consejo para la Transparencia por medio del Instructivo N° 6 "Sobre Gratuidad y Costos Directos de Reproducción" estableció la forma, costos promedios y manera en que la autoridad debe publicar la información asociada a los eventuales costos por acceder a la información, como fotocopias, escaneo de documentos, etcétera.

[106] Sobre este punto, se analizará más adelante este procedimiento por estar relacionado como una forma de hacer valer el derecho de terceros de proteger sus datos personales.

Luego, la ley indicará las causales de secreto o reserva por medio de las cuales la autoridad requerida puede negar total o parcialmente el acceso a la información. Estas causales – más desarrolladas en la Ley de Transparencia- son las mismas que aquellas que por medio de una ley de quórum calificado pueden declarar como secreto o reservado cierta información, esto es "*cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional"* indicadas en el artículo 8° inciso segundo de la Constitución Política de Chile[107].

El artículo que comento expresamente señala estas causales, así:
Artículo 21: Las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes:

> *1. Cuando su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente:*
>
> *a) Si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales.*
>
> *b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas.*
>
> *c) Tratándose de requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales.*
>
> *2. Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.*
>
> *3. Cuando su publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública.*
>
> *4. Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.*
>
> *5. Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política.*

De las causales anteriores, la que nos importa para efectos de relacionar la tensión entre el acceso a la información con la protección de datos personales, resulta ser la del N° 21 N° 2, esto es, afectación de los derechos de las personas, que será analizada posteriormente.

Siguiendo con el procedimiento de acceso a la información, continúa la norma indicando aquellos documentos que se mantendrán en secreto o reservados que una ley de quórum calificado así lo haya indicado, en relación a ciertas materias y por un determinado plazo(artículo 22), para finalmente indicar el derecho que le asiste a toda persona requirente de información de acudir ante el Consejo para la Transparencia en amparo de su derecho de acceso a la información (como una garantía del derecho fundamental de acceso a la información pública) cuando la entidad requerida no ha dado respuesta al requerimiento, ha hecho entrega incompleta de la información o la deniega (artículos 24 y siguientes), para finalizar el título IV indicando el recurso especial de reclamación ante la Corte de Apelaciones respectiva remedio procesal frente a una decisión del Consejo que ordena o deniega la entrega de la información.

El Título V, denominado "Del Consejo para la Transparencia" (artículos 31° a 44°) indicará la creación de un órgano especializado encargado de promover, fiscalizar, garantizar y sancionar el cumplimiento de las normas de transparencia y publicidad del Estado. Indicará éste título, todo lo referente a su parte orgánica, funcional y administrativa, que serán analizadas con más detalle más adelante.

Finaliza la Ley con su Título V, denominado "Sanciones", donde radican las funciones sancionatorias que puede ejercer el Consejo para la Transparencia contra las autoridades o servicios que no han dado cumplimiento a las normas de transparencia y publicidad, por medio de la sumario administrativo[108], que puede terminar con

[107] Con esto, queda prohibido por mandato constitucional, establecer causales de secreto o reserva de manera reglamentaria como se autorizara anteriormente por medio de D.S. N° 21 de 2001, como se explico en la primera parte de este informe.
[108] La instrucción de sumarios pueden ser consultados en el sitio web del Consejo para la Transparencia, disponible en http://www.cplt.cl/actos-y-resoluciones-con-efectos-sobre-terceros/consejo/2009-04-08/125721.html#T7.

sanciones[109] pecuniarios a los jefes del servicio (descuento de remuneraciones de entre el 20 a 50 %) u otras, como suspensión del cargo por el plazo de 5 días.

1.2 Régimen chileno de protección de datos de carácter personal

Nuestra Constitución Política de la República[110], vigente desde 1980, reconoce en su artículo 19 N° 4 que: *La Constitución asegura a todas las personas: "El respeto y protección a la vida privada y a la honra de la persona y su familia"*; continúa en el numeral N° 5 que garantiza "*La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar solo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".* En nuestro derecho, parte de la doctrina entiende la protección de la vida privada como una manifestación de la dignidad, sin perjuicio que los tribunales, no han realizado una construcción parecida a la del Tribunal Federal Alemán como en el caso de la Ley Federal de Censo de 1983 en que (en conjunto con el artículo 1° de la CPR), respecto la Ley Federal de Censo en 1983 en que…. "Para una parte de la doctrina nacional, la vida privada puede ser definida como "*la posición de una persona o entidad colectiva personal en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su integridad corporal o psicológica o a las relaciones que ella mantiene o ha mantenido con otros por parte de agentes externos que, sobre la base de una valoración media razonable, son ajenos al contenido y finalidad de dicha interioridad o relaciones"*[111].

Por otra parte, el tratadista Alejandro Silva Bascuñán, ha indicado que la finalidad de la norma es "*lo que pretende este precepto es colocar, en una sola forma, no solo dos garantías, la inviolabilidad del hogar y la de la correspondencia, sino también la afirmación genérica- que puede tener enormes consecuencias en el orden jurídico- de todo lo relativo al santuario íntimo de la persona, como son el respeto a su propia intimidad, a su propio honor"*[112].

Por su parte, la Corte de Apelaciones de Santiago (CAS), en un fallo de primera instancia ha indicado que "*…es menester precisar que la vida privada se entiende aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento, mientras que por vida pública, comprende aquella que llevan los hombres públicos y de la que conocen los terceros, aun sin su consentimiento, siempre que sean de real trascendencia"*[113].

Como se aprecia, el articulado constitucional refunde- en breve- varios derechos como el derecho a la honra tanto de la persona como de su familia, inviolabilidad de la correspondencia y toda forma de comunicación privada, lo cual resulta desafortunado, puesto que se trata de situaciones distintas. De la misma manera, ha correspondido a los tribunales la delimitación de qué se entiende por vida privada finalmente[114].

1.2.1 Tratamiento reciente del Tribunal Constitucional respecto a la Privacidad[115]

En una reciente Sentencia, nuestro Tribunal Constitucional ha precisado el alcance de la privacidad indicando en primer lugar que *"el respeto y la protección de la dignidad y de los derechos a la privacidad de la vida y de las comunicaciones, son base esencial del desarrollo libre de la personalidad de cada sujeto, así como de su manifestación en la comunidad a través de los grupos intermedios autónomos con que se estructura la sociedad"*[116] para continuar intentando definir el concepto de privacidad diciendo *"Que el derecho a la privacidad entendido por nuestro constituyente como la posición de una persona o entidad colectiva personal en virtud de la cual se encuentra libre de intromisiones o difusiones cognoscitivas de hechos que pertenecen a su interioridad corporal o psicológico a las relaciones que ella mantiene o ha mantenido con otros, por parte de agentes externos, que sobre la base de una valoración media razonable, son ajenos al contenido y la finalidad de dicha interioridad o relaciones"*[117] . Así mismo, ha resaltado igual que con otros derechos fundamentales, que no resultan ser absoluto,

---

[109] Las sanciones impuestas por el Consejo para la Transparencia pueden ser revisadas en http://www.cplt.cl/actos-y-resoluciones-con-efectos-sobre-terceros/consejo/2009-04-08/125721.html#T9.

[110] En adelante CPR.

[111] VIVANCO, Ángela. Curso de Derecho Constitucional. Editorial Jurídica de Chile. Tomo II, pág. 345.

[112] BASCUÑAN SILVA, Alejandro. Sesión 129 de la Comisión de Estudios de la Nueva Constitución. En CUADRA, Enrique. Los Derechos Constitucionales. Tomo I. Tercera Edición. Página 213.

[113] SCA. Revista de Derecho y Jurisprudencia, Tomo XC, N°2, año 1993, segunda parte sección 5ª, Considerando. 7º, pág. 164-174.

[114] Como indica Pedro Anguita, la Comisión de Estudios de la nueva Constitución dedico un breve periodo a la discusión del articulado en comento, sin entrar a definir lo que se entendería por vida privada, dado que las agresiones podrían ser múltiples, razón por la cual se opta por una versión sintética que más bien parece un principio que una regla, según el autor. ANGUITA, Pedro. "Jurisprudencia Constitucional sobre el Derecho a la propia imagen y a la vida privada en Chile (1981-2004). Chile. Ediciones Universidad Diego Portales...2009.

[115] Con más detalle en CARMONA S., Carlos y NAVARRO B. Enrique, editores. Recopilación de Jurisprudencia del Tribunal Constitucional (1981-2011). Chile. Colección Conmemoración 40 años del Tribunal Constitucional (1971-2011). Cuadernos del Tribunal Constitucional, N° 45 año 2011.

[116] Considerando 21 STC Rol N° 389-03

[117] Considerando 38º STC Rol N° 1.683-10 INA.

puesto que *"el carácter no absoluto de los derechos fundamentales, es decir, aquellos que están reconocidos en el ordenamiento jurídico positivo, nacional e internacional. Es así como los derechos fundamentales pueden estar afectos a límites inmanentes o intrínsecos, dado que por su naturaleza (como el derecho a la libertad personal que no puede invocarse por las persona jurídicas) o a los límites extrínsecos, que se imponen por el constituyente o el legislador, en atención a la necesidad de preservar ciertos valores vinculados a intereses generales de la colectividad (la moral, la seguridad nacional, el orden público, la salubridad pública) o la necesidad de proteger otros derechos que representan valores socialmente deseables (por ejemplo, el derechos a vivir en medio ambiente libre de contaminación)"*[118]. Finalmente, ha enfatizado *que "la privacidad en sus varios rubros, por integrar los derechos personalísimos o del patrimonio moral de cada individuo, merecen reconocimiento y protección excepcionalmente categóricos tanto por la ley, como también por los actos de autoridad y las conductas de particulares o las estipulaciones celebrados antes éstos"*[119]

Con ese criterio, nuestro Tribunal Constitucional hace referencia a la noción de dejar fuera de conocimiento de terceros aspectos de la vida privada que son propiamente parte de su derecho a la personalidad. Se trata en definitiva de impedir una especie de instrumentalización del individuo. En el derecho español, por ejemplo, es parte de este derecho a la personalidad, entendido como diverso a la vida privada, el de protección a los datos personales. Lo anterior se traduce en una doble garantía: por una parte, permite el desarrollo libre de las personas, pero por otra parte, exige una demanda de protección del sector público.

1.2.2Protección de datos personales ¿Derecho Fundamental en el Derecho Chileno?

En nuestro catalogo de derechos en la Constitución, no se hace referencia a un denominado "derecho fundamental de protección de datos personales" como vimos que sí se ha realizado en países extranjeros, por lo tanto, cualquier alusión a él, necesariamente pasará por *"asegurar el respeto a la vida privada"* consagrado en el artículo 19 Nº4 de nuestra Carta Fundamental.

Sin embargo, existió en nuestro país una iniciativa que pretendía elevar a rango constitucional este derecho como diverso a la vida privada[120], bajo el fundamento que hemos venido hablando anteriormente y que motiva en realidad el surgimiento de todo un desarrollo bastante específico de un derecho fundamental, como es la posibilidad de la tecnología de ingresar a aquella esfera íntima de las personas y el tratamiento automatizado que pueda permitir una vigilancia constante de parte de cualquier persona o del Estado respecto de otra, que dé paso para incurrir en las más diversas formas de discriminaciones, atentados a la seguridad, afectación de otros derechos fundamentales como la libertad entre otros. Así, el citado proyecto, indica que *"resulta insoslayable que el contacto permanente de las personas con sus semejantes al interior de la comunidad social de la cual forma parte, así como todos aquellos avances tecnológicos que se han ido desarrollando en la sociedad, han ido transgrediendo aquellos ámbitos que forman parte de la intimidad personal"*. Por otra parte, y en lo que vimos en la evolución histórica de protección de datos, consagra un reconocimiento constitucional de una serie de principios básicos en materia de protección de datos personales, como son el principio de consentimiento, finalidad en el tratamiento de datos y los denominados derechos ARCO (acceso, rectificación, actualización y cancelación). En este sentido el proyecto recoge la segunda gran idea que debiera estar contemplada paralelamente a un reconocimiento como es asegurar mecanismo de protección, instrumentos que permitan controlar la información.
Así, considerado "*Se impone entonces, una concepción más dinámica y abierta, que permita la relación armónica de las nuevas tecnologías -absolutamente necesarias para el actual desarrollo humano- lo que implica el reconocimiento no sólo de un derecho, sino que de nuevos instrumentos de protección, por lo que se hace indispensable su incorporación en sede constitucional"*. Cita al respecto una serie de otros países que ya tienen integrado dentro de su catálogo de derechos un reconocimiento propio como es el caso de Portugal en su artículo N° 35[121] (primer país en reconocerlo) España en el artículo N° [122]18.4 (1978). En nuestro continente, países como Perú en su reforma a la Constitución de2005 en su artículo N° 2.6[123], Venezuela en el artículo 40[124], Colombia[125], Ecuador[126], Guatemala[127], Nicaragua[128], México[129].

---

[118] Considerando N° 25° STC Rol N° 1.365-09.
[119] Considerando N° 20°, STC Rol N°521-06
[120] Boletín N° 5.883-07 que "Modifica el artículo 19 N° 4 de la Carta Fundamental, con el objeto de consagrar como garantía constitucional, la protección de los datos personales y su resguardo legal".
[121] Artículo N° 35 Constitución Portuguesa. "Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ello y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. En el apartado 2 indica que ""No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe, religiosas o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos"."
[122] Artículo N° 18.4 Constitución Española: "La ley limitará el **uso de la informática** para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"; y en su artículo 105 b) indicará 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 la persona".
[123] Artículo 2.6 de la Constitución de Perú: "toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".
[124] Artículo 40 de la Constitución Bolivariana: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática".

El proyecto, en su artículo único indica que "Toda persona tiene derecho a la protección de sus datos personales, los que deben ser tratados para fines concretos y específicos, con su propio consentimiento, o en virtud de otro fundamento contemplado en la ley, y tendrá asimismo, derecho a acceder a dichos datos, para obtener su rectificación, actualización o cancelación, según procediere. Una ley orgánica constitucional establecerá las normas para la debida aplicación de este derecho, como asimismo el órgano autónomo que velará por el cumplimiento de dicha ley y controlará su aplicación." Sigue estando en tramitación desde el año 2008, sin cambios posteriores.

1.2.3 ¿Habeas data Constitucional en el Derecho Chileno?

El Habeas data[130] constituye un poder de disposición de parte de las personas para conocer los datos que manejan otros respecto de ellos. Se ha dicho que es "*el conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables*"[131]. Constituye pues una disposición, una facultad de proteger los derechos de las personas a acceder a informaciones sobre sí mismo, en cualquier tipo de mecanismo de procesamiento de datos, automatizado o manual, físico o digital, para que puedan ser revisados e incluso cancelados en caso de ser incorrectos. Se trata de un derecho de reacción por parte de las personas en atención a conocer efectivamente qué, cuánto, por qué y para qué conocen otros información sobre sus datos. Constituye una garantía en un sistema democrático a participar en contra del procesamiento de datos que puede llevar a cabo otro o el mismo Estado, de ahí su denominación como una "autodeterminación informativa". Algunos autores, ponen cuidado en no considerar que las personas tengan un derecho de propiedad absoluto y definitivo de sus datos, puesto que debe ser entendido en el sentido de alcanzar un conocimiento cierto y veraz del procesamiento de éstos[132].

Países como Portugal (1976), España (1978), Países Bajos (1983), Suecia (1990), Hungría (1987), Brasil (1988), Colombia (1991), Paraguay (1992), Perú (1993), Argentina (1994) han constitucionalizado esta acción en sus respectivas cartas fundamentales. A nivel internacional, encuentra reconocimiento si bien no en normas Constitucionales, sí en importantes instrumentos internacionales como el Convenio 108 del Consejo de Europa (art. 5), Parlamento Europeo a través de la "Declaración de Derechos y Libertades Fundamentales" de 1989, la Directiva 45/96 a la que ya hemos aludido, entro otros.

Doctrina autorizada en la materia como el profesor Humberto Nogueira, ha indicado varios argumentos para incluirla dentro de nuestra Constitución de 1980, así permite impedir una desnaturalización o limitación respecto de cualquier acto de autoridad, sea cual sea, que afecte el núcleo del derecho, puesto que cualquier limitación a derechos fundamentales supone identificar la realidad a la que alude y determinar el tratamiento jurídico contenido en el precepto que reconoce, siendo los límites de carácter intrínsecos[133]. Las consecuencias que trae para el autor

---

[125] Artículo 20 de la Constitución Colombiana: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlo y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

[126] Artículo 94 de la Constitución Ecuatoriana de 1998:"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito".

[127] Artículo 31 de la Constitución de Guatemala: "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepción los propios de las autoridades electorales y de los partidos políticos".

[128]Artículo 26 de la Constitución de Nicaragua "Toda persona tiene derecho: a su vida privada y la de su familia, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo; a conocer toda información que sobre ella hayan registrado las autoridades estatales, así corro el derecho de saber por qué y con qué finalidad tiene esa información".

[129] Artículo 16 de la Constitución Federal Mexicana: "Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y, en su caso, obtener su rectificación, cancelación o destrucción en los términos en que fijen las leyes"

[130] Hay autores que defienden el habeas data como una acción al habeas corpus (Acción Constitucional de Amparo en nuestro Derecho), que en lugar de "traer el cuerpo" (habeas corpus), se trata de "traer los datos". Así, SAGÜES, Néstor. El habeas data: alcances y problemática, En SANCHEZ, Alberto. El Derecho Público actual. Homenaje al Prof. Dr. Pablo Ramella y otros. Buenos Aires. 1994, página 179. En CHIRINO SÁNCHEZ, ob cit. p 219.

[131] PEREZ LUÑO, Enrique. Los Derechos Humanos en la sociedad Tecnológica. Página 139. En NOGUEIRA ALCALA, Humberto. Reflexiones sobre el establecimiento constitucional del habeas data y el proyecto en tramitación parlamentario sobre la materia. En Revista Ius et Praxis de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca. Año 3 N°1, página. Editorial Universidad de Talca, Talca, Chile, 1997. Página 266.

[132] CHIRINO SÁNCHEZ, Alfredo y otro. El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica. En CANALES GIL, Álvaro y otros Coordinadores. Protección de datos de carácter personal en Iberoamérica. II Encuentro Iberoamericano de protección de datos, La Antigua-Guatemala, 2-6 de Junio de 2003. Valencia. Tirant Lo Blanch. 2006. Página 220.

[133] Ob. cit. página 276.

esta inclusión en la Constitución son: 1) Limitaciones deben proceder de la propia Constitución 2) Limitaciones sólo deben ser por ley 3) Actos que limiten derechos deben ser motivados 4) Toda limitación pasa a ser eventualmente controlable por organismos internacionales 5) Limitaciones interpretadas restrictivamente 6) Aplicación del principio de proporcionalidad 7) Respecto del contenido esencial del derecho por parte de las limitaciones 8) Deben adoptarse aquellas medidas menos gravosas para el derecho 9) El derecho de habeas data sólo podría ser modificado, jamás cancelado 10) Obligación jurisdiccional del juez inmediata.

Por el contrario, y en doctrina internacional, hay quienes[134] manifiestan su índole procesal constitucional, ya que la acción dependería de los tribunales. Se refiere principalmente a la panorámica latinoamericana, que como vimos, ha aceptado en su mayoría esta acción como constitucional. Así, en Europa el acento está puesto más bien en el carácter preventivo para proteger *ex ante* de daños en el tratamiento de datos. En Estados Unidos, se ha optado por un modelo de acciones tutelares individuales. El acento correcto para los autores, está en considerar la acción no como un proceso pensado bajo la lógica de una sanción en caso de daño, sino en la prevención, única forma de lograr el máximo desarrollo de la libertad y personalidad, pero entendido como un plan de vida de los ciudadanos (un *"estatus civitatis"*[135]*).*

En nuestro país la acción de habeas data no tiene reconocimiento constitucional, sino que sólo legal, como sucede en el artículo 12 de la ley N° 19.628 sobre Protección de la vida privada[136]. Sin embargo, actualmente se encuentra en tramitación su inclusión en la Constitución a través de los proyectos posteriores que modifican la Ley N° 19.628 (Boletines N° 6704-07 y –N° 8143-03), y de la moción parlamentaria (Boletín N° 6495-07) presentada por Senador Jaime Pizarro.[137].

1.2.4 La Ley 19.628 sobre protección a la Vida privada y datos de carácter personal[138]

Chile no podía quedarse atrás en la regulación de datos personales, siendo el primero que lo reguló a nivel Latinoamericano con la publicación de Ley N° 19.628 "sobre Protección de la vida privada y protección de los datos de carácter personal" publicada en el Diario Oficial el 28 de agosto de 1999, con vigencia después de un periodo de vacancia de 60 días. El origen estuvo en una moción parlamentaria iniciada por el Boletín (896-07) la cual duró cerca de 10 años de tramitación. Analizaremos brevemente las principales normas para luego centrarnos en las críticas, que nos parecen más esclarecedoras y explicativas.

La Ley tendrá aplicación respecto de todo el tratamiento automatizado o manual de datos personales que efectúen personas naturales o jurídicas, sean de carácter privado o público. Con esto, se despejan las primeras dudas que se discutieron en Europa en algún momento al decidir si solamente se aplicaba respecto de bases de datos digitales o también manuales, situación ahora superada.

Sin perjuicio, de ser una de las primeras leyes de protección de datos, como se analizará más adelante, ha sido fuertemente criticada por su poca aplicación práctica

Estructura de la Ley N° 19.628

La ley está compuesta de un Título preliminar, V títulos y uno final. El título preliminar denominado "Sobre disposiciones Generales" indica el campo de aplicación de la Ley (artículos 1° al 3°) quedando quienes realicen

---

[134] Alfredo Chirino, Marvin Carvajal. Ob. cit. 223 y ss.

[135] Ob. Cit. p 225

[136] Artículo 12.- Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente. Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

[137] Artículo único: Modificase el artículo 19 N° 4 de la Constitución Política de la República, agregándose los siguientes incisos segundo y tercero nuevos: "Toda persona tiene derecho a controlar la información que le concierne, de modo de obtener un adecuado resguardo a sus derechos fundamentales En ejercicio de este derecho, toda persona podrá conocer sus datos personales y los que le afecten personalmente o a su familia, y obtener su rectificación, complementación y su cancelación, si estos fueren erróneos o afectaren sus derechos constitucionales, de acuerdo con las regulaciones establecidas por la ley".

[138] Prevención: Todos los artículos señalados en esta sección, deben entenderse que pertenecen a la Ley N° 19.628.

tratamiento de datos sujetos a las disposiciones de esta ley, los sujetos que pueden realizar tratamiento de datos, que según se desprende del artículo 1° puede ser cualquier persona, con la limitante de atender a lo dispuesto en la ley y finalidades permitidas por la ley, y por último, respetando los derechos de las personas titulares de los datos y las facultades que la ley otorga (en relación con los derechos que la ley reconoce en el Título II).

Luego, en el artículo 2 de la Ley N° 19.628 indica algunas definiciones que tendrán que tenerse presente para efectos de la ley, así entiende por:

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas

d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

g) Datos sensibles, aquellos datos personales que se refieran a las características físicas o morales, de las personas o ha hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bases de datos, cualquiera fuere el procedimiento empleado para ello.

i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado de los solicitantes.

j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o banco de datos.

k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República y los comprendidos en el inciso segundo del artículo 2° de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a personas determinadas o determinables.

m) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquier sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

o) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

p) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

En resumen, la ley permite que cualquier persona pueda efectuar tratamiento de datos de carácter personal, salvo en relación con aquellos denominados sensibles los que sólo podrán ser tratado cuando su titular consienta expresamente en ellos, la ley lo autorice o sea necesario para la determinación u otorgamiento de beneficios de salud (art. 10). La ley no habla sobre el tratamiento de datos personales de las personas jurídicas. Tampoco

quedará necesariamente restringido a un procesamiento de datos necesariamente automatizado, sino que también a uno de soporte papel o manual.

Si bien la ley establece como general la expresión "dato personal", existen categorías de éstos, como el que se identifica en el artículo 3° haciendo referencia al secreto estadístico, existiendo otros como la propia ley indica, datos sensibles y datos con contenido patrimonial en referencia a aquellos relativos a morosidades de pago (relacionados con el Título III de la Ley). Luego, existen datos secretos o reservados o de acceso restringido como son el secreto bancario, filiación política y secreto tributario.

En su Título I, denominado "De la utilización de datos personales" la ley principalmente en su artículo 4° inciso primero indicará la regla general en el tratamiento de datos, esto es "*sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello" ,* consentimiento que por cierto implica a) que la persona sea debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público, b) la autorización debe constar por escrito, c) dicha autorización puede ser revocada sin efecto retroactivo, lo que debe constar por escrito. Pese a lo anterior, las excepciones que siguen en la parte final del artículo 4°, hacen posible el tratamiento de datos personales sin el consentimiento del titular, así, se pueden tratar sin autorización del titular y con autorización legal: a) los datos que provengan o que se recolecten de fuentes accesibles al público[139], b) cuando se trate de datos de carácter financiero, bancario o comercial, c) se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, d)cuando los datos personales sean necesarios para la dirección directa o comercialización o venta directa de bienes o servicios, e) tampoco requiere esta autorización personas jurídicas privadas para el exclusivo uso suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadístico, de tarificación y otros de beneficio general de aquéllos.

La redacción y contenido de esta norma, ha sido en general la que da pie a sostener que la Ley N° 19.628, en realidad defendió los intereses de las empresas y legalizó el negocio de tratamiento de datos por empresas privadas de manera indiscriminada[140].

Luego, la ley indica que aquella persona encargada o responsable del registro de banco de datos personales podrá establecer un procedimiento automatizado de transmisión, con ciertos resguardos como la cautela de los derechos de los titulares y que la transmisión diga relación con las tareas o finalidades de los organismos participantes (artículo 5° en relación con el artículo 1° de la Ley N° 19.628). En el mismo articulado, regula el procedimiento de transmisión de datos, la posibilidad de eliminar datos por parte de los responsables de las bases de datos, sin contar con autorización del titular, proceder a la eliminación (carezcan de fundamento legal), bloqueo (toda vez que la exactitud de los datos no pueda ser establecida o tenga un origen dudoso) o modificación (cuando los datos sean erróneos, inexactos, equívocos o incompletos (artículo 6°).

Asimismo, indica el Título I, el deber de confidencialidad de quienes trabajan en el tratamiento de datos personales, la observancia de requisitos en el caso de internalización del tratamiento de datos por terceros por medio de mandato y el *deber de utilización de los datos sólo para los fines* para los cuales hubieren sido recolectados, salvo que sean provenientes de fuentes accesibles al público (artículos 6°, 7°, 8° y 9°), para finalizar indicando – en principio-la prohibición del tratamiento de datos personales de carácter sensible[141], salvo consentimiento del titular o que se trate de datos para la determinación y otorgamiento de beneficios de salud que correspondan a sus titulares (artículo 10°).

El Título II, se encarga de desarrollar lo que se conoce como habeas data, siendo como derecho de toda persona titular de datos de solicitar a quien sea responsable de una base de datos, pública o privada, le indique los datos almacenados que dicen relación con su persona, la procedencia, destinatarios, propósito de su recolección, y almacenamiento y organismos a los cuales han sido transmitidos regularmente. Los derechos que asisten al titular de los datos se analizarán en la siguiente parte.

A su vez, en esta parte la ley regula el procedimiento de habeas data que se ejerce respecto del responsable de la bases de datos indicando los plazos de respuesta y eventuales acciones judiciales ante los Tribunales Civiles en caso de falta de respuesta o denegación por causas distintas a la Seguridad de la Nación o el Interés Nacional, con la posibilidad de apelar a la Corte de Apelaciones respectiva como segunda instancia procesal (artículo 16°).

Cabe destacar, como se hará presente en la segunda parte de este informe, que en Chile no existe una Superintendencia, Agencia u otro organismo para velar por el cumplimiento de las normas de la Ley N° 19.628, por lo tanto, se ha reservado un procedimiento judicial poco efectivo, desconocido y de poca aplicación para velar por la garantía de habeas data. Proyectos en actual tramitación pretenden modificar dicha circunstancia, a los que también se hará referencia en la segunda parte.

---

[139] Artículo 2° letra i) Ley N° 19.628.
[140] En este sentido, autores como Renato Jijena y Pedro Anguita.
[141] De acuerdo a la definición del artículo 2° letra g) de la Ley N° 19.628.

El Título III denominado "De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", hace referencia a el tratamiento de datos provenientes de la morosidad o no pago de obligaciones económicas con las excepciones de los que provienen o se relacionan con ciertos datos(artículo 17°), establece el denominado "derecho al olvido" (artículo 18), esto es la prohibición de comunicar aquellos datos personales transcurridos 5 años desde que la obligación se hizo exigible, se saldó la deuda o se extinguió por otro medio legal.

El título IV establece entre sus artículos 20°, 21° y 23°, "Del tratamiento de datos por los organismos públicos", indicando en resumen que el tratamiento de datos llevado a cabo por éstos requiere: a) sólo podrá ejercerse dentro de materias de su competencia, con sujeción a la ley, y cumpliendo aquello, no requiere consentimiento del titular; b) los organismos públicos que sometan tratamiento de datos relativos a delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena.; c) obligación de llevar por el Registro Civil e Identificación el registro de los bancos de datos personales a cargo de organismos públicos[142].
Finalizando, el Título V se refiere a la "Responsabilidad por las infracciones a esta ley", las que se traducen en la responsabilidad de indemnizar por daño las afectaciones patrimoniales o morales por el tratamiento indebido de los datos personales (artículo 23°).
El Título final, indica expresamente en su artículo 24 una importante modificación al Código Sanitario en su artículo 127, indicando que "[*Las recetas médicas y análisis o exámenes de laboratorio y clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse y contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito…]*"

La Ley de protección de datos chilenas reconoce una serie de derechos, a saber:

3.1.- Derecho de información y acceso (Art. 12-15)

Existe un doble reconocimiento. Por una parte, el derecho a tratar datos personales[143] y por otra, una facultad positiva de exigir respecto de cualquier detentador de bases de datos, público o privado, que informe sobre los datos relativos a su persona, procedencia, propósito de almacenamiento, individualización de personas y organismos a los que se ha realizado transferencias (destinatarios).

3.2.- Derecho de rectificación o modificación (Art. 2 letra j)

En relación al principio de calidad de datos, el titular de datos puede solicitar al responsable de ficheros o bases que proceda a modificar aquellos que sean inexactos, equívocos, o incompletos. La modificación de datos la define la ley como todo cambio en el contenido de los datos almacenados en registros o bancos de datos. EL artículo 15 regula aquellos casos en que el responsable de ficheros puede oponerse a la modificación, por ejemplo, entorpezca las labores de fiscalización (en el caso que la base de datos esté en posesión de organismos públicos) o aquellos que por mandato legal deben ser siempre almacenados[144].

3.3.- Derecho de cancelación o eliminación

En este caso, el titular de datos podrá solicitar al responsable de bases de datos, que proceda a la eliminación de sus datos, cuando éstos carezcan de fundamento legal o cuando estuvieren caducos (art. 2° letra h).Igual exigencia de eliminación, o de bloqueo de los datos, surge cuando se hubieren proporcionado voluntariamente los datos personales o ellos se usen para comunicaciones comerciales y no se desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

3.4- Derecho de bloqueo

El titular de datos puede solicitar se proceda a la suspensión de operaciones respecto cualquier operación de datos almacenados (art. 2°, letra b). Como indica la ley, tal motivación puede deberse en referencia a aquellos datos que se dieron en forma voluntaria o los que se dieron con fines comerciales, los cuales en algún momento ya no se quieren. La ley obliga a bloquear los datos cuando no sea posible establecer su procedencia, sea dudosa y respecto de los cuales no cabe cancelación.

---

[142] Disponible en el sitio http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html.
[143] Para Pedro Anguita, tal previsión "resulta no tener parangón en el derecho comparado, ya que no hay ley de protección de datos personales en el mundo que reconozca la facultad de los ciudadanos de efectuar tratamiento de datos personales". ANGUITA, Pedro. La protección de datos personales y el derecho a la vida privada. Chile. Editorial Jurídica de Chile. 2007. Página 305.
[144] Por ejemplo, el número de cédula de identidad.

3.5.- Derecho de indemnización (artículo 23° inciso 1°)

El afectado por tratamientos inadecuados de sus datos personales que haya sufrido un daño moral o patrimonial, tiene derecho a ser indemnizado por el responsable de las bases de datos. Lo anterior en realidad, resulta ser más bien un deber de responsabilidad en el tratamiento de datos por los administradores de éstos. La reclamación se realiza a través de un procedimiento sumario, pudiendo ser interpuestas en forma conjunta aquella que pretenda invocar la infracción junto a la demanda civil de indemnización. Procesalmente, el juez aprecia la prueba en conciencia y durante la tramitación puede tomar todas las providencias que estime necesarias para proteger los derechos del titular de datos afectados. La indemnización es fijada por el juez considerando los hechos que envuelven el caso y la gravedad de la infracción (artículo 23).

3.6.- Derecho de oposición

Hemos dejado el estudio de este derecho para el final, puesto que en realidad no se consagra expresamente en la ley. Resulta tener una aplicación negativa, tras el reconocimiento de que en todos aquellos casos que la ley permita el tratamiento de datos personales, siempre cabe la posibilidad de que su titular pueda oponerse a su tratamiento. Únicamente se contempla la oposición en el caso del artículo 3° inciso segundo, para impedir el uso de datos personales con fines publicitarios de investigación y encuestas.

Principios reconocidos en la ley N° 19.628.

La doctrina ha sistematizado una serie de principios que estarían reconocidos en la Ley de protección de datos, a saber:

Principio de consentimiento

El tratamiento de datos de personas naturales debe realizarse cuando disposiciones legales así lo autoricen o cuando su titular consienta expresamente en ello. La autorización puede ser revocada por escrito y sin efecto retroactivo. Dicha persona debe, además, ser informada del propósito del almacenamiento, como de su posible comunicación a terceros.

Principio de datos especialmente protegidos

Haciendo referencia a los datos sensibles, que son “aquellos que se refieren a características físicas o morales de las persona o a hecho o circunstancia de su vida privada o intimidad, teles como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual (artículo 2° letra f) y g)). La regla general es que no puede haber respecto de ellos un tratamiento.

El principio de la calidad de los datos

La información que obra en bases de datos debe ser exacta, actualizada y veraz (artículo 9°). En relación a ella, en la parte de definiciones, la ley refiere a datos caducos (artículo 2° letra d). Así, se configura una serie de medidas que permiten mantener un resguardo de este principio. Por lo que debe procederse a su eliminación cuando no tienen fundamento o hayan caducado.

Por otra parte, implica la posibilidad de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Y por último, deben bloquearse aquellos datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación (artículo 6°).

En conclusión, implica entre otras cosas, que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público, en cuyo caso no será necesario contar con la autorización de su titular.

Principio de seguridad y secreto
La ley contempla la posibilidad de realizar la disociación de datos, que permite el manejo de datos personales, siempre que no se puede asociar a una persona determinada o determinable (artículo 2° letra l)). Además, dice relación con el debido resguardo que deben cuidar aquellas personas responsables de registros de bases de datos, siendo responsable de los daños que se produzcan (artículo 11°). En relación a las personas que manejas dichas bases de datos, existe la obligación de guardar secreto sobre los mismos cuando hayan sido obtenidos de bases de datos no accesibles al público.

El principio de cesión.
La regla general será la circulación de datos, es decir, la posibilidad de darse a conocer a terceros. Dicha cesión puede tener su origen en un envío de oficio o a requerimiento del responsable de la base de datos. Tales transferencias de datos, deben cautelar los derechos de los titulares y la finalidad de la transferencia (único motivo). Las excepciones permiten la omisión de estos requisitos cuando se trata de datos que provienen de bases accesibles al público o existe obligación por un Tratado Internacional de realizarla (artículo 5°).

Como se desprende de lo anterior, se trata de dos disposiciones distintas, con 9 años de diferencia. La tendencia indica que – en general – las leyes de acceso a la información resultan ser posteriores a las leyes que resguardan la privacidad[145], siendo nuestro país ejemplo de lo anterior.

Siendo posterior la Ley de Acceso a la Información, es ésta la que establece ciertos límites que reconocen y resguardan la divulgación de datos personales por parte de los organismos públicos en un procedimiento de acceso a la información pública. El legislador del año 1999, no contemplaba la posibilidad cierta de un eventual conflicto con una ley de acceso, puesto que ésta no existía como un cuerpo sistemático y único, sin perjuicio de la revisión de las primeras normas sobre Transparencia y Publicidad descritas en la primera parte de este informe.

¿La ley de acceso a la información pública, considera la gestión de los datos personales en las excepciones o en alguna otra sección del documento?

Si, como se indicó anteriormente, en nuestro país existen diversas disposiciones en la Ley de Transparencia que dicen relación con la protección de datos personales, como es la especial causal de reserva del artículo 21 N° 2 en cuanto indica **"Que las *únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes 2. Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico."***

En el mismo sentido apunta el derecho de oposición de terceros (artículo 16° y 20°) y el procedimiento que regula la Ley de Transparencia en el caso que comento, toda vez que alegada y fundada por el tercero, la administración queda impedida de hacer entrega de la información. Por cierto que respecto de la solicitud puede haberse requerido información o datos personales del tercero, pudiendo éste oponerse a dicha entrega.

En el mismo sentido apuntan las funciones y atribuciones del Consejo para la Transparencia en el artículo 33 letra m) esto es, *"Velar por el adecuado cumplimiento de la Ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado"*, sin poder sancionatorio más allá de la representación que hace al organismo público que proceda a hacer entrega de información de datos personales.

En este punto, se volverá en el capítulo III, al momento de describir la forma de resolución de conflictos entre protección de datos personales y acceso a la información.

¿La ley que protege los datos personales, brinda lineamientos acerca de la divulgación de los datos personales? ¿Hace alguna distinción en relación al interés general que algunos datos pudieran tener?

La ley N° 19.628 habla en su artículo2° letra i) sobre las "*Fuentes accesibles al público"*, en el sentido de bases que contienen datos personales, públicos que no son de acceso público o reservado. En este sentido, resultan ser bases de acceso público la información contenida en los Registros que lleva el Conservador de Bienes Raíces, donde se identifican una serie de datos personales como n° de Cédula Nacional de Identidad, ubicación de propiedades (que puede coincidir con el domicilio), rol de avalúo de la propiedad, entre otros. Asimismo, resulta ser las publicaciones en los Diarios Oficiales, medios de prensa (con resguardo de identidad de menores de edad según la Ley de Prensa), los listados de teléfono, y el padrón electoral publicado por mandato legal por el Servicio Electoral.

Por otra parte, la ley indica la prohibición de tratamiento de aquellos datos denominados sensibles en los términos del artículo 2° letra g), salvo previo consentimiento de su titular o en los casos que su tratamiento sea datos necesarios para la determinación y otorgamiento de beneficios de salud (artículo 20° de la Ley de protección de datos).Este criterio ha sido adoptado por la Ley de Transparencia, en cuanto prohíbe la publicación de estos antecedentes como parte de aquellos antecedentes que deben mantenerse permanentemente a disposición en los sitios web (obligaciones de Transparencia Activa, artículo 7° de la Ley N° 20.285).

La ley de datos personales, en su Título III (artículo 17) permite la comunicación de informaciones que verse sobre obligaciones de carácter económico, financiero, bancario o comercial cuando constan en una serie de instrumentos

[145] CORDERO V. Luis. Delimitando la Ley de Acceso a la Información Pública: Los dilemas tras la regulación. En LETELIER, Raúl y RAJEVIC, Enrique coordinadores. Transparencia en la Administración Pública. Chile. Editorial Abeledo Perrot. 2010.

mercantiles que menciona[146]. Asimismo, también pueden comunicarse sin autorización de su titular otras obligaciones de dinero que determine el Presidente de la República, del cual a la fecha no se tiene conocimiento que haya sido dictado. Tampoco podrán comunicarse aquellas deudas contraídas con empresas públicas o privadas que proporcionen los servicios de electricidad, agua, teléfono y gas, así como tampoco aquellas contraídas con concesionarios de autopistas.

Queda prohibido publicar las deudas anteriormente indicadas cuando la persona titular deudora se encuentre cesante, prohibiendo además a los responsables de estas bases de datos revelar la aplicación de esta parte de la ley.

La ley en su Título III sobre Tratamiento de datos personales de los organismos públicos, prohíbe la comunicación de datos personales relativos a las condenas por delitos, infracciones administrativas o faltas disciplinarias que traten los distintos organismos públicos, pudiendo hacerlo solo cuando se encuentre prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena.

En otras disposiciones, pero directamente relacionadas con datos personales, se ha establecido la reserva de aquellos datos estadísticos son sustento legal en la Ley Orgánica Constitucional del Instituto Nacional de Estadísticas N°17.374, en sus artículos 20° y siguientes. Lo mismo ocurre con el denominado secreto tributario descrito en el artículo 35° del Código Tributario.

Y finalmente, se encuentra prohibida la divulgación de aquellos datos personales que sin ser sensibles, el titular no consienta en la entrega de los mismos.

2. Diseño institucional

2.1. Diseño institucional para la implementación de la regulación de acceso a la información

La Ley de Transparencia creó un organismo denominado "Consejo para la Transparencia[147]" regulado por las disposiciones del Título V. Si bien, durante la tramitación legislativa de la Ley N° 20.285, en principio no existía la idea de la creación de un nuevo organismo encargado de velar por el cumplimiento de las normas de Transparencia, llegándose a indicar inclusive que resultaba innecesario, durante la tramitación, mediante la indicación sustitutiva del ejecutivo y en el Informe de la Comisión de Constitución[148], la entonces Ministra Secretaría General de la Presidencia, Paulina Veloso consigna la idea de al igual que en países vecinos – como México – se creara una institución encargada de realizar una "fiscalización permanente" a cargo del entonces denominado "Instituto de Promoción de la Transparencia". La idea de crear un organismo independiente y autónomo ya había sido sugerido desde el Grupo de Trabajo sobre Probidad y Transparencia la que inclusive abogaba por la idea de darle rango Constitucional y no solamente legal como lo es ahora. Independiente de la denominación que se pensó pasando desde el "Instituto de Acceso a la Información Pública", prosperó finalmente la idea de denominarlo "Consejo para la Transparencia".

Naturaleza Jurídica del Consejo para la Transparencia

En su artículo 31° inciso 1°, de la Ley de Transparencia indica la creación del *"Consejo para la Transparencia, como una corporación autónoma de Derecho Público, con personalidad jurídica y patrimonio propio"*, regido por sus propios estatutos (artículo 41°) los que serán propuesto al Presidente de la República, estableciéndose en ellos las normas de funcionamiento del Consejo[149]. Con la denominación "corporación autónoma de Derecho Público" se hace referencia a que el Consejo se encuentra regulado por sus respectivas leyes (Ley N° 20.285) y no como la regla general que resulta ser la aplicación de la Ley N° 18.575 sobre LOCBGAE, que regula a los sujetos indicados en el artículo 21° inciso 2°, como Ministerios, Intendencias, Gobernaciones y Servicios Públicos.

---

[146] Obligaciones que constan en letras de cambio y pagares protestados, cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa, como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorro y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios, y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentre en alguna modalidad pendiente.

[147] Sitio oficial: http://www.cplt.cl/consejo/site/edic/base/port/inicio.html

[148] Biblioteca del Congreso Nacional de Chile. Historia de la Ley N° 20.285, Informe de la Comisión de Constitución del Senado p. 173.

[149] Los Estatutos del Consejo para la Transparencia fueron publicados en el Diario Oficial el 28 de mayo de 2009, por medio del Decreto Supremo N° 20 de la Secretaría General de la Presidencia. Disponibles en: http://www.leychile.cl/Navegar?idNorma=1002606

De lo contrario, como anota el Director Jurídico del Consejo para la Transparencia *"Lo anterior no es casual. Si el Consejo se rigiera por las normas organizadoras de la LOCBGAE sería un servicio público de carácter descentralizado, o sea, de aquellos que actúan con "personalidad jurídica y patrimonio propios que la ley les asigne" y están "sometidos a la súper vigilancia del Presidente de la República a través del Ministerio respectivo (artículo 29, inciso 3° Ley N° 18.575)…*agrega*…No hay duda en que el Consejo para la Transparencia tiene personalidad jurídica y patrimonio propio; pero mal podría controlar al Gobierno en materias de transparencia si, al final del día, estuviese sujeto a la súper vigilancia del Presidente. Al revés, su rol es precisamente supervigilar al Gobierno. Por ello, al no establecer esta relación típica el legislador nos dice, inequívocamente, que está resguardando la autonomía de este organismo"*[150]. Por ello, además, según indica el artículo 31° inciso 2° de la Ley de Transparencia, los Decretos Supremos que se refieran al Consejo, en que no aparezca una vinculación con un Ministerio determinado, deberán ser expedidos a través del Ministerio Secretaria General de la Presidencia[151] (MINSEGPRES). Este Ministerio tendrá, además, una serie de otras actuaciones relevantes en materia de implementación de la Ley de Transparencia.

Objetivos del Consejo para la Transparencia

Luego, el artículo 32° de la Ley de Transparencia indica los objetivos del Consejo, éstos son *"Promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información"*[152].

Relacionados con los objetivos de la Ley de Transparencia que señaláramos en la primera parte de este informe, el Consejo para la Transparencia es el encargado de velar por ellos. En el mismo sentido, se han definido como objetivos estratégicos del Consejo, "*Promover la consolidación de un modelo de gestión gubernamental que, inspirado en el Principio de Transparencia y el Derecho de Acceso a la Información Pública, profundiza la democracia y fomenta la confianza en la función pública sobre la base de la participación y el control ciudadano"*. Su misión es: "*Promover y cooperar en la construcción e institucionalización de una cultura de la transparencia en Chile, garantizando el derecho de acceso a la información pública de las personas"*[153].

Los objetivos estratégicos del Consejo para la Transparencia han sido expuestos en sus Memorias Institucionales, siendo éstos: 1) **Promover** el principio de transparencia y **difundir** el derecho de acceso a la información pública, generando información relevante sobre los niveles de implementación en el sector público y buenas prácticas instaladas.·2)**Garantizar** el derecho de acceso a la información pública velando por su accesibilidad, exigibilidad y disponibilidad, y 3) **fiscalizar** el cumplimiento de los deberes de transparencia a través de los medios y procedimientos que establezcan las normativas aplicables. 4) Perfeccionar la **regulación** de la normativa en materia de transparencia y del derecho de acceso a la información, favoreciendo la eficiencia de la gestión pública y el control ciudadano. 5) **Instalar** el Consejo para la Transparencia en base a un modelo de gestión pública de calidad que promueve la participación ciudadana, incorporando experiencias comparadas y mejores prácticas institucionales.[154]

Consejo y Administración Interior del Consejo

El artículo 36° de la Ley N° 20.285, indica que la dirección y administración superior del Consejo corresponden a un Consejo Directivo[155] integrado por cuatro consejeros designados por el Presidente de la República, previo acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio. El Presidente hará la proposición en un solo acto y el Senado deberá pronunciarse respecto de la propuesta como una unidad. Los consejeros duraran seis años en sus cargos pudiendo ser designados para un nuevo periodo. Se renovarán por parcialidades de tres años. El Consejo elegirá de entre sus miembros a su Presidente. Para el caso que no haya acuerdo, se hará por sorteo. La Presidencia del Consejo será rotativa. El Presidente durará dieciocho meses en el ejercicio de sus funciones, y no podrá ser reelegido por el resto del actual periodo como consejero.

De lo anterior se desprende:
1.- La elección de los consejeros depende de dos de los poderes del Estado, esto es, Poder Ejecutivo y Legislativo.

---

[150] RAJEVIC, Enrique. El Consejo para la Transparencia como "Administración Independiente". En LETELIER, Raúl y RAJEVIC, Enrique coordinadores. Transparencia en la Administración Pública. Chile. Editorial Abeledo Perrot. 2010. P. 229 y ss.
[151] Así, han sido dictados por DS del MINSEGPRES el DS N° 13 de 2009 que aprueba el Reglamento de la Ley de Transparencia y el DS N° 20 de 2009, que aprueba sus estatutos.
[152] En el mismo sentido el artículo 2° de los Estatutos del Consejo para la Transparencia.
[153] Olavarría, Mauricio. La Institucionalización y Gestión Estratégica de Acceso a la Información y Transparencia Activa en Chile. Edición del Consejo para la Transparencia y el Banco Interamericano de Desarrollo (BID). 2011. Pág. 50.
[154] El mapa estratégico para el años 2012, puede revisarse en http://www.cplt.cl/mapa-estrategico-2012/consejo/2012-06-13/161051.html
[155] El Primer Consejo Directivo estuvo formado por el Sr. Juan Pablo Olmedo Bustos, quién además fue su primer Presidente, Sr. Alejandro Ferreiro, Sr. Raúl Urrutia (su segundo Presidente) y Jorge Jaraquemada. La composición actual del Consejo, se encuentra disponible en
http://www.cplt.cl/consejo/site/edic/base/port/quienes.html

2.- La propuesta presidencial debe ser adoptada por un alto quórum de Senadores en ejercicio, lo que lleva a exigir un acuerdo entre las dos principales fuerzas políticas senatoriales (oposición y de gobierno).

3.- No hay mayores requisitos para ser nombrado consejero, puesto que es facultad discrecional del Presidente proponerlos. Sin embargo, en el proyecto original del Ejecutivo se habría señalado que "*debieran ser de reconocido prestigio y excelencia en materias relativas a la gestión pública, sea en el sector privado y público"*, lo que fue desechado en la Comisión Mixta[156].

4.- Durante el año 2011 se realizó la primera renovación parcial del Consejo para la Transparencia, dejando sus cargos los Consejeros Juan Pablo Olmedo y Raúl Urrutia, los que no fueron renovados en sus cargos – según se ventiló – por distintos roces con el gobierno por algunas decisiones del Consejo para la Transparencia.

Las primeras propuestas presidenciales fueron rechazadas por el Senado, existiendo un periodo de vacancia bastante largo, lo cual se tradujo en una falta de quórum para sesionar y, por lo tanto, un retraso en la toma de decisiones del Consejo en resoluciones de amparos de acceso a la información. La Ley no contempla una forma de sustitución o de remplazo durante la vacancia de consejeros, situación que actualmente se encuentra recogida en el proyecto que modifica la Ley de Transparencia (Boletín N° 7686-07).

5.- El sistema de elección de los consejeros permite que se garantice la independencia entre éstos el Presidente de la República y el Senado, dotando de imparcialidad a las decisiones que toman.

Los artículos 37° y 38° de la Ley N° 20.285 indican las inhabilidades e incompatibilidades para ejercer el cargo de consejero, así como indica las causales de remoción o cese del cargo, respectivamente.

Así, son causales de inhabilidad no pudiendo ser designados como consejeros los Diputados y los Senadores, los miembros del Tribunal Constitucional, los Ministros de la Corte Suprema, Consejeros del Banco Central, el Fiscal Nacional del Ministerio Público, ni las personas que conforman el alto mando de las Fuerzas Armadas y de las Fuerzas de Orden y Seguridad Pública.

Son incompatibles los cargos de Consejeros con los de Ministro de Estado, Subsecretarios, Intendentes y Gobernadores, Alcaldes y Concejales, Consejeros Regionales, miembros del Escalafón Primario del Poder Judicial, Secretario y Relator del Tribunal Constitucional, Fiscales del Ministerio Público, miembros del Tribunal Calificador de Elecciones y secretario-relator, miembros de los Tribunales Electorales Regionales, sus suplentes y sus secretarios-relatores, miembros de los demás Tribunales creados por ley, funcionarios de la Administración del Estado y miembros de los Órganos de Dirección de los Partidos Políticos (artículo 37).

Luego, la remoción de consejeros corresponde a la Corte Suprema a requerimiento del Presidente de la República, de la Cámara de Diputados mediante un acuerdo adoptado por simple mayoría o a petición de diez diputados. Las causales para la remoción son por incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones. La remoción es decidida por el pleno de la Corte Suprema especialmente convocada, por mayoría de los miembros en ejercicio. Esta participación del Poder Judicial, es la única a la que hace referencia la Ley de Transparencia.

Ahora bien, las causales de cesación en el cargo son: a) por expiración del plazo por el que fue designado, b) renuncia ante el Presidente de la República, c) postulación a un cargo de elección popular y d) incompatibilidad sobreviniente, circunstancia que será calificada por la mayoría de los consejeros (artículo 38 de la Ley de Transparencia).

El gobierno interior del Consejo corresponde a su Consejo Directivo, conformado por los 4 consejeros. El quórum mínimo para sesionar es de 3 consejeros, adoptándose sus decisiones por la mayoría. En caso de empate, el Presidente del Consejo tiene voto dirimente (artículo 40° de la Ley N° 20.285, artículo 9° de los Estatutos del Consejo). Puede realizar sesiones ordinarias como extraordinarias. Son atribuciones de los Consejeros las indicadas en el artículo 11 de los Estatutos, a saber: *En cada una de las sesiones, los integrantes del Consejo Directivo tendrán derecho a: a) Participar de los debates; b) Ejercer su derecho a voto y en caso de no compartir la opinión mayoritaria formular un voto particular, cuyos fundamentos entregará a los demás Consejeros para su inclusión en el acuerdo respectivo. c) Formular consultas y peticiones acerca del funcionamiento interno del Consejo para la Transparencia y d) Obtener la información precisa que esté en poder del Consejo para cumplir las funciones asignadas.*

Las atribuciones del Presidente se encuentran enumeradas en el Título IV de los Estatutos del Consejo para la Transparencia, como por ejemplo, presidir las sesiones, moderar los debates o suspender las sesiones, representar protocolarmente al Consejo, dirimir con su voto los empates, someter a aprobación la planificación, organización,

[156] Ob. Cit. p. 236.

dirección y coordinación del Consejo planteadas por el Director General del Consejo, así como, someter a aprobación las instrucciones generales y recomendaciones, entre otras.

El siguiente cargo de importancia en el Consejo corresponde a su Director General, quien es su representante legal, debiendo cumplir las funciones estipuladas en el artículo 42 de la Ley de Transparencia[157].

El funcionamiento interno del Consejo cuenta, también con "Unidades Funcionales". Cada una de ellas ha sido creada a partir de la dictación del Reglamento del Director General para el buen funcionamiento del Consejo. Según éste[158] (artículo 9° y siguientes), se encuentran la Unidad de Planificación y Calidad, Unidad de Asesoría Jurídica, Unidad de Comunicaciones y Relaciones Institucionales, y la Unidad de Promoción de Clientes. Asimismo, crea la Dirección Jurídica (Título IV), la Dirección de Operaciones y Sistemas (Título V), la Dirección de Estudios Título VI), la Dirección de Administración, Finanzas y Personas (Título VII), la Dirección de Fiscalización (Título VIII)y la Unidad de Auditoría Interna (Título IX).

Patrimonio y Administración Financiera del Consejo para la Transparencia

En cuanto a la administración financiera del Consejo para la Transparencia, la Ley de N° 20.285 en su artículo 44 indica que estará constituido por:

a) Los recursos que contemple anualmente la Ley de Presupuestos
b) Los bienes muebles e inmuebles que se le transfieran o que adquiera a cualquier título y por los frutos de esos mismos bienes.
c) Las donaciones, herencias y legados que el Consejo acepte.

El tema presupuestario, desde sus orígenes, ha sido un problema. En ese sentido, el Consejo para la Transparencia no ha logrado la independencia económica puesto que para aquello sería necesario contar con una Ley Orgánica Constitucional, por lo tanto, el tema presupuestario dependerá de un elemento técnico (dado por las operaciones contables y financieras para determinar el costo de funcionamiento del organismo) como de la voluntad política de invertir más o menos en Transparencia.

Para el primer año de funcionamiento y la construcción del presupuesto de instalación del Consejo, se recibió el apoyo técnico de la Dirección de Presupuestos (DIPRES). Para el primer año, este monto fue de M$2.043.903 de pesos. Para el año 2010, el presupuesto fue de M$2.783.210. Complementariamente ese año, la DIPRES otorgó un suplemento presupuestario de M$200.000. Para el año 2011, el presupuesto alcanzó los M$3.250.968. Adicionalmente, se autorizaron suplementos por M$19.762 y M$376.396. Lo solicitado por el Consejo para la Transparencia como ítem presupuestario siempre ha resultado menor a lo otorgado del Tesoro Público. Así, por ejemplo, el presupuesto del año 2010 fue un 30% menor a lo solicitado, para el 2011 fue un 18% menor[159].

Personal del Consejo para la Transparencia

El personal del Consejo para la Transparencia se rige por el Código del Trabajo, sin perjuicio de lo cual resultan aplicables las normas del Título III de la Ley N° 18.575, esto es, normas de Probidad Administrativa. En los Estatutos del Consejo, se indica, además, que "*El proceso de reclutamiento del personal se realizará mediante concurso público, conforme a las directrices del Consejo Directivo y con las excepciones fundadas que el mismo determine. La selección se realizará tomando en cuenta el mérito, capacidad, confiabilidad e idoneidad para desempeñar el cargo y se sujetará a los principios de publicidad, imparcialidad, sujeción estricta a las bases de la convocatoria e igualdad"* (artículo 23° inciso 2°).

El personal que desempeñe funciones Directivas del Consejo, deberán ser seleccionados de acuerdo con la Ley N° 19.882, esto es, a través del Sistema de Alta Dirección Pública.

La fiscalización en lo concerniente al personal y juzgamientos de cuentas corresponde a la Contraloría General de la República.

---

[157] Sus funciones son: a) Cumplir y hacer cumplir los acuerdos del Consejo Directivo; b) Planificar, organizar, dirigir y coordinar el funcionamiento del Consejo, de conformidad con las directrices que defina el Consejo Directivo; c) Dictar los reglamentos internos necesarios para el buen funcionamiento del Consejo, previo acuerdo del Consejo Directivo; d) Contratar al personal del Consejo y poner término a sus servicios de conformidad a la ley; e) Ejecutar los demás actos y celebrar las convenciones necesarias para el cumplimiento de los fines del Consejo; f) Delegar atribuciones o facultades específicas en funcionarios del Consejo; g) Ejercer las demás funciones que le sean delegadas por el Consejo Directivo; h) Informar de la marcha general del Consejo mensualmente al Consejo Directivo y i) Las demás funciones que adicionalmente le encomiende el Consejo Directivo.

[158] Reglamento Orgánico del Consejo para la Transparencia, aprobado por la Resolución Exenta N° 398 de 18 de julio de 2012, que deroga la Resolución Exenta N° 43 de 2010. Disponible en:
http://www.cplt.cl/consejo/site/artic/20090408/asocfile/20090408104702/n_398.PDF

[159] Olavarría, Mauricio. Ob. Cit. p 44.

La evolución del personal del Consejo para la Transparencia, puede revisarse en:

TABLA N° 1: Evolución de la Dotación, 2009 - 2011

Unidad	2009	2010	Enero 2011	Febrero 2011
Dirección General	7	10	11	11
Dirección Jurídica	11	18	18	18
Dirección de Estudios	9	13	13	13
Dirección Adm. y Finanzas	10	13	13	13
Dirección Operaciones y Sist.	6	7	7	7
Dirección de Fiscalización	--	7	6	5
Administrativos	5	5	5	5
Sub-Total Contratos Indefinidos	48	73	73	72
Alumnos en Práctica	--	--	1	1
Plazo Fijo	--	6	7	9
Honorarios	--	3	1	1
Sub-Total Contratados	--	9	9	11
Dotación Total	48	82	82	83

Fuente: CPLT 2010b

Funciones y Atribuciones del Consejo para la Transparencia

Las funciones y atribuciones del Consejo para la Transparencia son las indicadas en el artículo 33 de la Ley de Transparencia, a saber:

a) Fiscalizar el cumplimiento de las disposiciones de esta ley (Ley de Transparencia) y aplicar las sanciones en caso de infracción a ellas.
b) Resolver, fundadamente, los reclamos por denegación de acceso a la información que le sean formulados de conformidad a esta ley.
c) 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,
d) 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 de público a dicha legislación.
e) Formular recomendaciones a los órganos de la Administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean.
f) Proponer al Presidente de la República y al Congreso Nacional, en su caso, las normas, instructivos y demás perfeccionamientos normativos para asegurar la transparencia y el acceso a la información.
g) Realizar, directamente o a través de terceros, actividades de capacitación de funcionarios públicos en materias de transparencia y acceso a la información.
h) Realizar actividades de difusión e información al público, sobre las materias de su competencia.
i) Efectuar estadísticas y reportes sobre transparencia y acceso a la información de los órganos de la Administración del Estado y sobre el cumplimiento de esta ley.
j) Velar por la debida reserva de los datos e informaciones que conforme a la Constitución y a la ley tengan carácter secreto o reservado.
k) Colaborar con y recibir cooperación de órganos públicos y personas jurídicas naturales, nacionales o extranjeras, en el ámbito de su competencia.
l) Celebrar los demás actos y contratos necesarios para el cumplimiento de sus funciones.
m) Velar por el adecuado cumplimiento de la Ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la administración del Estado.

El artículo 34° agrega que *"Para el ejercicio de sus atribuciones, el Consejo podrá solicitar la colaboración de los distintos órganos del Estado. Podrá, asimismo, recibir todos los testimonios y obtener todas las informaciones y documentos necesarios para el examen de las situaciones comprendidas en el ámbito de su*

competencia. Igualmente, para el cumplimiento de sus fines, el Consejo podrá celebrar convenios con instituciones o corporaciones sin fines de lucro, para que éstas presten la asistencia profesional necesaria para ello".

Dicho lo anterior, es posible clasificar las atribuciones y funciones del Consejo para la Transparencia de la siguiente manera:

a) Funciones o atribuciones normativas (artículo 33, letra d), e) y f)

EL Consejo para la Transparencia, desde el año 2009 ha dictado una serie de Instrucciones Generales[160] de carácter vinculante para los sujetos obligados en materia de Transparencia. Estas son:

1) Instrucción General N° 1° sobre la Presentación de Reclamos ante las Gobernaciones.
2) Instrucción General N° 2° sobre Designación de Enlaces de Transparencia.
3) Instrucción General N° 3° sobre Índice de Actos y Documentos Calificados como Secretos o Reservados.
4) Instrucción General N°4° sobre Transparencia Activa.
5) Instrucción General N° 5 sobre Transparencia Activa para Empresas Públicas, Empresas del Estado y Sociedades del Estado.
6) Instrucción General N° 6 sobre Gratuidad y Costos Directos de Reproducción
7) Instrucción General N° 7, que Complementa la Instrucción General N° 4°.
8) Instrucción General N° 8 sobre la Obligación de Informar los antecedentes preparatorios de las normas jurídicas generales que afecten a empresas de menor tamaño.
9) Instrucción General N° 9, que modifica Instrucciones Generales N° 4° y N° 7°, sobre Transparencia Activa.
10) Instrucción General N° 10, sobre el Procedimiento Administrativo de Acceso a la Información.

En el ejercicio de esta facultad, el Consejo el año 2011, dictó las "Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado"[161], las que como se desprende de su denominación, sistematizan e indican las obligaciones en materia de protección de datos que deben cumplir los organismos públicos, entregándoles orientaciones respecto los criterios jurídicos aplicables. Lo anterior, en cumplimiento de la atribución del artículo 33 letra j) debiendo velar por la debida reserva de los datos e informaciones que conforme a la Constitución y a las leyes tengan el carácter de secreto y reservado y la atribución de la letra m) de la Ley de Transparencia, debiendo el Consejo para la Transparencia velar por el debido cumplimiento de la Ley N° 19.628 por parte de los organismos públicos.

b) Funciones resolutivas (artículo 33 letra b)

El Consejo para la Transparencia es el organismo público al que la Ley ha encomendado resolver, fundadamente, los amparos y reclamaciones en materia de acceso a la información pública. Lo anterior, como el organismo administrativo que resuelve contiendas entre peticionarios o reclamantes de información en contra de un organismo público, sea acogiendo o denegando total o parcialmente la entrega de la información, de acuerdo al procedimiento especial de acceso a la información regulado en los artículos 24 y siguientes. Se debe tener presente, que la decisión del Consejo no es la última instancia, puesto que el artículo 28 de la Ley de Transparencia otorga la posibilidad de entablar el recurso de ilegalidad ante la Corte de Apelaciones respectiva, pudiendo ser interpuesto éste por el órgano obligado, por el tercero o por el solicitante de acceso a la información.

c) Funciones fiscalizadoras y sancionatorias (artículo 33 letra a)

Por medio de la fiscalización el Consejo para la Transparencia es capaz de recoger información de los sujetos obligados para analizar el nivel de cumplimiento de las exigencias legales. Con ella, se busca recoger los antecedentes necesarios que permitan detectar insuficiencias, realidades, esquemas de trabajo, falencias y debilidades y no tan sólo llevar a cabo sanciones administrativas. El Consejo inspecciona el cumplimiento de la legislación en materia del derecho de acceso a la información, puesto que es un mandato legal que le entrega la Ley de Transparencia. Según sea la evaluación realizada por el Consejo, es posible que en consonancia y como una forma de mejorar los niveles de cumplimiento, pueda dictar normativa tendiente a ello, conforme a las atribuciones del artículo 33 letra d), e) y f). Lo que la Ley no indica, es la manera en que se realizan estas fiscalizaciones, lo que ha llevado al Consejo a realizar una serie de ejercicios, sea evaluando el cumplimiento de la normativa de Transparencia Activa, barreras de entrada a solicitudes de acceso a la información, disponibilidad de la información, evaluación de sitios

[160] Disponibles en http://www.consejotransparencia.cl/consejo/site/cache/nroedic/taxport/20_0_0_1.html
[161] Disponibles en: http://www.consejotransparencia.cl/consejo/site/artic/20110914/asocfile/20110914100108/propuesta_de_recomendacion_pd_vf_09sept2011_publicacion_do.pdf

electrónicos, niveles de cumplimiento por sectores, niveles de cumplimiento por determinados sujetos obligados e inclusive mecanismos de autoevaluación. En lo que va de andar la marcha del Consejo, se han realizado fiscalizaciones a Universidades Públicas[162] (ya en su tercera versión), fiscalización de nivel de cumplimiento en hospitales autogestionados[163], fiscalización en el sector Municipal en materias de Transparencia Activa[164], y fiscalización en materia de Transparencia Activa a la Administración Central del Estado[165].

Por otra parte, la ley de transparencia en su título VI, establece el régimen de infracciones y sanciones, pudiendo el Consejo aplicarlas toda vez que a) se deniegue sin fundamento una solicitud de acceso a la información, b) no entrega de la información una vez que existe decisión firme que lo obligue e c) incumplimiento de las normas de Transparencia Activa (artículos 45 y siguientes de la Ley de Transparencia). Para el establecimiento de las sanciones, se debe llevar a cabo un procedimiento dentro del denominado "Derecho Administrativo Sancionador", esto es, deber de existir la legalidad de la sanción y tipificación de la infracción, requisitos que se cumplen en el caso de la Ley de Transparencia. Así, identificadas la norma legal vulnerada y la tipificación de la conducta, el funcionario administrativo puede resultar sancionado. En el procedimiento participan tanto la Contraloría General de la República como el Consejo para la Transparencia. Ambas instituciones firmaron un Convenio de Colaboración en junio de 2009[166], donde precisamente en su convención cuarta, indica que será el Consejo el que incoe los sumarios correspondientes, siendo la Contraloría la que realice la investigación de los hechos, proponga sanciones, pero será el Consejo el que en definitiva previa evaluación prudencial, aplique o sobresea la causa.

A la fecha se han iniciado la instrucción de 73 sumarios administrativos[167], en su mayoría contra Municipalidades y por infracción a las normas de Transparencia Activa del artículo 7° de la Ley de Transparencia. En cuando a sanciones[168], se han cursado 6, todas contra Municipalidades en su mayoría por vulneración a normas de Transparencia Activa y con multas de entre 20% y 40% de la remuneración del Alcalde.

d) Funciones de promoción, difusión, colaboración (artículos 33 letras c, g, h, i, k, l)

En este grupo, encontramos una serie funciones que como su nombre lo indica dicen relación con labores de difusión de la transparencia a los ciudadanos, por la constatación previa de la pasividad y desconocimiento inicial de éstos de la Ley de Transparencia. Lo anterior, permite al Consejo encomendar la realización de estudios sobre niveles de satisfacción de clientes, niveles de cumplimiento de estándares de transparencia (en relación con la facultad sancionatoria), celebración de convenios de cooperación con instituciones tanto nacionales como internacionales que permitan la una integración, actuar conjuntamente, implementación, establecimiento de planes pilotos, mecanismos de cooperación técnica y de personal, etcétera. A la vez, permiten las campañas de difusión a través de medios masivos y la contratación de espacios de publicidad (campañas del 2010 y 2011).

2.2. Diseño institucional para la implementación de la regulación de datos personales

En nuestro país a la fecha no existe una entidad encargada de velar por el cumplimiento de la Ley de Protección de Datos Personales. Siendo ello una falencia, existen diversos intentos legislativos en tramitación que atribuyen estas funciones al Consejo para la Transparencia (boletín N° 6.120-07) en caso de bases de datos a cargo de organismos públicos o privados, o al Servicio Nacional del Consumidor en el caso de bases de datos a cargo de privados, y al Consejo para la Transparencia tratándose de bases de datos de organismos públicos (Boletín N° 8.143-03).

---

[162] Realizadas en : noviembre de 2011 (http://www.consejotransparencia.cl/primera-fiscalizacion-a-universidades-estatales/consejo/2012-07-20/161054.html) , febrero de 2012 (http://www.consejotransparencia.cl/segunda-fiscalizacion-a-universidades-estatales/consejo/2012-07-20/160003.html) y Junio de 2012 (http://www.consejotransparencia.cl/tercera-fiscalizacion-a-universidades-estatales/consejo/2012-07-20/163649.html)

[163] Julio a noviembre de 2011. Resultados disponibles en http://www.consejotransparencia.cl/primera-fiscalizacion-a-hospitales-autogestionados/consejo/2012-07-19/115653.html

[164] Realiza entre enero y marzo de 2012, resultados disponibles en http://www.consejotransparencia.cl/fiscalizacion-en-el-sector-municipal-sobre-transparencia-activa/consejo/2012-04-27/111106.html.

[165] Realizada en dos ocasiones: noviembre a diciembre de 2010 (disponible en http://www.consejotransparencia.cl/primera-fiscalizacion-a-la-administracion-central-del-estado-en-transparencia-activa/consejo/2012-07-19/121342.html) y en octubre a diciembre de 2011 (disponible en http://www.consejotransparencia.cl/segunda-fiscalizacion-a-la-administracion-central-del-estado-en-transparencia-activa/consejo/2012-07-19/124436.html).

[166] Disponible en http://www.consejotransparencia.cl/consejo/site/artic/20090408/asocfile/20090408125721/convenio_contraloria.pdf

[167] Disponibles en http://www.consejotransparencia.cl/actos-y-resoluciones-con-efectos-sobre-terceros/consejo/2009-04-08/125721.html#T7.

[168] Disponibles en http://www.consejotransparencia.cl/actos-y-resoluciones-con-efectos-sobre-terceros/consejo/2009-04-08/125721.html#T8

2.3.- Mecanismos para resolución de controversias

Para la descripción de los mecanismos de resolución de controversias se deberán detallar los siguientes aspectos:

a. Instancias de apelación para que los ciudadanos planteen controversias.
b. Mecanismos establecidos para la resolución de controversias entre el Acceso a la Información y la Protección de Datos Personales.
c. Mecanismos de cumplimiento de las resoluciones

Visto en los anteriores capítulos la parte doctrinaria, normativa y jurisprudencial más importante a nivel nacional, corresponde analizar lo que para algunos autores son "dos caras de la misma moneda"[169]: la protección de datos y la transparencia. La zona de contacto entre ambos derechos ha resultado ser la necesidad del Estado de obtener información de sus ciudadanos para el ejercicio de una administración eficaz y, por la otra, la necesidad de tomar las medidas necesarias para asegurar a esos ciudadanos que la información relativa a su personalidad no será entregada a cualquiera. Pero, resulta que por aplicación del artículo 8° inciso segundo de la Constitución, se establece que son "*públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen…"* lo cual se ve reforzado por lo dispuesto en el artículo 5° de la Ley de Transparencia al indicar que "*En virtud del principio de transparencia de la función pública, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirven de sustento o complemento directo o esencial, y los procedimientos que se utilicen para su dictación , son públicos, salvo las excepciones que establece esta ley y las previstas en otras leyes de quórum calificado"* lo que implica el derecho de cualquier ciudadano a exigir información al Estado sobre información que éste posea.
El derecho de acceso a la información pública no es en todo caso absoluto, puesto que queda sujeto a las reservas de entrega de información, que en el caso de análisis, resulta ser la del artículo 21 n° 2 de la Ley de Transparencia, esto es, el *"Artículo21: Las únicas causales de secreto o reserva en cuya virtud se podrá negar total o parcialmente el acceso a la información, son las siguientes: N° 2.- Cuando su publicación, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud,* **la esfera de su vida privada** *o derechos de carácter comercial o económico"*. Así, esta causal de reserva se constituye en la concretización de la protección del derecho a la vida privada contenida en el artículo 19 n° 4 de la Constitución, el que tratamos en extenso en el tercer capítulo.
Cabe destacar, que en la mayoría de las legislaciones que han regulado el Derecho de Acceso a la Información Pública y normado la privacidad, resulta ser una de las excepciones más utilizadas[170].

3.1. Respecto las solicitudes de acceso a la información pública.

Reconocido como un derecho humano fundamental en diversos instrumentos internacionales y nacionales, el derecho de acceso a la información pública permite a cualquier persona solicitar información pública. En la práctica, frente a ella, la entidad requerida deberá pronunciarse dentro del plazo legal (20 días hábiles), sea entregando la información o negándola, pero antes pudo haber advertido la existencia que la eventual revelación de información o en el contenido de ésta, se encuentren contenida información que pueda **afectar derechos de terceros**.

Con la debida notificación, el tercero puede oponerse a la entrega de información por motivos fundados siendo su silencio manifestación que accede a la entrega de la información. En los hechos, esta situación vendría a constituir un primer foco de conflicto en cuanta información que por mandato constitucional y legal es pública, pero que contiene información que afecta los derechos de terceras personas, la cual debería ser declarada reservada de oficio y sin que medie oposición, por parte de la entidad requerida.

Hecho lo anterior y deducido un amparo de acceso a la información pública, será el Consejo para la Transparencia el llamado a resolver la disputa. Así, enfrentado a dos derechos, el Consejo ha debido recurrir a criterios argumentativos como son el denominado **"Test de daño"** y **"Test de interés público".** En el primero de ellos, la negación de la entrega de información será justificada cuando la entrega de la información sea capaz de provocar un daño o menoscabo a un bien jurídico protegido (en este caso, un dato personal). Así, bastará con una probabilidad razonable de que la divulgación de la información pueda causar este perjuicio, pero cumpliendo con algunas consideraciones como son la de especificidad (identificación del daño), oportunidad (daño probable en un

[169] BANISAR, David. The Right to information and privacy: Balancing Rights and Managing Conflicts. Governance Working Paper Series. United States of America. Acces to Information Program. World Bank Institute. 2011. En el mismo sentido RAJEVIC MOSLER, Enrique. Reflexiones sobre el uso y abuso de los datos personales en Chile [en línea]. Santiago, Chile. http://www.expansiva.cl/media/publicaciones/libros/pdf/12.pdf >p.147 [26.7.12]
[170] Sucede así en USA, en cuanto es la segunda más invocada para negar acceso a un documento público. Lo mismo ocurre Canadá, donde el 31% de las denegaciones de información son por aplicación de esta excepción.

tiempo inmediato) y probabilidad (mayor o menor ocurrencia del daño, en atención a ciertos conocimientos previos)[171].

Este primer criterio, ha sido considerado explícitamente por el Consejo en la resolución A45-09 en su considerando 8º el cual establece: *"que para determinar lo señalado en los considerandos precedentes se hace necesario aplicar, en este caso, lo que la doctrina comparada denomina un test de daño, consistente en realizar un balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación.*

Así lo ha planteado también la doctrina en el caso de México, al señalar que: «Generalmente se concede que no basta que un documento verse, por ejemplo, sobre seguridad nacional para que éste pueda ser automáticamente reservado del conocimiento público. Se tiene que demostrar, además, que la divulgación de ese documento genera o puede generar un daño específico al valor jurídicamente protegido. En otras palabras, se requiere de una ponderación de los valores en conflicto —en este caso publicidad contra seguridad— para poder determinar de manera cierta que la primera pone en riesgo a la segunda, y que por ello procede una reserva temporal del documento. A los criterios que guían este análisis se les conoce como la —prueba de daño»[172].

Por otra parte, el denominado "Test de interés Público", el Consejo ha indicado en su decisión A115-09 *"Que conviene considerar que cuando la transparencia puede exponer la vida privada o el patrimonio de las personas, la doctrina y la legislación comparada entienden que en principio existe una barrera que restringe la divulgación de los documentos que contienen esta información. Pese a ello "…pueden existir circunstancias excepcionales en que el interés público justifique su divulgación. Estas circunstancias excepcionales suponen una difícil y compleja valoración de los intereses en juego. Algunos países han previsto en sus legislaciones los estándares que guían esta ponderación y que se conocen como la prueba de interés público".*

Otros casos en que el Consejo tuvo que aplicar estos criterios en relación con las disposiciones de la Ley N° 19.628, fue motivado por la solicitud de acceso que le fuera formulada a la Dirección Nacional del Servicio Civil, solicitando la nómina de los candidatos seleccionados en el proceso concursal para proveer el cargo de Subdirector de Estudios y Desarrollo del Servicio de Registro Civil e Identificación. De los postulantes, solamente uno de ellos se opuso a la entrega de información. Haciéndose cargo de una de las alegaciones para fundamentar la reserva de la información. El Consejo en sus decisiones A29-09, A107-09, A186-09, A35-09, A162-09, C488-09, C94-10, ha razonado respecto de quienes no se opusieron a la entrega de la información en el sentido que si bien la información debiera ser considerada reservada por aplicación del art. 7 de la Ley N° 19.628, tal no era el caso, puesto que no habiendo sido deducida la oposición dentro de plazo (art. 20 de la Ley de Transparencia), se entiende que acceden a la entrega de la información. Lo anterior, no solamente fundado en que la sola falta de oposición indica de por sí acceso a la entrega de la información, sino que por el alto interés público que resulta revelar la información para conocer el funcionamiento de la Dirección Nacional del Servicio Civil, dado que se trata de candidatos a un puesto de alta jerarquía. Si hubiese sido una postulación a un cargo de nivel inferior, no deducida la oposición, tal información resultaría ser reservada prevaleciendo la causal de reserva.

3.2. Respecto del cumplimiento de normas de Transparencia Activa

Las normas de Transparencia Activa obligan a las entidades públicas que indica la ley a mantener publicada y en forma actualizada una serie de informaciones que de acuerdo a la Ley N° 19.628 son datos personales, como por ejemplo, las remuneraciones del personal sea a honorario o a contrata. En efecto, en este caso, la información publicada en los distintos sitios web de los servicios públicos, permite identificar plenamente a una persona puesto que aparece su nombre junto a sus remuneraciones mensuales devengadas. El caso fue llevado al Consejo para la Transparencia, tras una reclamación de un grupo de trabajadores de Televisión Nacional de Chile (TVN) por infracción a las normas de transparencia activa, al no mantener en sus sitios web información relativa a las remuneraciones percibidas por los miembros del Directorio del canal. El Consejo decidió obligar a TVN a publicar dicha información en sus sitios web, frente a lo cual la estación dedujo recurso de ilegalidad e inaplicabilidad. El iter procesal de larga data, hace imposible reducirlo en breves palabras, pero el fallo del Tribunal Constitucional[173] que resuelve el asunto, resulta ser de tal importancia en materia de datos personales, convirtiéndose en lo que algunos denominan "*un giro jurisprudencial, puesto que reconoce que la protección de los datos personales es un mandato constitucional, anclado dogmáticamente en el artículo 19 N° 4, debiendo destacarse que, para un efectivo cumplimiento de aquél, debe darse una especial protección a los que revisten la cualidad de sensibles, por cuanto a su respecto la potencialidad lesiva de la vida privada se intensifica"*[174].

---

[171] CONTRERAS V., Pablo. Ponderación entre el Derecho de Acceso a la Información Pública y el resguardo de la seguridad de la Nación. En LETELIER, Raúl y RAJEVIC, Enrique coordinadores. Transparencia en la Administración Pública. Chile. Editorial Abeledo Perrot. 2010. Página 286.

[172] *LÓPEZ-AYLLÓN, Sergio y POSADAS, Alejandro. "Las pruebas de Daño e Interés Público en Materia de Acceso a la Información. Una Perspectiva Comparada". /en/ Derecho Comparado de la Información N° 9, 2007, p. 23.*

[173] STC rol N° 1732-10 INA acumulada con la causa rol N° 1800-10 INA.

[174] QUEZADA, Flavio. El giro jurisprudencial del Tribunal Constitucional en la protección de datos personales. http://diarioconstitucional.cl/mostrararticulo.php?id=124&idautor=106. En línea. [29.04.2012]

Así, indica en el Considerando Vigésimo Quinto que "la protección de la vida privada de las personas guarda estrecha relación con la protección de datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa"; Continúa en el Considerando Vigesimoctavo "Que el legislador, cuando ha señalado ámbitos esenciales de la esfera privada que se encuentran especialmente protegidos, ha definido la información relativa a los mismos como datos sensibles…Así, aquellas informaciones –según la ley- forman parte del núcleo esencial de la intimidad y su resguardo deben ser mayor…".

3.3. Atribución del artículo 33 letra "m"" de la Ley de Transparencia

El Consejo para la Transparencia, dentro de sus funciones y atribuciones, tiene una directa relación con la protección de datos indicada en el artículo 33 letra m de la Ley de Transparencia. Así, corresponde al Consejo "*Velar por el adecuado cumplimiento de la Ley N° 19.628, de protección de dato de carácter personal, por parte de los órganos de la administración del Estado"*. Sin duda el Estado, hoy por hoy, es uno de los mayores detentadores de información privada y especialmente sobre datos personales. Si sumamos la lógica de presunción de publicidad del artículo 5° de la Ley de Transparencia, encontramos nuevamente un foco de conflicto por el contenido de datos personales de información que obra en poder del Estado. Para ello, el legislador otorgó al Consejo una función genérica y amplia de velar por la aplicación de la Ley N° 19.628 por parte de los organismos públicos.

De esta manera, por ejemplo, y ejerciendo la atribución que le concede el artículo 33 letra e (Formular recomendaciones) de la Ley de Transparencia, el Consejo ha dictado una Recomendación sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado, que busca establecer obligaciones y limitaciones que deben observar los distintos servicios, la cual entró en vigencia el 14 de Septiembre de 2011. Al respecto, llama la atención lo que pareciera ser un error por parte del Consejo al indicar en la Instrucción que "Cuando en el ejercicio del derecho de acceso a la información pública establecido en la Ley de Transparencia, se soliciten antecedentes que**, obrando en poder de la Administración, contengan datos personales de los que es titular el solicitante**, se aplicará el procedimiento establecido **en dicha Ley**, incluyendo la posibilidad de **recurrir de amparo ante este Consejo**".

Así, en la resolución A134-10 una persona que solicitó, vía acceso a la información pública, a Carabineros de Chile que explicara como obtuvo sus datos sensibles contenidos en la ficha médica, el Consejo decidió en el considerando 9º que ella *"puede ser amparada por la Ley de Transparencia en los términos que ésta establece, esto es, sólo en cuanto el reclamante requirió acceder a uno o más documentos que den cuenta de la obtención de sus datos personales por parte de Carabineros de Chile."*.

En el mismo sentido, fueron los pronunciamientos en las causas roles 178-10 (en que lo solicitado fue la copia de una declaración prestada ante la Policía de Investigaciones) considerando el Consejo *"Que asimismo, en este caso se puede apreciar que el reclamante está haciendo uso del habeas data, traducido en el ejercicio de los derechos de acceso, rectificación o cancelación sobre los datos de carácter personal que obren en poder de un tercero"* (Cons.8º).

En un caso similar, pero respecto una solicitud en que se pide copia de ficha clínica, el Consejo estimo: *"Que, previo a analizar las particularidades del caso de la especie, cabe señalar que, a juicio de este Consejo, la información requerida, al tratarse de información relativa a las atenciones médicas recibidas por una persona, se trata de un dato sensible, a la luz de lo dispuesto en el artículo 2°, letra g) de la Ley N° 19.628…(*Cons. 8º)" y – continúa en el siguiente considerando en el cual indica que "*es posible verificar que el titular de los datos, reclamante en la especie, está haciendo uso del habeas data, particularmente el ejercicio del derecho de acceso a los datos de carácter personal que obran en poder de un tercero"*.

Pensamos que este "empoderamiento" que hace el Consejo, si bien es beneficioso para el solicitante, puesto que en definitiva obtiene la información, no es el camino correcto que debe seguirse, ya que no es posible confundir el ejercicio de derechos (acceso a la información y habeas data) ni establecer procedimientos que no están contemplados en la ley.

Como indica José Luis Piñar, "*potenciar la privacidad a través del fortalecimiento de la transparencia no son en absoluto propuestas contradictorias sino complementarias y es imprescindible que se fije con certeza la relación entre privacidad y protección de datos; definir el contenido y los contornos del derecho y diferenciar entre acceso a información y acceso a los datos personales"*[175]

Más bien pareciera que el Consejo debería utilizar los mecanismos que la propia Ley de Transparencia le otorga, como son la aplicación del principio de divisibilidad, conforme el cual *"Si un acto administrativo contiene información que pueda ser*

[175] PIÑAR, José Luis. Presentación en Seminario Internacional Implementación de la Ley de Transparencia y el Derecho de Acceso a la Información Pública en Chile, organizado por el Consejo para la Transparencia. 19 y 20 de Abril 2010. Santiago.http://www.cplt.cl/potenciar-la-privacidad-a-traves-del-fortalecimiento-de-la-transparencia-no-son-propuestas-contradictorias/consejo/2010-04-21/165802.html [2.05.2012]

conocida e información que debe denegarse en virtud de causa legal, se dará acceso a la primera y no a la segunda" (artículo 11 letra e).

Creemos, que una aplicación más intensiva por parte de las distintas reparticiones públicas usando, por ejemplo, el tachado de datos personales contenidos en documentos públicos, podría ser una forma de abordar el problema desde la Transparencia en casos de conflictos de ambos derechos. Por otra parte, resulta conveniente la instauración de políticas de realización de versiones públicas de documentos que contengan datos de carácter personal, con parámetros previamente establecidos sobre su contenido, en aquellos casos en que la publicación de la información resulte relevante (por ejemplo, en el caso de concursos públicos, calificaciones, etc.). Así, aparte de fomentar la transparencia se llega al deseable equilibrio con protección de datos, sin necesidad de acudir al Consejo.

4. Organizaciones en acción

De acuerdo con la Ley N° 19.628 sobre Protección de Datos, el artículo 1° es categórico al indicar que cualquier persona puede realizar tratamiento de datos personales, siempre que lo haga de manera concordante con la legislación y las finalidades permitidas. Lo anterior, por cierto incluye al Estado, uno de las principales – si es que el no mayor- entidades que tratan información de las personas. Las razones o finalidades de ese tratamiento pueden ser diversas, desde el registro de aquellos datos obligatorios como el número de cédula de identidad (RUN)a cargo del Servicio de Registro Civil e Identificación o el Rol Único Tributario (RUT) hasta los registros de ingresos de personas a edificios o eventos, consultas crediticias, etc.

En general, cada servicio público podrá efectuar tratamiento de datos personales, recolectando para esos efectos información desde distintas fuentes, sea a través de información que el ciudadano entrega para una petición, consulta, reclamo, inicio de procedimiento, etc. Inclusive el tratamiento de los datos personales de los propios funcionarios que trabajan en las distintas reparticiones públicas.

Sin embargo, tratándose del tratamiento de datos por parte de organismos públicos, la ley de protección de datos dedica en su Título IV algunas precisiones sobre su tratamiento. Así, el artículo 20 indica que el **tratamiento de datos sólo podrá efectuarse respecto de las materias de su competencia y con sujeción al resto de las disposiciones de la ley**. Lo anterior, es consecuencia de la sujeción al principio de legalidad del actuar de la administración del Estado. En esas condiciones, los organismos públicos no requieren consentimiento del titular de los datos.

Luego, el artículo 21 hace referencia a una categoría de datos, respecto de los cuales la administración no debe comunicarlos bajo ciertos supuestos, esto es: aquellos organismos que realicen tratamiento de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán ser comunicadas una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena. La contra excepción consiste en la entrega de esta información que es solicitada por los tribunales de justicia u otros organismos dentro del ámbito de su competencia, los que en todo caso deben mantener la reserva o secreto de éstos.

Por otra parte, el artículo 22 indica que los organismos públicos que efectúen tratamiento de datos personales, están obligados a registrar los bancos de datos personales que manejan, siendo el Servicio Civil e Identificación el responsable de llevar dicho registro. Este registro, es de consulta pública[176], debiendo, además, constar respecto cada una de las bases la siguiente información: a) fundamento jurídico de su existencia, b) finalidad, c) tipos de datos almacenados, d) descripción del universo de personas que comprende. El reglamento de la Ley N° 19.628[177], en el artículo 3° viene a completar el contenido de dicho registro, debiendo agregarse el indicar el nombre del banco de datos e identificar el organismo público responsable del banco de datos personales. Por otra parte, la referida norma indica que:

a) ¿Quiénes deben inscribir las bases de datos? El Reglamento precisa que en el Servicio de Registro Civil deberán inscribirse todas las bases de datos que de acuerdo con la ley respectiva lleven las autoridades, órganos del Estado y organismos descritos y regulados por la Constitución Política de la República y aquellos comprendidos en el inciso segundo del artículo 1° de la Ley N° 18.575, LOCBGAE.

b) Las inscripciones deberán ser requeridas en las Oficinas del Servicio de Registro Civil e Identificación o bien de manera electrónica. De ser realizadas por este medio, deben adoptarse las respectivas medidas de seguridad (artículo 2°).

c) La entrega de una certificación al organismo público que registró las bases de datos (artículo 4°).

[176] Se ha dispuesto del sitio web http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.html, en donde se pueden consultar las bases de datos inscritas.
[177] Aprobado por el Decreto N° 779, publicado en el Diario Oficial el 24 de agosto de 2000.

d) Aquellos organismos públicos que contaban con bases de datos anteriores a la entrada en vigencia del reglamento, debieron proceder a su inscripción dentro de 3 meses. En tanto la nuevas bases de datos, deberán ser inscritas dentro del plazo de 15 días desde que se inicien las actividades del respectivo banco de datos (artículo N°6).

e) El Servicio Civil e Identificación tiene la obligación de otorgar por medios electrónicos y a cualquiera que lo solicite, un informe en el que conste el nombre de un determinado banco de datos personales, las menciones acerca de la información que contiene y el nombre del organismo responsable de su registro (artículo 7°).

f) Respecto de las correcciones por errores y omisiones de las inscripciones, deberá ser realizada por el propio organismo, vía electrónica o en las oficinas del Servicio Civil e Identificación. Las modificaciones de las inscripciones deberán ser requeridas igualmente por el encargado de las bases de datos, dentro del plazo de 15 días desde que se produzca tal modificación, por las vías antes indicadas.

Cabe destacar que la obligación de inscripción de las bases de datos **no conlleva la obligación de hacer entrega de dichas bases de datos al Servicio de Registro Civil e Identificación**, las cuales quedan en poder del respectivo órgano. Por otra parte, el encargado del registro no tiene facultades legales para exigir ni la ley indica la sanción en caso que no se realicen dichos registros. El Servicio de Registro Civil no posee un rol de fiscalización ni para revisar el origen, finalidad y existencia de la registrada base de datos, ni la información que ésta contiene. El registro es una mera circunstancia de hecho, de constatación. Así, aun siendo una "obligación" el registro de las bases de datos, el informe de la ONG Fundación Pro Acceso realizado entre septiembre y diciembre de 2009 y repetido entre noviembre y enero de 2010, reveló que de los 164 servicios consultados el año 2009, 50 de los que respondieron, 39 tenían bases de datos y sólo 5 de estos organismos habían dado cumplimiento al registrarlas[178]. La cifra aumentó el año 2010, concluyendo que de las 58 entidades que respondieron en 2010, un 52% registro dichas bases. En un estudio pronto a publicarse, se espera que tal cifra haya aumentado.

Cabe destacar que el Servicio de Registro Civil e Identificación, de ninguna manera viene a sustituir o tener las facultades que poseen las Agencias de Protección de Datos en legislaciones comparadas al estilo de la Agencia de Protección de Datos Personales Española, por ejemplo.

Tratamiento de datos personales por organismos públicos

La regla general en el sector público para efectuar tratamiento de datos personales se encuentra centrada principalmente en el artículo 20° que permite a cualquier organismo público el tratamiento de datos, siempre que actúe dentro del marco de su competencia, no requerirá autorización del titular de datos para efectuar el tratamiento de éstos. Lo anterior, permite a las distintas reparticiones del Estado contar con un gran volumen de información que permite maximizar en tiempo y recursos la entrega de servicios a los ciudadanos, en atención a los principios de eficiencia y eficacia a que debe atender la administración pública. Esto se traducirá en la atribución de realizar tratamiento de datos no tan sólo de aquellos que provienen de la propia entrega de datos, sino que de la recolección de datos o la celebración de convenios o transferencias. En el mismo sentido, las actuales **políticas de interoperabilidad** de las gestiones que realiza la administración pública, permite un acceso a un sinnúmero de datos que poseen diversas reparticiones públicas de manera instantánea. En nuestro país, el plan que forma parte de la estrategia digital[179] es conocido técnicamente como **"Plataforma Integrada de Servicios Electrónicos del Estado" (PISEE)**, el cual busca maximizar los tiempos y recursos en la atención ciudadana, evitando la duplicidad de gestiones o el requerimiento de información excesiva que ya obra en poder del Estado. Así, por ejemplo, se destaca en la iniciativa objetivos como la mejora de la calidad de información, atención y servicios de las personas facilitando el acceso a la información actualizada oportuna y confiable, facilitar los procedimientos administrativos y transparentar ante el ciudadano la información que el Estado posee[180]. En cuanto a protección de datos, el plan impone la necesidad de contar con un definido contorno de protección, bajo clausulas de confidencialidad y prohibición de cesión de datos a terceros ajenos o privados para fines distintos a los de su competencia.

Tres son las claves para entender la regulación de tratamiento de datos, a las cuales ya nos hemos referido en general en la segunda parte de este informe. El primero de ellos, dice relación con lo indicado en el artículo 4° inciso primero de la Ley N° 19.628, toda vez que indica *"El tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello"*. En seguida, no será necesario contar con la autorización del titular cuando se trate de fuentes de datos personales accesibles al público y, en el caso expresamente relacionado con administración de datos de servicios públicos, en relación al artículo 20, toda vez que actuando dentro de las materias de su competencia y con sujeción a la ley de protección de datos, tampoco será necesario contar con el consentimiento de su titular. Así, la regla será contar

[178] Fundación Pro Acceso: Protección de datos personales en el sector público. 2010. Disponible en http://www.proacceso.cl/files/Estudio%20Datos%20Personales%202011.pdf [Fecha de consulta 21.09.12]
[179] Más información en www.estrategiadigital.gob.cl.
[180] VALENZUELA, Cecilia: Ministerio de Economía, Fomento y Reconstrucción. Estrategia Digital. Plataforma Integrada de Servicios Electrónicos del Estado PISEE. Presentación en el Seminario Internacional de e-gov, 1 de octubre de 2009. Disponible en http://www.egov.usm.cl/wp-content/uploads/2009/10/Plataforma-ISEE_.pdf [fecha consulta 26.09.2012]

necesariamente con disposición legal habilitante que permita al servicio tratar datos, o sin ésta cuando el titular ha consentido en ello.

Por otra parte, encontramos el principio de finalidad de datos, esto es, los organismos públicos no pueden realizar tratamiento de datos fuera de la finalidad de recogida de los datos, en la medida que provengan o se hayan recolectado de fuentes accesibles al público, lo anterior en cumplimiento de lo dispuesto en el artículo 9° de la Ley de Protección de Datos.

Finalmente, cabe destacar el tratamiento de aquellos datos denominados sensibles (artículo 2° letra G Ley N° 19.628), respecto de los cuales los organismos públicos por excepción podrán realizar tratamiento de datos (artículo 10° de la Ley N° 19.628), salvo cuando una ley lo autorice, el titular consiente en ello o sean datos necesarios para el otorgamiento de beneficios de salud de sus titulares.

I .- Sobre el resguardo de las fichas clínicas en particular

Existen una serie de disposiciones en materia de salud que autorizan el tratamiento de datos personales en el sector. Por ejemplo, y mediante la modificación introducida por la Ley N° 19.628 al artículo 127 del Código Sanitario, indica que "*Las recetas médicas y análisis de salud o exámenes de laboratorio clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos"*.

Por otra parte, el Decreto con Fuerza de Ley N° 1 del Ministerio de Salud del año 2005 que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.933indica como facultades del Ministerio de Salud (MINSAL) en su artículo 4° N° 5 "*Tratar datos con fines estadísticos y mantener registros o bancos de datos respecto de las materias de su competencia. Tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud. Para los efectos previstos en este número, podrá requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria. Todo ello conforme a las normas de la Ley N° 19.628 y sobre secreto profesional*". En el mismo sentido apunta el artículo N° 50 letras F), al indicar respecto del Fondo Nacional de Salud con la misma función. Asimismo, las Instituciones de Salud Previsional (ISAPRES), quedan autorizadas a requerir a los prestadores las fichas clínicas de los pacientes e inclusive que ésta sea revisada por otro médico, con el debido resguardo y confidencialidad tanto por parte de las ISAPRES como de los prestadores (art. 189 N° 5 letra C letra h) DFL N° 1 2005 MINSAL). La ley también otorga como funciones y atribuciones a la Superintendencia de Salud el deber de resguardar la confidencialidad de la ficha clínica (artículo 110° N° 17 DFL N° 1 2005 MINSAL).
En la relación médico paciente, es necesario contar con un espacio de reserva y de confidencialidad. Las conversaciones, prescripciones, datos y cualquier otro antecedente que surge de esta relación queda registrada en una ficha que contiene lo que la ley considera datos sensibles, respecto de los cuales otorga especial protección, limitando el tratamiento que pueden dar los organismos tanto público como privados. Esta ficha da cuenta de la historia médica del paciente. En los últimos años, el avance de la tecnología ha permitido eliminar el registro en papel de tales documentos, siendo ahora la tendencia el uso de la "ficha médica digital". *"La Ficha Clínica en que queda registrada la historia médica del paciente tiene por objeto la optimización del acto médico. Constituye un documento de trabajo diario del médico, donde éste y quienes intervienen de alguna manera en el cuidado del enfermo dejan constancia de su evolución clínica y de los tratamientos y procedimientos realizados con el fin de disponer de una información circunstanciada sobre el curso de su enfermedad"*[181]. En el mismo sentido se ha señalado que *"La Ficha clínica es el documento de mayor relevancia en salud debido a que es fundamental para una atención segura y continua del paciente. A su vez, posee un valor significativo para el establecimiento sanitario en sus procesos administrativos, de docencia, de investigación, así como para la administración de justicia"*[182] [183].

El marco normativo de la ficha clínica se encuentra regulado principalmente en los siguientes cuerpos legales:

---

[181] Colegio Médico de Chile. Ficha Clínica: Derecho a la información y reserva de la información contenida. Disponible en http://www.colegiomedico.cl/Default.aspx?tabid=255 [Fecha consulta 1.10.2012]
[182] Hospital de Padre Hurtado. Norma de manejo de ficha clínica. 2009. Disponible en http://www.hurtadohosp.cl/archivos/CalidadySeguridad/NormasdeCalidad/Normas_de_Ficha_Clinica/NMFC.pdf [fecha consulta 1.10.2012]
[183] Para un análisis respecto del contenido técnico de la ficha médica, VARAS, Jorge y otros. Ficha Clínica: composición y manejo, registros clínicos. Revista Chilena de Obstetricia y Ginecología. Hospital Santiago Oriente Dr. Luis Tisné. 2010. Volumen 5, pág. 57-61. Disponible en http://www.revistaobgin.cl/files/pdf/57a610.pdf [Fecha de consulta 1.10.2012].

a) Manual de Procedimientos de la Sección de Orientación Médica y Estadística (SOME), aprobado por la Resolución Exenta N° 926 de 14 de junio de 1989 del MINSAL que regula la extensión, archivo, despacho, eliminación y confidencialidad de la Ficha Clínica. En el N° 10, regula la confidencialidad de la historia clínica, señalando que: *"Las historias clínicas son documentos reservados, de utilidad para el enfermo, el establecimiento, la investigación, la docencia y la justicia, debiendo guardar el debido secreto profesional toda persona que intervienen en su elaboración o que tenga acceso a su contenido"*. En su párrafo 3°, se establece que las historias clínicas pueden ser solicitadas por escrito, por consulta médica, hospitalización, investigación o estudio, tramitación de beneficios económicos y otros casos que deben ser autorizados por escrito por el médico".

b) La Directiva Permanente Interna Administrativa N° 4, del Ministerio de Salud que establece las normas para el manejo de las historias clínicas en los establecimientos del Sistema Nacional de Servicios de Salud, que establece en su N° 1 que "Las historias clínicas deberán considerarse reservadas y secretas, de utilidad para el enfermo, el establecimiento, la investigación, la docencia y la justicia, por lo que se podrá autorizar su uso para otros fines, guardando en todos los casos el secreto profesional". A su vez, su N° 6 señala que el paciente, su representante legal o el médico cirujano tratante podrán requerir una copia de los exámenes de laboratorio que se le hayan practicado al enfermo, un informe con el diagnóstico de su enfermedad y tratamiento practicado.

c) Decreto Supremo N° 161, de 1982, del Ministerio de Salud, Reglamento de Hospitales y Clínicas, que en su artículo 22 dispone que "Toda la información bioestadística o clínica que afecte a personas internadas o atendidas en el establecimiento tendrá carácter reservado y estará sujeta a las disposiciones relativas al secreto profesional. Sólo el Director Técnico del establecimiento podrá proporcionar o autorizar la entrega de dicha información a los Tribunales de Justicia y demás instituciones legalmente autorizadas para requerirla. Respecto de otra clase de instituciones, sólo podrá proporcionarse información con la conformidad del paciente o entregarse datos estadísticos globales en los que no se identifique a personas determinadas".

d) La reciente Ley N° 20.584[184] que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, indica en su párrafo 5° Titulado "De la reserva de la información contenida en la ficha clínica", en su artículos 12 que "La ficha clínica es el instrumento obligatorio en el que se registra el conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas, que tiene como finalidad la integración de la información necesaria en el proceso asistencial de cada paciente. Podrá configurarse de manera electrónica, en papel o en cualquier otro soporte, siempre que los registros sean completos y se asegure el oportuno acceso, conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella. Toda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como dato sensible, de conformidad con lo dispuesto en la letra g) del artículo 2º de la ley Nº 19.628". El artículo 13 indica que "La ficha clínica permanecerá por un período de al menos quince años en poder del prestador, quien será responsable de la reserva de su contenido. Un reglamento expedido a través del Ministerio de Salud establecerá la forma y las condiciones bajo las cuales los prestadores almacenarán las fichas, así como las normas necesarias para su administración, adecuada protección y eliminación. Los terceros que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica. Ello incluye al personal de salud y administrativo del mismo prestador, no vinculado a la atención de la persona. Sin perjuicio de lo anterior, la información contenida en la ficha, copia de la misma o parte de ella, será entregada, total o parcialmente, a solicitud expresa de las personas y organismos que se indican a continuación, en los casos, forma y condiciones que se señalan:

a) Al titular de la ficha clínica, a su representante legal o, en caso de fallecimiento del titular, a sus herederos.
b) A un tercero debidamente autorizado por el titular, mediante poder simple otorgado ante notario.
c) A los tribunales de justicia, siempre que la información contenida en la ficha clínica se relacione con las causas que estuvieren conociendo.
d) A los fiscales del Ministerio Público y a los abogados, previa autorización del juez competente, cuando la información se vincule directamente con las investigaciones o defensas que tengan a su cargo. Las instituciones y personas indicadas precedentemente adoptarán las providencias

[184] Promulgada el 13 de abril de 2012. Entró en vigencia el 1 de octubre de 2012.

necesarias para asegurar la reserva de la identidad del titular de las fichas clínicas a las que accedan, de los datos médicos, genéticos u otros de carácter sensible contenidos en ellas y para que toda esta información sea utilizada exclusivamente para los fines para los cuales fue requerida".

No cabe duda que el contenido de los datos consignados en una ficha clínica corresponde a datos de carácter sensible. Es más, su divulgación sin autorización constituiría una violación al derecho a la vida privada en los términos del artículo 19 N° 4 de la Constitución Política de la República, por contener datos que pertenecen a aquel espacio más íntimo o reservado de las personas, entregados únicamente con el objetivo de obtener un alivio o tratamiento de enfermedad, resguardado siempre bajo confidencialidad y acceso limitado.
Un tema debatido doctrinariamente en materia de acceso a la información y protección de datos personales dice relación con el denominado ejercicio del *habeas data* en sede del ejercicio de acceso a la información. La tesis del Consejo para la Transparencia ha sido que en el ejercicio del derecho de acceso a la información pública consagrado en el artículo 10 de la Ley N° 20.285, es posible solicitar a los organismos públicos información sobre el mismo peticionario. Este criterio ha sido utilizado precisamente al momento de resolver solicitudes de acceso que dicen relación con requerimientos de copias de fichas clínicas u otros antecedentes médicos, como informes, peritajes, evaluaciones, reconsideraciones por licencias médicas, etc. En efecto, según la tesis del Consejo, es posible acceder a datos personales mediante solicitudes de acceso, entendiendo que éste constituye el derecho que tiene toda persona a exigir a quien sea responsable de un banco de datos, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente (artículo 12 de la Ley N° 19.628). Este sería el denominado "*habeas data impropio" o "derecho de acceso a datos de carácter personal"*[185].

El Consejo ha sostenido su tesis principalmente en las disposiciones del artículo 10, en cuanto cualquier persona puede solicitar información de cualquier órgano de la Administración del Estado (artículo 10° LT), es pública toda información que obra en poder del Estado (artículo 5° LT), los principios del procedimiento de acceso a la información (Artículo 11° LT). Asimismo, en las Recomendaciones del Consejo para la Transparencia sobre protección de datos de carácter personal por parte de los órganos de la Administración del Estado, en el punto N° 5.1 final indica que *"Cuando en el ejercicio del derecho de acceso a la información pública establecido en la Ley de Transparencia, se soliciten antecedentes que, obrando en poder de la Administración, contengan datos personales de los que es titular el solicitante, se aplicará el procedimiento establecido en dicha Ley, incluyendo la posibilidad de recurrir de amparo ante este Consejo. No obstante ello, en lo relativo a la gratuidad del acceso, se observará lo dispuesto en la Ley Nº 19.628".*

Por el contrario, los dogmáticos de protección de datos, han indicado que mediante este razonamiento se ha "*desnaturalizado"*[186]el habeas data de la Ley de Protección de Datos y la función del Consejo para la Transparencia, cometiéndose un error conceptual y jurídico. Así, el derecho de acceso a la información pública del artículo 10° de la LT es completamente distinto al ejercicio del habeas data contenido en el artículo 12° de la Ley de Protección de Datos Personales, puesto que en el ejercicio del derecho de acceder a información no incluye el acceder a datos personales, y porque existe un procedimiento judicial distinto de recurrir al Consejo para la Transparencia en caso de negativa o disconformidad en la entrega de los datos solicitados.

La tesis del Consejo para la Transparencia en el acceso a fichas clínicas[187]

Como se explicaba anteriormente, el Consejo para la Transparencia ha aceptado el acceso a las copias de fichas clínicas mediante el ejercicio del derecho de acceso a la información pública, pero hay que distinguir:
1.- Acceso a las fichas clínicas de personas fallecidas (C398-10, C322-10, C556-11, C740-10).
Respecto de ellas, la tesis del Consejo ha sido considerar que una persona fallecida no es titular de datos personales, de acuerdo a lo dispuesto por el artículo 2° letra ñ) de la Ley de protección de datos, al definir como titular de datos a la persona natural a la que se refieren los datos de carácter personal. Sin embargo, su honra se proyectaría como un derecho de sus propios familiares, toda vez que su memoria constituye una prolongación de dicha personalidad, protegida y asegurada como parte de la honra de la familia. Por lo tanto, resultan ser los descendientes de las personas fallecidas las llamadas a determinar la información que desean sustraer del conocimiento de terceros no vinculados. Aceptar una tesis de reserva absoluta, implicaría la posibilidad de desconocer eventuales

[185] Este criterio ha sido aplicado a una serie de materias de diversa índole, por ejemplo, el acceso a las declaraciones efectuadas ante organismos públicos como denuncias (Rol C1118-12), solicitudes de copia de evaluaciones o resultados en concursos públicos (C707-10, C1139-11), copia de las actas evaluación realizadas por el Consejo Técnico de Gendarmería encargados de autorizar beneficios carcelarios como las salidas dominicales (C376-12), informes de desempeño laboral (C1503-11), entre otros.
[186] JIJENA, Renato. La desnaturalización del habeas data en los tribunales chilenos. Disponible en http://www.habeasdataorg.cl/2010/01/25/desnaturalizacion-del-habeas-data-en-los-tribunales-de-justicia-chilenos/ [Fecha de consulta 22.09.2012].
[187] Recopilación de casos de acuerdo al Estudio Normativo del Consejo para la Transparencia sobre Protección de datos de carácter personal, realizado por la Unidad Normativa del Consejo, abril 2011.

situaciones de negligencia de la praxis médica y el derecho de ejercer acciones judiciales y responsabilidades civiles y penales. Sin embargo, para acceder al contenido de dichas fichas, es necesario no tan solo tener un vínculo de parentesco con el fallecido, sino que resulta necesario constar alguna de las siguientes circunstancias (Rol C556-10):
a.- Ser heredero del fallecido de acuerdo a lo dispuesto en el artículo Nº 983 del Código Civil, o que se actúe en representación de uno o más herederos.
b.- Tener una legitimación activa para ejercer otros derechos que supongan el acceso previo a la ficha clínica del difunto.

Así, a falta o cumplimiento de ambas circunstancias, es posible acceder o rechazar a dicha documentación, por ejemplo en la causa rol C556-10, en el cual la requirente sobrina del fallecido no concurrió respecto de ella ninguna de las circunstancias anteriores y en cambio en la rol C322-10, en que tratándose de un requerimiento del hijo del difunto y cumpliendo ambos requisitos, se accedió a la entrega de la ficha.
2.- Acceso a las fichas clínicas cuyo titular solicita copia de éstas o en representación legal de otro (rol C398-10, C240-10)

Se plantea el caso en que lo solicitado dice relación con fichas médicas o documentos en que consten atenciones médicas requeridos por el propio solicitante del cual es titular o actúa en representación de otro. Según la jurisprudencia del Consejo para la Transparencia, en el caso C240-10, en el que un padre de un hijo internado en un hospital psiquiátrico solicitó copia de la ficha clínica de su hijo y otros documentos. Si bien el Consejo rechazó el amparo, este indicó que por ficha clínica habrá de entenderse que ésta contiene información sobre las características físicas o morales de una persona y su estado de salud físico o psíquico, datos que han sido calificados como sensibles según lo dispuesto en el artículo 2° letra g) de la Ley de Protección de Datos Personales, razón por la cual su divulgación se encontraría prohibida, salvo la concurrencia de las hipótesis del artículo 10° de dicho cuerpo legal (ley lo autorice, exista consentimiento del titular o sean necesarios para la determinación u otorgamientos de beneficios de salud) . Ahora bien, en el caso que comento, dicha ficha efectivamente hubiera sido entregada si el padre hubiera acreditado la representación legal de su hijo internado en el centro hospitalario, situación que no concurrió[188]. Distinto fue la decisión en el caso Rol C400-12, en que el Consejo luego de despejar las dudas respecto que la solicitud de la ficha clínica puede realizarse en sede de acceso a la información (siguiendo la línea jurisprudencial en la resolución de casos C134-10, C178-10 y C49-11), acogió el amparo, debiéndose hacerle entrega de la ficha clínica del titular peticionario, con el resguardo de ser entregado personalmente o a su apoderado según lo dispuesto en el punto N° 4.3 de la Instrucción N° 10 del Consejo para la Transparencia, esto es, sea retirada personalmente o por apoderado en los términos exigidos por la Ley N° 19.880.

II . Sobre el listado de beneficiarios de un plan social

Como se indicó en los primeros capítulos de este informe, al momento de analizar las disposiciones de la Ley de Transparencia, el artículo 7° de dicho cuerpo legal precisa la publicación de cierta información que debe estar permanentemente a disposición del público en los sitios electrónicos de todos los servicios, denominada "Transparencia Activa". Dentro de dichas obligaciones, en la letra i) indica expresamente dentro de esta información *"el diseño, montos asignados y criterios de accesos a los programas sociales en ejecución, además de las nóminas de los beneficiarios de programas sociales en ejecución. No se incluirán en estos antecedentes los datos sensibles, esto es, los datos personales que se refieren a las circunstancias físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos o la vida sexual".*
Complementa lo anterior, la Instrucción General N°4 del Consejo para la Transparencia sobre Transparencia Activa, indicando que:
a.- Los órganos y servicios públicos que dispongan de programas de subsidios o beneficios deberán publicar una planilla por cada uno de ellos, indicando el nombre del programa, el diseño del subsidio o beneficio, dentro del que se deben consignar: unidad, órgano interno o dependencia que los gestiona, requisitos y antecedentes para postular, montos globales asignados, periodos o plazos de postulación, criterios de evaluación y asignación, plazos asociados a este procedimiento, objetivo del subsidio o beneficio, individualización del acto por el cual se estableció el programa (tipo, denominación, número, fecha del acto y un link al texto íntegro del mismo) y un vínculo a la página del sitio web institucional y/o documento donde se entrega información complementaria a su respecto.
b.- Para el caso que se trate de programas sociales en ejecución deberá, además, contemplarse una nómina con el nombre completo de los beneficiarios, indicando la fecha de otorgamiento del beneficio y la identificación del acto por el cual se otorgó. Dicha nómina excluirá datos como, por ejemplo, domicilio, teléfono y correo electrónico del beneficiario, por no ser estrictamente necesarios para individualizarlos.
c.- Se entenderá por "beneficiario" a la persona natural o jurídica, a la asociación y/o entidad que sea destinatario/a directo/a de los programas sociales en ejecución de los respectivos órganos de la Administración del Estado.

[188] En el mismo sentido, pero acreditando debidamente la personería suficiente y por mandato especial, el Consejo ha estimado necesario tener en cuenta la forma en que se manifiesta el consentimiento del titular en el tratamiento de sus datos personales sensibles, el cual debe resultar inequívoco (Rol C418-10 y C351-10), en atención al principio de seguridad de datos.

d- No se individualizarán a los beneficiarios cuando ello suponga la revelación de datos sensibles, esto es, datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. En esto casos, deberá informarse el número total de beneficiarios y las razones fundadas de la exclusión de la nómina.
e.- En caso que un órgano actúe como colaborador de otro servicio, con la finalidad de facilitar o acercar a la comunidad a la postulación y/o acceso a los subsidios y otros beneficios que éste último entregue, la obligación de publicar por transparencia activa recae en éste y no en el primero. Sin perjuicio de lo anterior, se considerarán buena práctica que el órgano colaborador informe en su página web los beneficios a los que se pueden acceder por su intermedio o en sus dependencias y que otorgan otros servicios, con indicación del link de la página web del servicio competente que contenga la información del programa respectivo.

¿Por qué hacer pública esta información?

Uno de los criterios del Consejo para la Transparencia en orden a identificar a quienes son beneficiarios del Estado, corresponde al mismo criterio por el cual se justifican la entrega de información de funcionarios públicos: el hecho de obtener un beneficio o subsidio del Estado, hace que se reduzca el ámbito de la privacidad en aras del control social, lo cual no implica la publicación de información de datos de carácter personal como el RUT, el cual para publicarse es necesario contar con la autorización del titular o una ley lo autorice (Rol C272-10). En el mismo sentido respecto del domicilio como dato personal (Rol C33-09, A140-09, C415-09, C713-10, C832-10) o la dirección del correo electrónico (rol C521-10, A140-09). La tesis del legislador y de la Instrucción del Consejo para la Transparencia busca varios objetivos, entre ellos, a) Informar la forma, tiempo y monto de los beneficios, los requisitos de postulación, montos globales asignados, norma legal habilitante, dependencia o entidad encargada de la gestión, b) Transparentar, esto es, mediante la publicación de la nómina de beneficiarios se busca mantener un registro público de beneficiarios, c) Rendir cuentas, esto es, contabilizar los montos asignados en beneficios sociales y realizar un escrutinio público, por ejemplo, detectando irregularidades en las cifras. Detrás de la información, existe un evidente interés público en pos del control social de las asignaciones pecuniarias.

En cuanto al tratamiento de estos datos, cabe tener presente el principio de finalidad de datos del artículo 9° de la Ley de Protección de Datos Personales, debiendo entonces aquellos organismos que otorgan beneficios actuar dentro de sus competencias en relación con los postulantes y beneficiarios cuya recopilación de datos tiene por objetivo tales asignaciones.

3.2.-Revelar el modo en que se gestiona información personal de funcionarios públicos

III. - Currículum Vitae

El currículum vitae es el documento en que consta la trayectoria profesional y académica de una persona, todos antecedentes que son necesarios tener en consideración al momento de evaluar y seleccionar a un candidato entre varios. En la administración pública, este documento forma parte de un expediente administrativo, por lo tanto, se trata de información que obra en poder del Estado.

Podríamos identificar al menos 3 hipótesis en que pudiera solicitarse el acceso a este documento: a) Caso de participantes del proceso de selección que solicitan antecedentes de los otros concursantes, b) Caso en que terceros solicitan acceso a estos documentos en ejercicio de sus derechos de acceso a la información sin participar necesariamente en el proceso o invocando otras razones, c) Casos en que se solicita información sobre currículum que obran en poder de la administración, pero sin tener relación con un concurso o en ejercicio de funciones públicas, sino como parte del cumplimiento de contratar determinadas personas para la ejecución de proyectos u otros afines.

Recordemos que siempre podrá ser posible dar respuesta negativa de la institución requerida, realizando el proceso de oposición descrito en el artículo 20 de la Ley de Transparencia, siendo tarea del Consejo resolver o de las Cortes de Apelaciones en su caso.

Sin perjuicio de lo anterior, el Consejo para la Transparencia, ha establecido algunos criterios generales de aplicación, a partir de una solicitud de acceso en que lo solicitado era el currículum vitae de determinadas personas que trabajan en un Municipio y de quiénes evaluaron en un proceso de concurso público (C95-10). En este caso, el Consejo ha indicado que:

- Ha sentado la premisa fundamental que la esfera de privacidad de aquel personal que trabaja en la administración pública sería más reducida que el resto de las personas, en virtud de las funciones que desempeñan (A47-09, A91-09, A181-09, C434-09).

- Que respecto el currículum vitae, este es entendido como "*La relación de títulos, honores y cargos, trabajas realizados, datos biográficos, etc. que califican a una persona"* (Diccionario de la Lengua Española, 22° Ed.).

- Que tratándose de currículum de particulares que se haya en poder de la Administración, es necesario realizar un test de interés público comprometido, la imparcialidad de los procesos de selección y su control por la ciudadanía. Cita al efecto, lo decidido respecto dos casos similares (C204-09 y C501-09), en que el Consejo estimó que "*Dicha información es pública (currículum vitae), toda vez que la individualización del equipo de trabajo del oferente, junto con su experiencia laboral, permiten constatar no solo las competencias y habilidades del equipo propuesto – criterios que sirven para determinar el adjudicatario- sino también a la procedencia de incompatibilidades en el equipo de evaluadores, constituyendo el acceso a la información un mecanismo de fiscalización que asegura la imparcialidad del proceso, configurándose un interés público en la divulgación de la información que este Consejo intenta proteger"* (Cons. 10°, decisión 210-09).

- Que por otra parte, el Consejo ha indicado que en dicho documento consta la trayectoria académica, profesional y laboral que tienen relación con la capacidad o habilidad y pericia para ocupar el cargo, por lo tanto, el acceso a dicha información permite a la ciudadanía evaluar las capacidades de la persona seleccionada para desempeñar su labor (C94-10, C279-10, C). Lo anterior, por cuanto se trata de información que obra en poder de la administración y que en casos de concursos públicos, por ejemplo, sirve de base o complemento esencial para la dictación de un acto administrativo, habida cuenta de la trayectoria profesional y académica de los postulantes.

- Sin embargo, lo anterior no obsta a que sea necesario proceder a tachar los datos personales que no tengan directa relación con un escrutinio sobre capacidad de los funcionarios como sería sus datos personales. Por lo tanto, en este sentido, se aplica el denominado "principio de divisibilidad" (artículo 11 letra e) de la Ley de Transparencia), esto es "*conforme al cual si un acto administrativo contiene información que pueda ser conocida e información que debe denegarse en virtud de causa legal, se dará acceso a la primera y no a la segunda".* Así, por ejemplo, la mencionada decisión C94-10 del Consejo para la Transparencia por ilegalidad[189], en que se eliminan aquellos antecedentes que permitan la identificación de los concursantes. Cita la experiencia mexicana del IFAI, resoluciones N° 2653/08, 5154/08, 2214/08, 1377/09 y 2128/09), en el sentido que *"tratándose del currículum vítae de un servidor público, una de las formas en que los ciudadanos pueden evaluar sus aptitudes para desempeñar el cargo público que le ha sido encomendado, es mediante la publicidad de ciertos datos de los ahí contenidos. En esa tesitura, entre los datos personales del currículum vítae de un servidor público susceptibles de hacerse del conocimiento público, ante una solicitud de acceso, se encuentran los relativos a su trayectoria académica, profesional, laboral, así como todos aquellos que acrediten su capacidad, habilidades o pericia para ocupar el cargo público".*

Es posible además, que el tercero cuyo currículum vitae es solicitado, pudiera oponerse a la entrega de la información aplicándose en ese caso la causal de reserva del artículo 21 N° 2, sin embargo, por las consideraciones anteriores, es plausible entender que el Consejo razonaría en el mismo sentido.

Por otra parte, cabe destacar que es posible constatar en algunos sitios web la publicación on line de algunos antecedentes profesionales de las autoridades de Gobierno[190], en forma de versión pública en que claramente permite identificar a la autoridad, sin relevar mayores datos personales (salvo fecha de nacimiento), dando cuenta de su trayectoria académica y laboral. Por ejemplo, en el mismo sentido apunta la página web de Tribunal Constitucional[191].

IV.- Salario o remuneraciones

Las remuneraciones de los funcionarios públicas son una publicación obligatoria en la página web de los distintos organismos y servicios públicos, la que debe ser actualizada al menos una vez al mes. En efecto, según lo dispuesto por el artículo 7° letra d) de Ley N° 20.285 (Transparencia Activa), se debe publicar *"La planta del personal, y el personal a contrata y a honorarios, con las correspondientes remuneraciones"*. En el mismo sentido apunta la Instrucción N° 4 del Consejo para la Transparencia sobre Transparencia Activa, que se encarga de precisar algunos puntos. Esta obligación incluye la publicación del nombre de la persona, título académico o técnico, grado, región, salario mensual, escala de remuneraciones, asignaciones especiales, pago de horas extraordinarias, comisiones de servicio. Como buena práctica, el Consejo ha estimado como tal la publicación de la remuneración bruta y líquida (realizados los descuentos legales). Respecto de autoridades elegidas por elección popular o cualquier otro mecanismo de elección, indicar además el periodo por el cual ejerce la función, el acto administrativo en virtud del cual fue investido, dietas y cualquier otra contraprestación bruta o líquida. Asimismo,

[189] SCA rol 6344-10, Cons. 8°.
[190] Por ejemplo, del Presidente de la República, Ministros, Subsecretarios. http://www.presidencia.cl
[191] http://www.tribunalconstitucional.cl/wp/tribunal/integracion-actual

indica como buena práctica la publicación de la declaración de intereses y patrimonio de autoridades obligadas a realizarlas. Por último, indica como buena práctica la publicación de los viáticos percibidos.

¿Son públicas las liquidaciones de sueldo?

Ahora bien, en cumplimiento de las normas de transparencia activa en definitiva lo que se tiene que mantener actualizado son los montos totales percibidos, pero ¿Se puede tener acceso al documento que respalda dicho emolumento, por ejemplo, solicitando copia de la liquidación de sueldo de un funcionario público?[192] En los hechos, existen al respecto casos que han sido conocidos por el Consejo para la Transparencia, como en el C211-10, en donde se solicitaban entre otros documentos, copia de las liquidaciones de sueldo de varios trabajadores municipales. Frente al requerimiento, el organismo reclamado entregó parcialmente la información. Acudiendo de amparo el solicitante, éste indicó que la reclamada dio respuesta parcial a lo solicitado. El Municipio requerido indicó que puso en conocimiento a los potenciales afectados (artículo N° 20 Ley de Transparencia) los que se habrían opuesto verbalmente a la entrega de la información El Consejo razonó en base a los siguientes criterios, siendo generales para el caso de situaciones similares:

1.- Que siendo las liquidaciones de sueldo un documento en que constan tanto los ingresos como egresos de dinero pagados a los funcionarios públicos con ocasión de su trabajo y siendo obligación de la institución entregarla, esta información obra en poder de la administración, por lo tanto, en principio es pública (aplicación del artículo 5° y 10° de la Ley de Transparencia).

2.- Que según se constata, las liquidaciones de sueldo contienen una serie de datos respecto de los cuales cabe hacer un análisis para verificar su entrega o no. Así, figuran los RUT de los funcionarios públicos, cargas familiares, nombre de la Institución de Salud Previsional asociada, nombre de la Administradora de Fondos de Pensiones, horas extraordinarias, jornada de trabajo, días trabajados, otros descuentos (como adelantos). Respecto del RUT[193] de los funcionarios públicos, el Consejo para la Transparencia en la decisiones A283-10, A10-09, A126-09) ha indicado que se trata de un dato personal en los términos del artículo 7° de la Ley de Protección de Datos), por lo tanto, queda impedida su entrega aun cuando es un dato que obra en poder del Estado y que fue otorgado por el funcionario al momento de postular y entrar a trabajar a la Administración (artículo 13 del Estatuto Administrativo), pero que fue obtenido por ésta del propio interesado y no de un registro público. Por lo tanto, debe aplicarse el principio de divisibilidad[194], esto es, tachar el RUT del funcionario al momento de hacer entrega de la copia de la liquidación de sueldo. Respecto de los otros datos contenidos en las liquidaciones de sueldo debe aplicarse el mismo principio, tachando los descuentos legales (que son irrelevantes y de contexto para la ciudadanía) y los descuentos personales voluntarios que el trabajador haya contratado. El resto de la información, es pública.

V.- Declaraciones juradas

En nuestro país, la Ley sobre Probidad Administrativa incluyó la declaración de intereses, como un mecanismo para prevenir conflictos de intereses, la que se encuentra en el artículo 57[195] de la Ley N° 18.575, orgánica Constitucional de Bases de la Administración del Estado. Por otra parte la declaración de patrimonio no fue obligatoria sino hasta el año 2006, en que fue publicada la Ley N° 20.088[196], modificando la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, Ley N° 18.918, Orgánica Constitucional del Congreso Nacional, Código Orgánico de Tribunales, Ley N° 17.997, Orgánica Constitucional del Tribunal Constitucional, Ley N° 19.640, Orgánica Constitucional del

[192] La liquidación de sueldo es el documento extendido por el empleador, en que se detallan los ingresos y egresos por descuentos mensuales respecto la remuneración percibida por el trabajador durante generalmente un mes. Legalmente se entiende que *"…el empleador deberá entregar al trabajador un comprobante con indicación del monto pagado, de la forma como se determinó y de las deducciones efectuadas"*. Artículo 54 del Código del Trabajo.

[193] El RUT es un código numérico creado por el Decreto con Fuerza de Ley N° 3 de 1969, que permite identificar a todos los contribuyentes del país, tanto jurídicas como naturales.

[194] Decisión C211-10 Cons. "21) Que las remuneraciones percibidas por los funcionarios públicos tienen el carácter de información pública ya que dicen relación directa con el ejercicio de cargos y funciones públicas, y que, además, son pagados con fondos públicos, siendo objeto de transparencia activa. Sin embargo, el objeto al cual los funcionarios destinen voluntariamente dichas remuneraciones no guarda relación con el desempeño de sus funciones ni interfiere en el ejercicio de las mismas, siendo más bien una materia propia de la esfera de su vida privada, lo que lleva a este Consejo a concluir que la información pedida deberá ser entregada, aplicando el principio de divisibilidad, tajando la información contenida en las liquidaciones relativa a los gastos voluntarios efectuadas por los funcionarios a las que éstas se refieren"

[195] Artículo 57. El Presidente de la República, los Ministros de Estado, los Subsecretarios, los Intendentes y Gobernadores, los Secretarios Regionales Ministeriales, los Jefes Superiores del Servicio, los Embajadores, los Consejeros del Consejo de Defensa del Estado, el Contralor General de la República, los oficiales generales y oficiales superiores de las Fuerzas Armadas y niveles jerárquicos equivalentes de las Fuerzas de Orden y Seguridad Pública, los Alcaldes, Concejales Regionales deberán presentar una declaración de intereses, dentro del plazo de treinta días contado desde la fecha de asunción del cargo. Igual obligación recaerá sobre las demás autoridades y funcionarios directivos, profesionales, técnicos y fiscalizadores de la Administración del Estado que se desempeñen hasta el nivel de jefe de departamento o su equivalente. La obligación de presentar declaración de interés regirá independientemente de la declaración de patrimonio que leyes especiales impongan a esas autoridades y funcionarios.

[196] Moción Parlamentaria Boletín N° 2394-07

Ministerio Público, Ley N° 18.840, Orgánica Constitucional del Banco Central, Decreto Ley N° 211, Ley N° 18.460, Orgánica Constitucional del Tribunal Calificador de Elecciones, Ley N° 18.593, Orgánica Constitucional sobre Tribunales Electorales, Ley N° 18.695, Orgánica Constitucional de Municipalidades. Además, mediante esta modificación legal se reguló la declaración patrimonial para transparentar la evolución patrimonial de los directivos públicos.

Así, el marco regulatorio de las declaraciones de patrimonio e intereses es:

1) Artículos 57 y 60 a[197] de la Ley N° 18.575, Ley Orgánica Constitucional de Bases Generales de la Administración del Estado.

2) Manual de Transparencia y Probidad de la Administración del Estado elaborado por el Ministerio Secretaría General de la Presidencia.[198]

3) Decreto Supremo N° 99/2000, de la Secretaría General de la Presidencia, que aprueba el Reglamento de la declaración de intereses de autoridades y funcionarios de la Administración del Estado .

4) Decreto Supremo N° 45/2006, de la Secretaría General de la Presidencia, que aprueba el Reglamento de la Declaración de Patrimonio.

5) Reglamento para la Declaración Patrimonial de Bienes de la Ley N° 20.088.

¿Cuál es el contenido de las declaraciones de intereses?

La declaración de intereses deberá contar con las actividades profesionales[199] y económicas[200] en que participe la autoridad o el funcionario, detallando cada una de ellas. La declaración de intereses debe realizarse cada 4 años y cada vez que ocurra un hecho relevante que la modifique, considerándose de ese tipo cualquier hecho o actividad que afecte las actividades profesionales o económicas de los funcionarios. La actualización debe realizarse dentro de los 30 días anteriores a la fecha en que se cumplen los 4 años o dentro de los 30 días siguientes a la fecha que ocurra el hecho relevante. Se presentan 3 ejemplares, autenticados al momento de su recepción por el ministro de fe del órgano y organismo al que pertenezca o en su defecto ante notario público. Un ejemplar se remite a la Contraloría General de la República o Contraloría Regional para su custodia, archivos o consulta, otro ejemplar en la oficina del personal del órgano y otro al funcionario.

¿Cuál es el contenido de las declaraciones de patrimonio?

La declaración de patrimonio resultó ser obligatoria a partir del año 2006. Esta declaración contiene los puntos indicados en el artículo 60 c de la Ley N° 18.575, correspondiente ha:

a) Inmuebles del declarante, indicando las prohibiciones, hipotecas, embargos, litigios, usufructos, fideicomisos y demás gravámenes que les afecten, con mención de las respectivas inscripciones.
b) Vehículos motorizados, indicando su inscripción.
c) Valores del declarante a que se refiere el inciso primero del artículo 3º de la ley Nº 18.045, sea que se transen en Chile o en el extranjero.
d) Derechos que le corresponden en comunidades o en sociedades constituidas en Chile o en el extranjero.

La declaración contendrá también una enunciación del pasivo, si es superior a cien unidades tributarias mensuales.

Esta declaración se realiza cada 4 años, cuando el declarante sea nombrado en un nuevo cargo o cuando por cualquier causa concluya en sus funciones o cese del cargo que motivó su otorgamiento. Debe ser presentada dentro de los 30 días siguientes a la asunción en el cargo o la ocurrencia de algunos de los hechos que obligan actualizarla, ante el Contralor

[197] El artículo 60 A, establece que además deberán hacer una declaración de patrimonio, la que también deberán hacer los directores que representen al Estado en las empresas de sociedades anónimas.
[198] Disponible en . http://www.probidadytransparencia.gob.cl/assets/files/manual_transparencia_y_probidad_servicio_civil.pdf [fecha de consulta 31.10.2012].
[199] Por actividades profesionales se entiende que es el "ejercicio o desempeño de toda profesión u oficio, sea o no remunerado, cualquiera sea la naturaleza jurídica de la contratación y la persona, natural o jurídica, a quien se presten esos servicios". Además, se considerarán actividades profesionales las colaboraciones o aportes realizados a favor respecto de corporaciones, fundaciones, asociaciones gremiales u otras personas jurídicas sin fines de lucro que sean frecuentes y realizados en razón o con predominio de los conocimientos, aptitudes o experiencia profesional del directivo" (art. 3° y 4° Reglamento para la declaración de intereses de las autoridades y funcionarios de la Administración del Estado (D.S. 99/2000, Secretaría General de la Presidencia).
[200] Por actividades económicas se entiende que es el "ejercicio o desarrollo por parte de la autoridad o funcionario, de toda industria, comercio u otra actividad que produzca o pueda producir renta o beneficios económicos, incluyendo toda participación en personas jurídicas con o sin fines de lucro". (Art. 5° del Reglamento para la declaración patrimonial de bienes de la Ley N° 20.088).

General de la República o Contralor Regional para su consulta. Esta declaración, además comprende los bienes del cónyuge, siempre que estén casados bajo sociedad conyugal.
Ambas declaraciones son públicas, pudiendo ser consultadas en la Contraloría General o Regional según corresponda.

Respecto las declaraciones de intereses, estás pueden ser solicitadas vía acceso a la información pública, toda vez que como la Ley N° 18.575 indica, uno de los ejemplares obra en poder de la institución requerida, por lo tanto, ante una solicitud de acceso, cabría entregarla. Sin embargo, si estos documentos constan datos personales, como RUT, domicilio, teléfono, su entrega se encuentra prohibida por contravención a lo establecido en el artículo 7° de la Ley N° 19.628 (Decisión C1450-11), debiendo realizar tacha de los datos personales (Considerando 11 de la Decisión C444-10).

Distinta es la situación respecto las declaraciones de patrimonio, puesto que como indica la Ley N° 18.575 en el artículo 60 d, éstas deben ser presentadas ante la Contraloría General de la República o Contraloría Regional[201], no obrando en poder de la entidad eventualmente reclamada distinta al ente fiscalizador, por lo tanto, necesariamente debe ser realizada una solicitud de acceso a la información pública directamente ante la Contraloría, o en el caso que sea solicitada a un órgano que no la posea, debiera proceder a derivarla a ésta. Cabe tener presente, que respecto las decisiones de la Contraloría no es posible recurrir de amparo ante el Consejo para la Transparencia, sino que hacerlo directamente ante la Corte de Apelaciones respectiva.

Por otra parte, no existe obligación de publicar en el sitio web institucional de los funcionarios respectivos las declaraciones de patrimonio y de intereses, sino que es solamente indicado como una buena práctica de acuerdo a la Instrucción General N° 4 sobre "Transparencia Activa" del Consejo para la Transparencia.

Sin perjuicio de lo anterior, los Diputados y Senadores tienen obligación de publicar sus declaraciones de intereses y patrimonios de acuerdo a lo indicado en la Ley Orgánica del Congreso Nacional (artículos 5 c de la ley N° 18.918), en las páginas web institucionales. En el mismo sentido apuntan lo indicado en los reglamentos de ambas cámaras (art. 6 bis del Reglamento del Senado y art. 7 letra i del Código de Conductas Parlamentarias).

Ejerciendo las potestades que otorga la Constitución Política de Chile en el artículo N° 93, el Tribunal Constitucional, con motivo del control de constitucionalidad preventivo de la Ley N° 20.088, hace algunas precisiones respecto el sentido del término "consulta" o "consulta pública" respecto la frase "quien dará copia a quien los solicite". En efecto, ejerciendo el control, el intérprete constitucional arriba a la conclusión que es necesario realizar un examen en relación con lo dispuesto en el artículo 19 N° 4 de la Constitución, en cuanto asegura a todas las personas el respeto y protección a la honra y de la vida privada. En este sentido, dice el Tribunal "*el acceso por terceros a esa información (la contenida en las declaraciones de patrimonio), ha de serlo para las finalidades legítimas que la nueva normativa persigue, circunstancia esencial*
Que exige que todos los órganos del Estado involucrados por tales disposiciones, interpretarlas y aplicarlas con el objetivo señalado"[202]. En los hechos, esto se traduciría en una prohibición de publicación irrestricta. Sin perjuicio de lo anterior, varios organismos las han publicado en sus respectivos sitios web[203].

VI.- Sanciones administrativas

La aplicación de medidas disciplinarias debe acreditarse mediante sumario administrativo o investigación sumaria para efectos de establecer la responsabilidad administrativa en que pudiere incurrir un funcionario público[204]. La investigación sumaria tiene por objeto verificar la existencia de los hechos, la individualización de los responsables y determinar su participación. El sumario administrativo se lleva a cabo cuando se constatan hechos de mayor gravedad. En ambos casos, de ser responsables, los funcionarios públicos pueden ser objeto de alguna de las medidas disciplinarias que contempla la ley, como son la censura, multa, suspensión o destitución. Todo el procedimiento consta en un expediente administrativo, en el que se encuentran las diferentes actuaciones llevadas a cabo, es decir, los actos administrativos.

[201] Así, expresamente lo ha indicado la Contraloría General de la República en el dictamen N° 15.988 de 26 de marzo de 2010, indicando que *"No es función del organismo en donde se desempeña el declarante el recibir ni enviar las declaraciones de patrimonio, toda vez que dichas declaraciones, de conformidad a lo dispuesto en el artículo 60 d de la ley Nº 18.575, deben ser presentadas directamente a esta Entidad Fiscalizadora, pues no participa en dicho proceso el ministro de fe del Servicio, a diferencia de lo que ocurre con las declaraciones de intereses, por lo que la respectiva repartición no debiera llevar a cabo procedimiento administrativo alguno respecto de aquella declaración, a excepción de los que se deriven de la obligación que asiste al jefe de personal de la institución respectiva de velar por su confección y presentación oportuna."*
[202] STC 460-2005. Considerando 31°
[203] Por ejemplo, pueden examinarse las declaraciones de intereses y patrimonios de los Consejeros del Consejo para la Transparencia en su sitio web. http://www.cplt.cl/otras-autoridades/consejo/2012-01-10/154719.html [fecha de consulta 4.11.2012]. El Consejo para la Transparencia, además, en su sesión N° 101 de 9 de noviembre de 2009, acordó la necesidad de fijar las abstenciones establecidas en el Estatuto de la Corporación, mediante el "Acuerdo del Consejo para la Transparencia sobre Tratamiento de Conflictos de Intereses".
[204] Artículo 119 del Decreto con Fuerza de Ley N° 29, que aprueba la Ley N° 18.834, que fija el texto refundido, coordinado y sistematizado sobre Estatuto Administrativo.

Tanto la investigación sumaria como la instrucción de sumario, terminan con la resolución del jefe de la institución, que en definitiva, previa apreciación de los hechos y la prueba rendida, impone la sanción al funcionario o lo declara inocente.

De acuerdo a la Ley sobre Procedimientos Administrativos, los expedientes administrativos son públicos una vez concluidos, esto es, existe un acto administrativo terminal que pone fin a la investigación en este caso. Durante la tramitación, sólo son públicos para las partes interesadas en el resultado de ésta.

La jurisprudencia del Consejo para la Transparencia, en amparos en que lo solicitado corresponde precisamente a copias del sumario o carpeta de investigación o la copia de la resolución del jefe del servicio que impone la sanción, se ha pronunciado negando el acceso a dichos documentos mientras no esté afinado o terminado el sumario o investigación, puesto que éste es secreto mientras se encuentre pendiente, el cual sólo se levanta anticipadamente para el inculpado y su abogado (criterio sostenido en decisiones roles CA47-09, A95-09, A159-09, A411-09, C07-10, C561-11, C903-12). En estos casos, la entidad requerida debiera negar el acceso a la información aplicando la causal del reserva del artículo 21 N° 1 letra a), esto es, cuando la entrega de la información pudiera ir en desmedro de la investigación. En el mismo sentido apunta el Dictamen de la Contraloría General de la República N° 11.341/2010, al indicar que "*sólo una vez afinado el referido sumario administrativo, éste se encuentra sometido sin limitaciones al principio de publicidad, que constituye la regla general respecto de todos los actos de la Administración del Estado, conforme lo señalado en el dictamen N° 59.798, de 2008, pudiendo ser conocido, sólo a partir de esa instancia".*

Por otra parte, encontrándose afinado el sumario, el Consejo para la Transparencia ha indicado que éste es público, de acuerdo a los artículos 5° y 10° de la Ley de Transparencia (Decisiones Roles A47, A95-09 y A327-09).

Queda pendiente entonces la alegación que pudieren formular aquellos funcionarios públicos que fueron sancionados, cuya divulgación pudiere afectar su honra o vida privada. Al respecto, el Consejo ha seguido el criterio sentado en la decisión rol C411-09, en que lo solicitado era copia de los decretos alcaldicios mediante los cuales fueron destituidos ciertos funcionarios de una Municipalidad, indicando el respecto que:

a) Por aplicación del Test de Daño (Decisiones roles 617-09 y 664-10), la divulgación de tal información respecto de los ex funcionarios, el beneficio de conocer esa información sobre los resultados de un sumario incoado por supuestas irregularidades, que ya es público, así como las medidas que las autoridades tomaron frente a dichas irregularidades, es mucho mayor que mantener la información en reserva para proteger la reputación de los funcionarios sancionados. Así lo exige el control social de la función pública, pues ésta debe ejercerse con transparencia. Si un funcionario incurre en un acto ilegal o irregular es del todo relevante que la ciudadanía conozca dichos actos y las medidas disciplinarias para restaurar el imperio del derecho.

b) Que el ejercicio de funciones públicas interesa a toda la comunidad y, por lo mismo, la condición de funcionario público supone un estándar de escrutinio público en el que la privacidad, en lo relativo al ejercicio de dicha función, debe ceder en pos del necesario control social que debe ejercerse para garantizar el debido cumplimiento de aquellas.

c) Existe una disposición en la Ley de Protección de Datos Personales, que en su artículo 21, inciso primero (respecto del tratamiento de datos personales por organismos públicos) indica que: "*Los organismos públicos que sometan a tratamiento de datos personales relativos a condenas por delitos, infracciones administrativas, o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena*[205]*".*Por lo tanto, existiría una suerte de protección a la honra o vida privada de aquellas personas que han sido sancionadas, cuyos motivos o razones no podrían ser dados a conocer sino en las situaciones descriptas: prescrita la acción o la pena, o cumplida ésta. Sin embargo, el Consejo ha estimado que respecto de los archivos de los expedientes disciplinarios al interior de un organismo, así como de los actos administrativos que disponen una medida disciplinaria, no constituiría tratamiento de datos personales según lo dispuesto en el artículo 1° de la Ley de Protección de Datos, por lo que la aplicación del artículo 21 descrito anteriormente del mismo cuerpo legal no impediría hacer entrega de la información. Inclusive, pese a la probable oposición de terceros con la entrega de la información, la fundamentación del eventual daño que produciría la entrega de la información debe ser no solo probable, sino que específico.

d) En relación con lo anterior, y conforme a la rectificación de la Decisión A39-09, la aplicación del artículo 21 de la Ley N° 19.628, dicha normativa no es aplicable a las personas jurídicas, criterio

[205] De acuerdo al artículo 158 del Estatuto Administrativo, la prescripción de la acción disciplinaria prescribe pasado cuatro años desde el día en que el funcionario hubiere incurrido en la acción y omisión que le da origen. Ésta se suspende desde el momento en que se presentan cargos contra el inculpado en la investigación o sumario.

confirmado por sentencias de la Corte de Apelaciones roles N° 5610-2005 y 6545-2006 (Considerando 5°, Decisión A41-09).

VII.- Evaluaciones de desempeño

Sobre este caso, el Consejo ha sentado alguno de los siguientes criterios:

a) En un caso conocido por el Consejo, precisamente se requería, entre otras cosas, le fuera entregada al solicitante la programación individual de desempeño del último trimestre de cada uno de los funcionarios del estamento fiscalizador de la Región de Valparaíso y de la Dirección del Trabajo de la misma Región. En este caso, el Consejo concluyó que dentro de dicha información se incluye información respecto de cada funcionario, como su nombre, Rut y cargo, además de las metas propuestas, dimensiones de meta, el indicador y la ponderación que se le asignó a cada una. Dichos programas se realizan para precalificar al personal y sirven de base para su posterior calificación (Considerando 1° Decisión Rol C323-09).

Agregando que "dichos programas de desempeño son información pública de acuerdo a lo prescrito por los artículos 5° y 10 de la Ley de Transparencia, particularmente considerando que se trata de información relativa a la función pública que estos desempeñan y no a su vida privada. Lo anterior con la salvedad del R.U.T. de los funcionarios por las razones señaladas por este Consejo en las decisiones de los amparos A10-09, contra el Ministerio de Vivienda y Urbanismo, y A126-09, contra el Fondo Nacional de Salud".

b) Asimismo, ha sentado la importancia que reviste el conocimiento público de conocer las calificaciones funcionarias como mecanismo de rendición de cuentas no sólo ante las jefaturas, sino también ante la sociedad, criterio que cabría aplicar toda vez que la información solicitada se relaciona directamente con las calificaciones de los funcionarios públicos (criterio ya sostenido en las decisiones roles A10-00 yA126-09).

c) De existir datos personales de los funcionarios públicos contenidos en la documentación en que constan las programaciones de desempeño, como R.U.T o domicilio, éstas deben ser tachada por aplicación del principio de divisibilidad de la Ley de Transparencia.

VIII.- Antecedentes penales y policiales.

De los casos que fueron encontrados en la jurisprudencia del Consejo para la Transparencia, figuran las siguientes situaciones:

a) Solicitud de datos personales de terceras personas

En general, la tesis del Consejo es negar el acceso a información que obre en poder de los organismos públicos que diga relación con datos personales. Siendo los antecedentes penales y policiales de aquellos, la regla general nos indica que deben ser privados. La salvedad ocurriría en el caso que fuera el propio titular el que solicitare acceder a sus propios datos, inclusive sensibles en los términos de la Ley N° 19.628, accediendo a ellos a través del procedimiento de acceso de datos o habeas data del artículo 12 de la mencionada ley.

b) Solicitud de información sobre órdenes de aprehensión

Al menos en dos casos contra la misma institución, Policía de Investigaciones de Chile, el Consejo frente a un requerimiento en que lo solicitado dice relación sobre la existencia de órdenes de aprehensión vigentes, reconoce que la requerida puede poseer la información luego de un análisis de la legislación aplicada a la institución para cumplir con su función, cual es entre otros, el cumplimiento oportuno de las órdenes de aprehensión y arrestos pendientes decretados por los Tribunales.

Además señala, en cuanto al contenido de la solicitud, se solicita una serie de actuaciones judiciales, denominados registros, que son de libre acceso para los intervinientes. Sin perjuicio de lo anterior, los terceros podrían consultar dichos registros cuando dieran cuenta de actuaciones públicas de acuerdo a la ley.

Agrega el Consejo que si el juez ya realizó una evaluación sobre la afectación de la sustanciación o el principio de inocencia o indicó su reserva o secreto o publicidad*, "el órgano solicitado deberá respetar dicha calificación en la medida en que se encuentre dentro del plazo de 5 años a que se refiere el artículo 44 del Código Procesal Penal. Por lo tanto, si la actuación define que es secreta dicha orden deberá denegarse el acceso y, en caso contrario y de no decir nada, deberá accederse a la entrega, por ser la publicidad la regla general en esta materia (art. 9° del Código Orgánico de Tribunales"* (Considerando 7° Decisión Rol C843-10). En el mismo sentido respecto de la decisión C516-11, recurrida de ilegalidad ante la Corte de Apelaciones de Santiago, quien acogió la tesis del Consejo (SCA rol N° 6252-2011), poniendo acento en que la Policía de Investigaciones contaba con esa información.

IX.- Información vinculada a la Salud
Informe Psicológico:

A este respecto el Consejo se ha pronunciado en la causa Rol: C971-12, 26/10/2012 al resolver un amparo interpuesto por una funcionaria pública en contra de la Dirección Nacional del Servicio Civil, fundado en que recibió respuesta negativa a la solicitud de información sobre entrega del informe psicológico que le fue realizado, con motivo de la postulación al concurso público para el cargo de Jefe de Departamento Jurídico en dicho servicio, realizado el año 2011.
El Consejo señaló que se configura una afectación cierta, probable y específica de este sistema de reclutamiento, de manera que aplicando un test de daño ocurre que el beneficio público resultante de conocer esta información es inferior al daño que podría causar su revelación. De allí que se estime que respecto de estos informes deba aplicarse la causal de reserva del art. 21 Nº 1 de la Ley de Transparencia, sin embargo, es posible aplicar el principio de divisibilidad y entregar **sólo los puntajes asignados en dichos informes** (tanto por la consultora como por el Consejo de Alta Dirección o Comité de Selección, según el caso, cuando: i) los requiriese la propia persona evaluada, ii) se tratase de los puntajes del ganador (que se declaran públicos) y iii) fuesen puntajes de terceros incluidos en la terna o quina que, tras la aplicación del art. 20, consintieran en ello o no se opusieran oportunamente.
Por otra parte, el Consejo en la causa Rol Nº C614-09, 23/04/2010 en que resolvió un amparo interpuesto por una funcionaria de la Policía de Investigaciones de Chile (PDI) contra la propia institución, frente a la respuesta parcial a la solicitud de acceso a todos los antecedentes sicológicos y psiquiátricos referidos a ella que mantenga la PDI. El Consejo estimó que la entrega de evaluaciones sicológicas y psiquiátricas no afectan el debido cumplimiento de las funciones de la PDI, porque este caso se trata de una evaluación síquica de la reclamante que no dice relación con un proceso concursal ni con la comparación del solicitante con otros postulantes y, que la entrega tampoco afecta los derechos de terceros, pues la requirente está legalmente autorizada a conocer y es titular de los datos de carácter personal que se contengan.

3.3.- Casos resueltos por las autoridades de aplicación sobre las tensiones entre el derecho a saber y la protección de datos personales.

De acuerdo al Director Jurídico del Consejo para la Transparencia, durante el año 2011, cerca "*de la cuarta parte de las decisiones de fondo dictadas por el CPT durante el último trimestre tuvieron que ver con datos personales, en mayor o menor medida, esto es, una de cada cuatro, lo que significa que es relativamente frecuente que deba aplicarse la LPDP*"[206]. En relación a lo anterior, la Unidad Normativa dependiente de la Dirección Jurídica del Consejo elaboró un documento sobre "Jurisprudencia relevante del Consejo para la Transparencia en relación a la Protección de Datos Personales" (Abril, 2011), en el cual se detallan una serie de datos tanto cualitativos (análisis de casos) y cuantitativos (casos en que se ha dado aplicación a la Ley de Protección de Datos en materias de Transparencia).

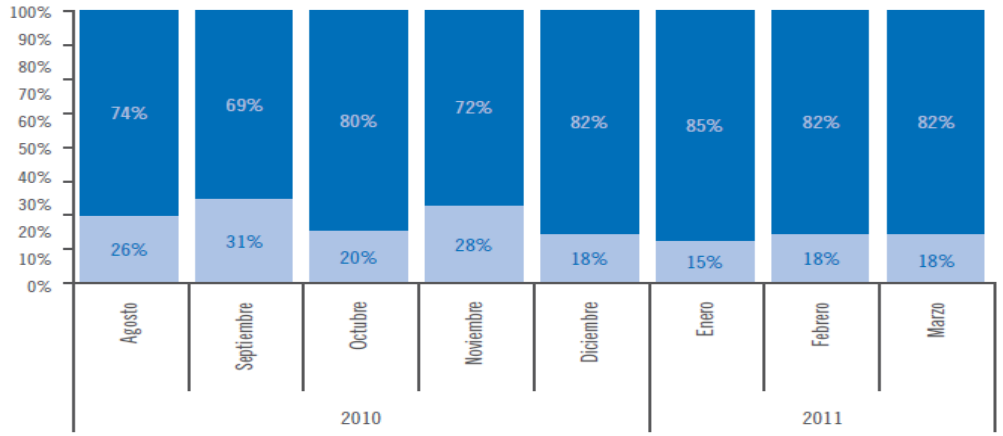
De acuerdo a los datos proporcionados en el referido documento, se anexan las siguientes tablas que dan cuenta de la relación entre número de solicitudes, decisiones de fondo, aplicación de la Ley de Protección de Datos y Ley de Transparencia.

TABLA 1
Número de decisiones con decisión despachada, según su tipo, desglosada según aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

AÑO	MES	DECISIÓN DE FONDO			DECISIÓN INADMISIBLES Y OTROS			TOTAL DECISIONES		
		Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total	Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total	Con Aplicación de Ley de Protección de Datos Personales	Sin Aplicación de Ley de Protección de Datos Personales	Total
2010	Agosto	13	31	44	12	42	54	25	73	98
	Septiembre	16	40	56	16	31	47	32	71	103
	Octubre	9	50	59	9	23	32	18	73	91
	Noviembre	16	61	77	16	21	37	32	82	114
	Diciembre	22	49	71	0	48	48	22	97	119
2011	Enero	14	40	54	0	37	37	14	77	91
	Febrero	16	32	48	0	40	40	16	72	88
	Marzo	26	40	66	0	79	79	26	119	145
Total		132	343	475	53	321	374	185	664	849

[206] Ob. Cit. P. 151.

GRÁFICO 2
Distribución de porcentaje mensual del total de decisiones despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



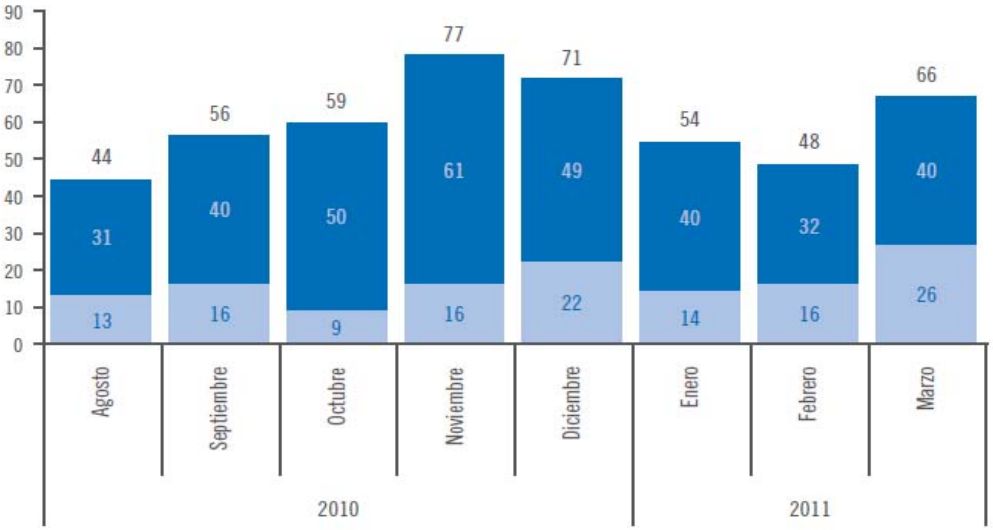
Fuente: Unidad de Reportes y Estadísticas - CPLT

Sin aplicación de Ley de Protección de datos personales

Con aplicación de Ley de Protección de datos personales

DECISIONES DE FONDO

GRÁFICO 3
Distribución de Número total mensual de decisiones de fondo despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

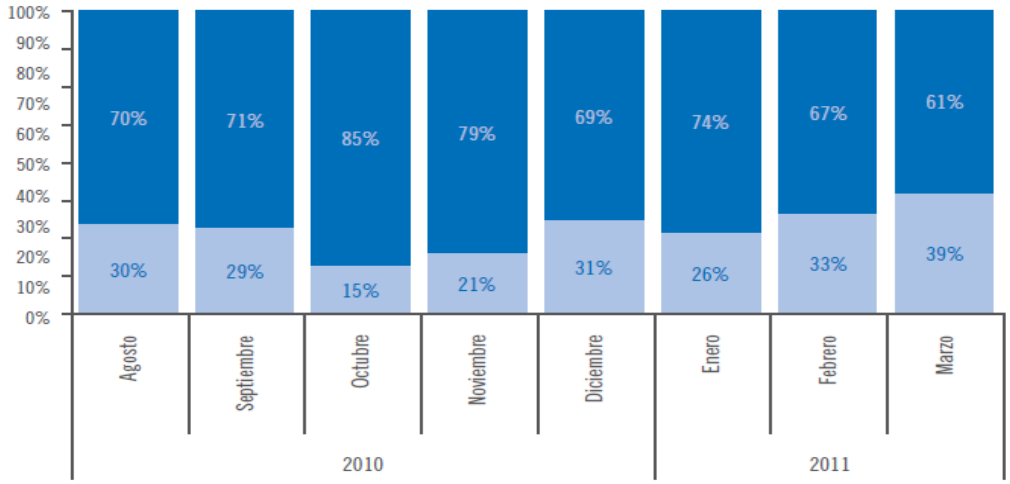


Fuente: Unidad de Reportes y Estadísticas - CPLT

Sin aplicación de Ley de Protección de datos personales

Con aplicación de Ley de Protección de datos personales

GRÁFICO 4
Distribución de porcentaje mensual del total de decisiones de fondo despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



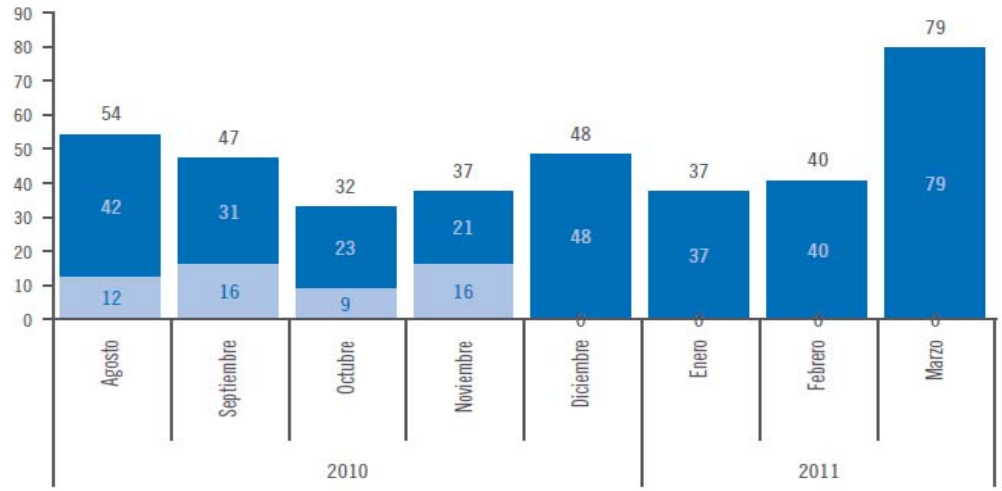
Fuente: Unidad de Reportes y Estadísticas - CPLT

Sin aplicación de Ley de Protección de datos personales

Con aplicación de Ley de Protección de datos personales

DECISIONES INADMISIBLES Y OTROS

GRÁFICO 5
Distribución de Número total mensual de decisiones inadmisibles y otras despachadas, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011

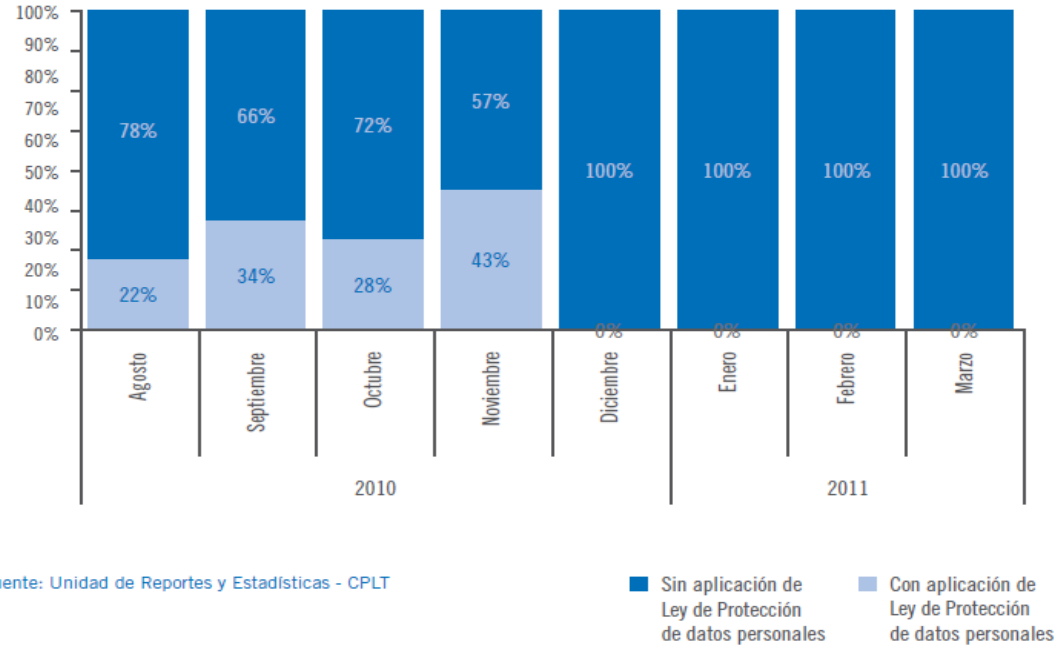


Fuente: Unidad de Reportes y Estadísticas - CPLT

Sin aplicación de Ley de Protección de datos personales

Con aplicación de Ley de Protección de datos personales

GRÁFICO 6
Distribución de porcentaje mensual del total de decisiones inadmisibles y otras, según Aplicación de Ley de Protección de Datos Personales, entre los meses agosto 2010 y marzo 2011



Fuente: Unidad de Reportes y Estadísticas - CPLT

Sin aplicación de Ley de Protección de datos personales

Con aplicación de Ley de Protección de datos personales

Caso SERVEL (Decisión de amparo Rol C407-09)

El día 1 de octubre de 2009, Sebastián Rivas solicitó al Servicio Electoral (SERVEL) "*copia del padrón alfabético computacional de inscripciones electorales vigentes, varones y mujeres".*
Frente a la solicitud de acceso, el SERVEL respondió básicamente que el padrón electoral se encuentra a la venta como un producto electoral del órgano y puede ser adquirido por cualquier persona, previo pago de $21.698.799 pesos chilenos. Inclusive se puede pedir desagregado por Región (pudiendo consultarse en la página web, sección "Catálogo de Productos Electorales".
Ante esta respuesta, el requirente recurrió de amparo al Consejo para la Transparencia, por el pago asociado, fundado en que el monto exigido resulta excesivo siendo que son datos públicos. Agrega que tal costo podría ser válido en el sentido que lo hubiera requerido impreso, pero éste fue solicitado de manera digital (CD), utilizando la expresión "*padrón alfabético computacional".* Agrega que se adujeron una serie de normas legales para justificar su cobro, replicando que en este caso se ha vulnerado el artículo N°18 de la Ley de Transparencia toda vez que éste exige el pago de los costos de reproducción por la entrega de la información. Finalmente, el mismo requirente plantea la preocupación por parte del contenido del padrón electoral, que contiene una serie de datos personales, inclusive sensibles, que son necesarios entregar para votar, pero ello no significa un consentimiento para hacerlos públicos.
En sus descargos, el SERVEL aduce que:

a) El costo cobrado se encuentra establecido en la Resolución Exenta N° 862/2002, del SERVEL.

b) Indica que al SERVEL le son aplicables las normas sobre Normas Complementarias de Administración Financiera (Ley N° 17.768 de 1988), que en su artículo N° 83 indica *"Facúltese a los Servicios dependientes de la Administración Central y descentralizada del Estado, del Poder Legislativo y del Poder Judicial, para cobrar el valor del costo de los documentos o copias de éstos que proporcionen a los particulares para la celebración de contratos, llamados a licitación o por otra causa, y cuya dación gratuita no esté dispuesta por ley, sin perjuicio de mantener a disposición de los interesados los respectivos antecedentes cuando ello proceda. También podrán cobrar por la reproducción de fonogramas, video gramas e información soportada por medios magnéticos, sus copias o traspasos de contenidos".*

c) Así, agrega, que en cumplimiento del Ordinario N° 877/2009 del Ministerio Secretaría General de la Presidencia, que impartió instrucciones sobre la fijación de los costos de reproducción en relación

con el artículo 18 de la Ley de Transparencia, el SERVEL dictó la Resolución Exenta N° 1079/2009, que estable que el valor del as inscripciones electorales por cada 1.000 es de 0.06030 UTM ($2.205).

En los considerandos, el Consejo para la Transparencia razona de la siguiente manera:

a) En primer lugar, fundamenta que el artículo 25 de la Ley N° 18.556 de 1986, Orgánica Constitucional sobre el Sistema de Inscripciones Electorales y el Servicio Electoral, declara que los registros electorales son públicos.

b) A continuación, indica una serie de información contenida en estos registros, según lo prescrito por el artículo 27de la Ley Orgánica mencionada, a saber: a) numeración impresa y sucesiva de cada una de las inscripciones, con la anotación abreviada de su fecha, b) anotación de los nombres y apellidos que constan en la cédula de identidad, c) nacionalidad, d) Profesión u oficio, e) Domicilio, con indicación de la comuna y calle o camino con su numeración o el nombre del predio, f) número de cédula de identidad para extranjeros, g) En caso de extranjeros debe dejarse constancia de que cumplen con el requisito de avecindamiento exigido para sufragar, h) Constancia de la cancelación de la inscripción, con indicación de la causal y fecha, i) Firma de la persona inscrita o constancia de la calidad de no vidente y analfabeta estampada por la Junta inscriptora y, por último, impresión del pulgar derecho de la persona inscrita o del izquierdo o constancia de la causa que le imposibilite absolutamente para estamparla.

c) Recalca, qué, dicha información, es pública según consignó el artículo 25 de la LOC N° 18.556.

d) Que tal como indicó en su respuesta original al requirente, el SERVEL indicó que en la página web, sección “catalogo de productos”, el padrón electoral computacional es *“la información de las inscripciones electorales vigentes, registradas en el Padrón Electoral Alfabético Computacional”*, indicando una serie de antecedentes de entrega y comerciales, como el formato de entrega, datos que contiene (idénticos a los de los registros físicos), etc.

e) Luego entra en el análisis de los costos de reproducción, resaltando los principios de gratuidad contemplado en la Ley de Transparencia (art. 11 letra k), relacionado con el artículo 18 (que establece el pago de los costos de reproducción), complementado con el inciso 3° del Reglamento de la Ley de Transparencia, que expresa en resumen que sólo se puede cobrar por los costos directos de reproducción, como los necesarios para obtener la información, en el soporte solicitado, excluyendo el tiempo de los funcionarios para recolectar la información.

f) A reglón seguido, la discusión se enmarca en señalar la validez del costo de reproducción cobrado por el SERVEL y la nueva disposición de la Ley de Transparencia. Así, el costo dispuesto por el servicio en atención a incrementar el valor solo tiene validez en cuanto el valor del soporte sea más caro, pero en este caso no lo es (sólo el valor de un CD). Por lo tanto, el Consejo estima que debe pagarse el costo directo de reproducción, equivalente a un CD, tal como lo exigiera el requirente.

g) Agrega, que con la entrada en vigencia de la Ley de Transparencia, ésta prevalece por sobre las Resoluciones que hubieren sido dictadas con anterioridad, las que siendo un número tan elevadas, en realidad serían un entorpecimiento fáctico de acceso a la información.

h) Finalmente, el Consejo se pronuncia sobre las inquietudes manifestadas por el requirente, en cuando la divulgación de datos personales, inclusive sensibles. Ante esto, el Consejo indica que es la Ley Orgánica Constitucional sobre Votaciones y Servicio Electoral la que indica que es pública, por lo tanto, el Consejo no cuenta con las atribuciones para requerir al SERVEL tachar los datos personales en cumplimiento con la Ley de Protección de Datos Personales, ya que ésta fue aprobada con quórum simple, estimando que no es posible estimar que derogó tácitamente a una norma aprobada con quórum orgánico constitucional como el exigido por la Ley N° 18.556. Lo anterior, por mandato Constitucional, en cuanto el artículo 18 de la Carta Fundamental, indica que el sistema electoral público no pudiendo subordinarse su interpretación a una norma legal simple, pues su regulación fue ordenada a una de mayor jerarquía. Por esto, pese a jurisprudencia contraria del Consejo, en el sentido de no entregar datos personales como el número de cédula de identidad, estima que en este caso es necesario otorgarlo para asegurar un control social , puesto que de esta manera es posible verificar que no existan inscripciones duplicadas.

i) Voto disidente: EL Consejero Juan Pablo Olmedo indicó en voto disidente que en realidad lo que dice la Ley Orgánica Constitucional es que los “libros son públicos”, no así el padrón alfabético. Es más, indico que de acuerdo a la Ley N° 19.628, aplicando el artículo 2° letra m), el registro o banco de datos permite *“relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos”*. Así, un banco de datos sólo podría crearse cuando la ley lo autorice y en atención al principio de

finalidad del artículo 9°, los datos allí contenidos "*deben utilizarse solo para los fines para los cuales se hubieren recolectado"*. Además, la Ley N° 19.628, sólo permite el trato de datos por parte de organismos públicos cuando actúan dentro de las materias de su competencia y con sujeción a las reglas que indica o con el consentimiento de su titular. Así, en materia electoral, no todos los datos que indica la ley que deben registrarse cumplen una finalidad electoral, como son la profesión, domicilio, fecha de nacimiento, número de cédula de identidad, todos los cuales no resultan necesarios para controlar esos procesos. Así – advierte el consejero Olmedo- el bajo costo de la reproducción de la información en soporte electrónico, arriesga severamente el derecho a la intimidad de las personas, ya que cualquiera podría utilizarlos, siendo que el SERVEL no estaría autorizado a realizar tratamiento automático de datos. Lo anterior, es más grave tratándose de datos sensibles como la circunstancia de ser no vidente o analfabeto (salvo cuando se autoriza su tratamiento de acuerdo al artículo 10 de la Ley N° 19.628). Finaliza indicando la experiencia comparada que es más cautelosa a la hora de hacer entrega de la información, citando el caso de México, Reino Unido y España.

Públicamente, la decisión del Consejo fue duramente criticada por diversos sectores. En los hechos, se tradujo básicamente en que previo al pago de alrededor de $200 pesos chilenos se puede actualmente comprar el padrón completo e inclusive costo $0 si se lleva el CD o pendrive. La situación se agrava aún más con la entrada en vigencia de la ley sobre inscripción automática y voto voluntario, a través del cual, el padrón electoral subió a un 65% de posibles votantes, incluyendo respecto de cada uno de ellos, todos los datos antes señalados. Así, el propio Consejo para la Transparencia en una declaración pública[207], en atención a la entrada en vigencia de la Ley N° 20.568, sobre inscripción automática, indicó que la anterior decisión tomó en consideración la regulación vigente en la época, y que tras la publicación en el sitio web del SERVEL con el sólo nombre, se podía tener acceso al domicilio y demás datos personales de todas las personas (un universo de cerca de 13.000.000 de chilenos), indicó que la nueva ley había modificado disposiciones en relación con la publicidad de los registros y el padrón, no siendo responsabilidad de la decisión adoptada el año 2010 lo que acontecía en su momento. Asimismo, en relación con el control preventivo que realizará el Tribunal Constitucional del proyecto de ley, mediante la STC rol N° 2152-11, considerando 32[208] indicó que habiéndose establecido por la nueva ley un procedimiento especial de acceso a la información del registro electoral, deberá regirse por estas disposiciones, prevaleciendo las de la LOC N° 18.556.

Así, la nueva forma de publicar la información sobre registro electoral, se realizaría por medio de la página oficial del SERVEL, pudiendo los electores verificar sus datos por medio del ingreso de su cédula de identidad o nombre (artículo 7° y 32° de Ley N° 20.568), lo que causó aun más revuelo[209] por la mayor facilidad con la que se podía realizar la consulta de los datos de los votantes. Inclusive, siendo conformado el padrón definitivo, éste podía ser descargado en formato PDF sin ninguna restricción, desagregado por comuna y región. Ahí, surgieron voces encontradas entre el Director del SERVEL, quien precisó que por ley, la información era pública, culpando al Consejo para la Transparencia y al Tribunal Constitucional, quienes ratificaron que así era. Por su parte, el Gobierno insistió en que la publicación de la nueva Ley de inscripción automática y voto voluntario, no obligaba al SERVEL a difundir esos datos[210].

---

[207] Disponible en http://www.consejotransparencia.cl/declaracion-publica/consejo/2012-04-27/180025.html [Fecha de consulta 5.11.2012]

[208] Considerando 32° "Que la disposición contenida en el inciso primero del nuevo artículo 4° que el numeral 1) del ARTÍCULO PRIMERO del proyecto introduce a la Ley N° 18.556, establece que *"el conocimiento público del Registro Electoral procederá en la forma dispuesta en el Párrafo 1° del Título II"*. Conforme a dicha disposición debe concluirse que, sin perjuicio de que el órgano público denominado Servicio Electoral se rija por la Ley N° 20.285, sobre Acceso a la Información Pública, el acceso a la información contenida en el Registro Electoral se efectúa únicamente en la forma que el proyecto de ley establece, sin que quepa aplicar las disposiciones de la Ley N° 20.285. Por de pronto, porque el legislador orgánico constitucional ha establecido un mecanismo especial de acceso, dada la relevancia e importancia que contiene, para el sistema democrático, el Registro Electoral, excluyendo otros mecanismos. Enseguida, porque la normativa se enmarca dentro del artículo 18 de la Constitución, que obliga a establecer un *"sistema electoral público"*. No se trata, en consecuencia, de forzar la integración de dos mecanismos legales. El proyecto de ley estableció su propio mecanismo, su propio sistema. Además, la ley del artículo 18 de la Constitución exige que ese sistema se rija por una ley orgánica constitucional, lo que no ocurre con la mayoría de los preceptos de la Ley N° 20.285. En consecuencia, el nuevo artículo 4º de la Ley N° 18.556, con excepción de su inciso segundo, se declarará conforme con la Constitución, en el entendido de que el acceso a la información contenida en el Registro Electoral se regirá exclusivamente por las normas de esta ley orgánica constitucional"

[209] Pueden consultarse una serie de publicaciones en medios de comunicación que alertan sobre esta problemática. Así, http://www.biobiochile.cl/2012/08/19/servel-revela-padron-electoral-completo-incluyendo-datos-personales-de-los-electores.shtml [fecha de consulta 28.10.2012], http://radio.uchile.cl/noticias/149820/ [Fecha de consulta 28.10.2012], http://www.lanacion.cl/servel-justifica-publicacion-de-los-datos-personales-de-los-electores/noticias/2012-08-20/123207.html [Fecha de consulta 29.10.2012]

[210] http://www.lanacion.cl/servel-aplica-filtro-para-resguardar-datos-privados-en-la-web/noticias/2012-04-27/124340.html [Fecha de consulta 28.10.2012].

Nómina de afiliados a un Sindicato:

El siguiente análisis de casos que se expone, dice relación con un cambio jurisprudencial de parte del Consejo para la Transparencia, que resulta notorio u favorable a proteger la identidad de determinadas personas que participan en sindicatos de trabajadores. En un principio, la tesis seguida por el Consejo para la Transparencia en las decisiones roles C108-10, C250-10, C866-10, C839-10, C59-11, C188-11, C492-11 y C532-11, frente a requerimientos de empleadores que solicitaban a la Dirección del Trabajo la nómina de afiliados a un sindicato, quiénes participaron en su constitución y a las solicitudes de afiliación, así como copias autorizadas de los documentos relacionados con dichas afiliaciones, fue la de hacer entrega de la información solicitada. En primer lugar, despejando la duda sobre que dicha información no ha sido elaborada por un órgano de la Administración del Estado, sino que por un órgano que no pertenece a ésta, sin perjuicio de lo anterior, obra en poder de la Inspección del Trabajo, por lo tanto, en principio es pública (aplicación del artículo 5° de la Ley de Transparencia). Pese a las alegaciones de los terceros (sindicato), en orden a oponerse a la entrega de la información fundamentado en que la divulgación de la información afectaría la afiliación y autonomía sindical, daría pie a la toma de represalias por parte del empleador al conocer la nómina de los trabajadores sindicalizados y la falta de causa para pedir. El Consejo desestimó dichas alegaciones, agregando que el régimen legal otorga una serie de elementos que impiden las represalias contra trabajadores, por lo tanto, no se ha probado el daño probable, específico y presente de los terceros con la divulgación de la información (Considerando 17° y ss). En el mismo sentido, respecto la decisión C250-10, en que la empresa solicita copia fiel e íntegra de los estatutos y registros de participantes en la constitución del sindicato, el Consejo resuelve, en que previa comunicación de eventual afectación de derechos de terceros (el sindicato), éstos accedieron a hacer entrega de los estatutos, pero no así de los registros de participantes que fue lo que motivó el amparo, argumentando la negativa de la entrega de información por afectación de derechos de terceros (art. 21 n° 2 de la Ley de Transparencia). En este caso, si bien el Consejo dispuso la entrega de la información, el voto disidente del Consejero Olmedo toma relevancia, en cuanto expone que:

a) Que según el Comité de Libertad Sindical de la OIT, considera que la obtención de información sobre la mera afiliación a un sindicato sin expresión de causa justificada, podría presentar una forma de discriminación anti sindical, y, por ende violar el convenio N° 87 sobre libertad sindical y protección del derecho de sindicación de 1948, puesto que la protección de esta información pretende evitar represalias por parte del empleador.

b) Que la recolección de datos de los afiliados a un sindicato no respeta los derechos de la personalidad, pudiendo ser utilizado para crear una “lista negra” de trabajadores.

c) Que la distribución de tal información, podría constituir una violación del artículo N° 2 del Convenio 98.

d) Concluye que la divulgación de esa información podría representar una violación a los principios enunciados en Convenios fundamentales de la OIT en materia sindical, ratificados por Chile.

En una nueva solicitud de acceso, esta vez realizada a la Dirección de Trabajo, se solicitó copia de las actas de reforma, nómina y estatutos del sindicato formado. El Consejo en la Decisión Rol C866-10, estimó como infundados la oposición que se realizó, ordenando la entrega de la información. Sin embargo, el voto disidente del Consejero Jaraquemada, indicó que dicha información era de origen privado y, por lo tanto, debía resguardarse en razón de la autonomía de los sindicatos.

Por último, frente a un requerimiento de acceso a la información que incluía entregar el nombre y cédula de identidad de los 26 trabajadores afiliados al sindicato, así como copia de los libros de socios de dicha organización sindical, el Consejo en su decisión Rol C188-11, determinó que como la empresa ya conocía la identidad y cédula de identidad de sus trabajadores, el amparo se restringía a entregar la afiliación sindical de los trabajadores, reiterando la jurisprudencia anteriormente explicada, agregó, además, que si bien los datos personales de los 26 afiliados son datos de los cuales son titulares (art. 2° letra f, Ley N° 19.628), el interés público de conocer la información prevalece por sobre el derecho al resguardo de tales datos, por cuanto la divulgación de la información permitirá la constatación de las exigencias legales necesarias para la constitución definitiva de un sindicato, así como también la súper vigilancia de las funciones públicas asignadas a la Dirección del Trabajo vinculadas a verificar tales requisitos (Considerando 9°). En esta decisión, ya aparecen conjuntamente dos disidencias: las del Consejero Olmedo y Jaraquemada.

El giro de la jurisprudencia del Consejo en esta materia comenzó a variar con la decisión Rol C432-10, en que frente a una solicitud del acta de una elección sindical, la Dirección del Trabajo además, entregó el detalle de la votación y sus partícipes, con indicación de su nombre, RUT y firma. El Consejo representó en este caso a la entidad requerida por cuanto por una parte hizo entrega de información no solicitada, como asimismo, hizo entrega de información protegida por la Ley de Protección de Datos Personales, y finalmente infringir el secreto electoral del Código del

Trabajo. Más moderada aún sería la jurisprudencia del Consejo en la Decisión Rol C 839-10, en cuanto frente al requerimiento de la identidad de los participes en la elección y/o renovación del directorio de un sindicato, indicó que se hiciera entrega sólo del número de afiliados que participaron en la renovación del directorio, reservando sus identidades aplicando la causal de reserva del artículo 21 N° 2 de la Ley de Transparencia. Lo anterior, puesto que el sindicato era provisional, por tanto, existía un riesgo probable, específico y cierto de que se pudiera afectar la libertad sindical, perjudicando a la organización. Este último criterio, sobre el nivel de riesgo probable, específico y cierto respecto de sindicatos en modalidad provisional, fue extendido a aquellos consolidados, dando prevalencia a la protección de la identidad de los trabajadores afiliados a un sindicato (Decisiones roles C492-11 y C532-11).

En el último caso recién citado, el Consejo estimó que dado que lo solicitado decía relación con que la divulgación del dato personal, afiliación sindical, permitiría eventualmente que las empresas pudieran impugnar actos electorales, lo que no sucedería por estar presentes un ministro de fe, prevalecería la vida privada de quienes concurran a las votaciones, resolviéndose que éstas son en definitiva secretas.

Caso de estudio mexicano

Por Javier Osorio

Introducción

Los derechos de acceso a la información y a la protección de datos no son absolutos. Existen múltiples aristas donde la coexistencia de ambos derechos se contrapone. La discusión del caso mexicano muestra la forma en que el diseño institucional y el marco normativo ayudan a delinear la extensión y los limites de cada derecho. Además, este estudio describe los mecanismos de resolución de conflictos cuando la contraposición de ambos derechos resulta irreductible. Finalmente, el documento presenta algunos casos que reflejan la complejidad de la tensión que existe entre el derecho de acceso a la información y la protección de datos personales en el sector gubernamental.

1. Relevamiento normativo

En México, los derechos de acceso a la información y protección de datos personales están regulados por una robusta estructura normativa. El artículo 6° de la Constitución Política de los Estados Unidos Mexicanos eleva estos dos derechos al más alto rango en el entramado legal del país. A su vez, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) determinan los elementos necesarios para el ejercicio de estos dos derechos. El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) es el órgano encargado de vigilar la observancia de ambas leyes, para lo cual cuenta con un reglamento para cada ley y una serie de lineamientos procedimentales.

El conjunto de instrumentos legales que salvaguardan el acceso a la información y la protección de datos personales es producto de un proceso evolutivo que puede dividirse en tres etapas de adecuación y robustecimiento gradual. El punto de partida está marcado por la creación de la LFTAIPG, que fue publicada el 11 de junio de 2002 y contó con la aprobación unánime de las Cámaras de Diputados y Senadores. Esta ley tiene dos características. Por una parte obliga a los órganos de gobierno a abrir su información en pos de la transparencia y la rendición de cuentas. Por otra parte otorga a toda persona el derecho de acceder de manera rápida y sencilla a cualquier información en posesión de organismos gubernamentales, a la vez que protege los datos personales resguardados por entidades públicas y contempla ciertos límites al ejercicio de este derecho en excepciones previstas por la ley. Este fundamento legal permitió la creación del Instituto Federal de Acceso a la Información Pública (IFAI) el 24 de diciembre de 2002. El IFAI es el organismo encargado de velar por el ejercicio del derecho de acceso a la información y el cumplimiento de los lineamientos que marca la ley por parte de las dependencias gubernamentales. Unos meses después, el 11 de junio de 2003, fue aprobado el Reglamento de la LFTAIPG. Posteriormente fueron emitidos diversos lineamientos de carácter procedimental y operativo que ayudan a la implementación de la ley y al ejercicio del derecho de acceso a la información.

La segunda etapa se caracteriza por la modificación del artículo 6° de la Constitución que establece el acceso a la información como un derecho fundamental para todos los mexicanos. Esta modificación constitucional, aprobada el 20 de julio de 2007, reconoce el acceso a la información como "la libertad de cualquier persona de buscar o investigar información del Estado y de sus órganos, misma que está protegida por un derecho para que el Estado o sus autoridades no le impidan hacerlo" (López Ayllón, 2009: 17). Al tratarse de un derecho fundamental, esta protección jurídica aplica en todo el país, en sus distintos órdenes de gobierno y cuenta con el respaldo del derecho internacional.[211]

Finalmente, el más reciente esfuerzo por fortalecer el marco normativo en la materia se vio reflejado en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), promulgada el 5 de julio de 2010, y la posterior emisión de su Reglamento el 21 de Diciembre de 2011. Dicha ley dota a los ciudadanos de los derechos y mecanismos para salvaguardar su identidad y privacidad mediante la protección de datos personales. A partir de la LFPDPPP, el IFAI cambió su denominación a Instituto Federal de Acceso a la Información y Protección de Datos y recibió el mandato de vigilar la aplicación tanto de la ley de acceso a la información como de la ley de protección de datos personales. En consecuencia, el IFAI generó una nueva rama burocrática al interior de su estructura organizativa que le permita cumplir con el nuevo mandato. Actualmente, el IFAI funge como una sola institución encargada de velar por el ejercicio y la protección estos dos derechos.

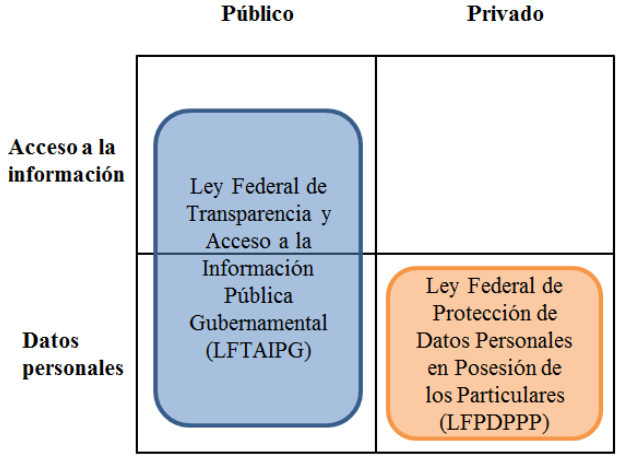
[211] El dictamen de la Cámara de Diputados sobre la propuesta de reforma al artículo 6° de la Constitución hace referencia explícita a instrumentos de derecho internacional como el artículo 19 de la Declaración Universal de los Derechos del Hombre, el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 13 de la Convención Americana sobre Derechos Humanos (Cámara de Diputados, 2007).

De esta forma, la evolución del marco normativo que regula los derechos de acceso a la información y protección de datos personales inició por el reconocimiento e instrumentación del derecho de acceso a la información en el sector gubernamental; posteriormente fue elevado en la Constitución con carácter de derecho fundamental; y finalmente fue extendido a la protección de datos personales en el sector privado.

Es importante enfatizar que la LFTAIPG abarca tanto el derecho de acceso a la información pública como la protección de datos personales en posesión de entidades gubernamentales. En contraste, la LFPDPPP se refiere exclusivamente al derecho de protección de datos personales que se encuentran en posesión de entes privados. Esta distinción es fundamental para señalar que la tensión entre el derecho de acceso a la información y el de protección de datos personales existe solamente en el ámbito de la información bajo resguardo de entidades públicas. Mientras que en el sector privado no existe dicha tensión ya a que el acceso a la información obliga solamente al Estado y no a los particulares. Por una parte, la coexistencia de dos derechos el ámbito de la información gubernamental genera la posibilidad de conflicto entre el ejercicio del acceso a la información y el de la protección de datos personales. Por otra parte, en lo referente a la información en posesión de particulares, no existe tal potencial de conflicto dado que no hay dos derechos que se contrapongan.

La Figura 1 presenta de manera más intuitiva la normatividad Mexicana en torno a la materia contenida en la ley (acceso a la información o protección de datos) y el ámbito de su aplicación (sector público o privado). La LFTAIPG regula los derechos de acceso a la información y protección de datos personales en el sector gubernamental. La LFPDPPP regula el derecho de protección de datos personales en posesión de particulares. Este estudio se centra en analizar la tensión entre acceso a la información y protección de datos personales en el ámbito público.

Figura 1. Materia y Ámbito de Aplicación de la Normatividad.



Fuente: Gráfica elaborada por el autor.
A continuación, se discuten por separado el tratamiento que da la ley a los derechos de acceso a la información y protección de datos personales haciendo mención de la finalidad, objeto, principios, sujetos obligados y definiciones conceptuales señaladas por la normatividad.

1.1 Derecho de acceso a la información

La comparación de los casos seleccionados para este estudio contempla el análisis del contenido de la regulación referente al acceso a la información en torno a cinco dimensiones clave: los principios rectores de la ley, finalidad, objeto, los sujetos obligados y la definición de conceptos centrales contemplados por la ley.

La ley de acceso a la información tiene como finalidad general proveer las disposiciones necesarias para garantizar el acceso de toda persona a la información en posesión de las entidades públicas a nivel federal (art. 1). Adicionalmente, el artículo 4 indica una serie de objetivos particulares de la ley que buscan transparentar la gestión pública, garantizar la protección de datos personales en posesión de organismos públicos, favorecer la rendición de cuentas, mejorar la gestión de documentos gubernamentales y contribuir a la democracia y el estado de derecho en México.

Los principios rectores de la ley de acceso a la información se encuentran contemplados en la Constitución. El artículo 6° constitucional indica que el derecho a la información debe estar regido por los principios de máxima publicidad; protección de datos personales; y transparencia y acceso a la información de manera gratuita, expedita e imparcial.

De acuerdo con el artículo 1° de la LFTAIPG, el objeto de regulación de la ley abarca toda la información en posesión de los poderes Ejecutivo, Legislativo y Judicial; los órganos constitucionales autónomos o con autonomía legal; y cualquier otra entidad federal. En principio, toda la información gubernamental es pública, salvo las excepciones temporales contempladas por la misma ley.

Los sujetos obligados están señalados en el artículo 3, fracción XIV de la LFTAIPG. En general, la ley obliga a los tres poderes del gobierno federal a garantizar el acceso a la información que se encuentra bajo su custodia. En particular, la ley señala como sujetos obligados (i) al Poder Ejecutivo Federal, los órganos de la Administración Pública Federal y la Procuraduría General de la República; (ii) la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y sus órganos; (iii) y el Poder Judicial Federal y el Consejo de la Judicatura. Adicionalmente, la ley contempla como sujetos obligados (iv) a los órganos constitucionales autónomos; (v) los tribunales administrativos federales; y (vi) cualquier otro órgano federal.

El artículo 3° define de manera explícita varios conceptos clave que guían la implementación e interpretación de la ley. Entre estos conceptos destacan la definición de *información*, que es entendida como "la contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título" (art. 3, frac. VII) y la definición de *documentos*, que hace referencia a "los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, 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 servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico" (Art. 3, frac. III). La ley también define los conceptos de *datos personales* y *sistema de datos personales*, cuyo tratamiento será discutido en la sección 1.2 de este documento. Adicionalmente, la ley define de manera explícita conceptos como *información reservada* (artículos 3-VI, 13, 14) y *seguridad nacional* que forman parte central de las excepciones del derecho al acceso a la información contempladas en la ley.

Respecto a estas cinco dimensiones básicas, la legislación Mexicana en materia de acceso a la información ofrece claridad y certidumbre jurídica en torno a los principios rectores de la ley, su finalidad y objeto, los sujetos obligados por la misma y la definición de conceptos clave. Estas características tienen amplios alcances ya que facilitan el ejercicio del derecho de acceso a la información por parte de la ciudadanía; mejoran la gestión de información y el cumplimiento de responsabilidades por parte de los sujetos obligados; e incrementan la efectividad en la vigilancia de la ley a cargo del IFAI y guían la resolución de controversias.

1.2 Derecho a la protección de datos personales

El derecho a la protección de datos personales en México está regulado por dos leyes referentes al ámbito particular, ya sea público o privado, donde se encuentre resguardado este tipo de información. Por una parte, la LFTAIPG provee los lineamientos para el acceso, gestión y protección de datos personales en posesión de organismos gubernamentales. Por otro lado, la LFPDPPP regula el tratamiento de los datos personales en posesión de empresas o personas físicas a fin de proteger la identidad, patrimonio y privacidad de las personas. Dado que la tensión entre el acceso a la información y la protección de datos personales existe solamente en el ámbito de la información gubernamental, esta sección se enfoca principalmente en discutir las características de la LFTAIPG en relación a la protección de datos personales en la esfera pública.

Dado que la LFTAIPG regula tanto el acceso a la información como la protección de datos personales en el sector gubernamental, la discusión acerca de la finalidad, principios, objeto y sujetos obligados mencionados en la sección 1.1, referente al derecho de acceso a la información, también aplica para el derecho a la protección de datos personales. Desde su promulgación en 2002, uno de los objetivos de la LFTAIPG consiste en "garantizar la protección de los datos personales en posesión de los sujetos obligados" (art 4, frac. III). Al respecto, la ley contiene definiciones y regulación específica en materia de datos personales. En términos generales, la normatividad considera los datos personales como toda la información que permita identificar a una persona física. En particular, el artículo 3°, fracción II, de la LFTAIPG define el concepto de *datos personales* como "la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad". La ley también hace referencia a los *sistemas de datos personales* como "el conjunto ordenado de datos personales que estén en posesión de un sujeto obligado" (art. 3, frac. XIII).

La confidencialidad de los datos personales es una de las excepciones del principio de máxima publicidad y transparencia que protege información cuya divulgación podría lesionar el derecho a la privacidad de las personas. La ley define la *información confidencial* como "la entregada con tal carácter por los particulares a los sujetos obligados […y comprende] los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización" (art. 18). Adicionalmente, la ley exige a los sujetos obligados que adopten las medidas necesarias para garantizar la seguridad de los datos personales; evitar su acceso no autorizado; prevenir su alteración o pérdida; y evitar su difusión, distribución o comercialización sin consentimiento expreso de los individuos (arts. 20 y 21). La regulación secundaria se encarga de detallar estas medidas de seguridad en el

Reglamento de la LFTAIPG y en los lineamientos para la protección de datos personales y para la elaboración de versiones públicas de documentos que deban salvaguardar información confidencial.[212]

La LFTAIPG contiene un breve apartado (Capítulo IV, Título I) de siete artículos específicamente dedicado a regular la protección de datos personales en posesión de organismos públicos. La ley señala a los sujetos obligados como los responsables de resguardar y gestionar los datos personales mediante la adopción de procedimientos y mecanismos que garanticen su seguridad, precisión y actualización (art. 23). Adicionalmente, la regulación indica que los titulares tendrán acceso a conocer o corregir sus datos personales que estén en posesión de organismos públicos, previa solicitud y acreditación de identidad (arts. 24 y 25). Si bien la LFTAIPG otorga a los ciudadanos los derechos de acceso y rectificación de datos personales en el ámbito público, estas prerrogativas contrastan con el menú más amplio de derechos que otorga la LFPDPPP a las personas en el ámbito privado. En referencia a los datos personales en posesión de particulares, la LFPDPPP especifica que los titulares de la información tienen el derecho de acceso, rectificación, cancelación y oposición. Estos son conocidos como derechos ARCO, y han sido señalados como elementos básicos de buenas prácticas en materia datos personales (López Ayllón, 2010: 61).

Esta asimetría de derechos relacionados con la protección de datos personales en el ámbito gubernamental frente al sector privado fue señalada durante las entrevistas realizadas a funcionarios del IFAI como una "agenda pendiente".[213] Al respecto, fue mencionada la "necesidad de homologar las herramientas legales con que cuentan los ciudadanos en el sector gubernamental y el sector privado",[214] a fin de equiparar el ejercicio de un mismo derecho en ambas esferas.

Sin embargo, la armonización de derechos de acceso, rectificación, cancelación y oposición en el sector gubernamental representa retos particulares, ya que puede generar tensión con temas relacionados con seguridad pública, seguridad nacional, materia fiscal, secreto bancario, información patrimonial, entre otros (López Ayllón, 2010: 61-75; Guerrero, 2010). En particular, la extensión de derechos ARCO sobre los datos personales en posesión de órganos gubernamentales puede entrar en conflicto con el artículo 22 de la LFTAIPG, el cual señala que no se requiere el consentimiento de los individuos para proporcionar sus datos personales "cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos". Estas posibles tensiones requerirían un tratamiento especializado en la legislación para regular los alcances y límites de los derechos ARCO en el sector público, así como para delinear las responsabilidades de los sujetos obligados y los mecanismos que permitan su armonización.

Si bien el derecho a la protección de datos busca salvaguardar la privacidad de las personas, la ley considera que en el caso de funcionarios gubernamentales el derecho de acceso a la información prevalece sobre la protección de datos y señala como una de las obligaciones de transparencia la publicación de los directorios de servidores públicos y sus remuneraciones (art. 7, fracs. III y IV). La preponderancia de la transparencia y la rendición de cuentas sobre los datos personales no se circunscriben a los funcionarios públicos, sino que se extiende sobre aquellos particulares inscritos en programas sociales y comanda la publicación de los padrones de beneficiarios (art. 7, frac. XI). En ciertos contextos, se podría considerar que la publicación de estos padrones vulnera la esfera de privacidad de los receptores de programas sociales, e incluso se podría argumentar que su difusión estigmatiza a sus beneficiarios y acentúa su situación de vulnerabilidad. Sin embargo, en el caso mexicano donde los programas sociales han sido utilizados como herramientas de movilización clientelar para fines electorales o como fuente de corrupción (Magaloni 2006, De la O, 2012), los legisladores consideraron que el interés general por la transparencia en el uso de recursos públicos destinados a programas sociales prevalece sobre el derecho a la privacidad de sus beneficiarios. El tratamiento de los padrones de beneficiarios es muestra que el acceso a la información y la protección de datos personales no es absolutos, ya que el rango de su extensión y la delimitación de sus excepciones operan en función de las características particulares de los contextos donde son aplicados.

2. DISEÑO INSTITUCIONAL

2.1 Diseño institucional para la implementación de la regulación de acceso a la información

Este apartado está dividido en tres secciones. La primera describe el tipo de legislación que crea la agencia encargada de proteger el derecho de acceso a la información y revisa sus atribuciones. El segundo apartado se refiere a los aspectos internos de la agencia regulatoria tales como su presupuesto, personal, grado de autonomía institucional y número de resoluciones recibidas. Finalmente, el tercer apartado analiza las reglas de designación y remoción de los directivos de la agencia y la duración de su mandato.

[212] Los artículos 47 y 48 del Reglamento de la LFTAIPG se refieren a la protección de datos personales. Los Lineamientos de Protección de Datos Personales, promulgados el 30 de septiembre de 2005, establecen las condiciones y requisitos mínimos para el manejo y custodia de los sistemas de datos personales que se encuentran en posesión de las dependencias. Adicionalmente, los Lineamientos para la Elaboración de Versiones Públicas por parte de las Dependencias y Entidades de la Administración Pública Federa, publicados el 13 de abril de 2006, detallan los procedimientos a seguir para la elaborar las versiones públicas de los documentos que contengan información reservada y/o confidencial.
[213] Entrevista a sujeto 1, Comisionado del IFAI, 9 de agosto de 2012.
[214] Entrevista a sujeto 11, Director del IFAI, 10 de agosto de 2010.

2.1.1 Aspectos externos

A diferencia de los otros casos contemplados en este estudio, en México la vigilancia de los derechos de acceso a la información y protección de datos personales está a cargo de una sola institución: Instituto Federal de Acceso a la Información y Datos Personales. El IFAI fue creado el 24 de diciembre de 2002 mediante el decreto publicado por el Presidente Vicente Fox en el Diario Oficial de la Federación. De esta forma, el IFAI quedó constituido como el organismo público gubernamental encargado de instrumentar la LFTAIPG. De acuerdo con el decreto de creación, el objeto del IFAI es "[…] promover y difundir el ejercicio del derecho de acceso 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" (Decreto 2002). El marco normativo le otorgó al IFAI tanto las facultades legales como el mandato de tutelar ambos derechos, así como la capacidad de resolver acerca de su ejercicio.

Respecto a la autonomía institucional, el artículo 6° de la Constitución en la fracción IV otorga al IFAI autonomía operativa, de gestión y de decisión. Estas características dotan al organismo de la autoridad necesaria para vigilar el cumplimiento del acceso a la información pública en posesión de la administración pública federal, revisar los casos en que autoridades nieguen el acceso a la información y determinar si la información que solicitan las personas es pública, reservada o confidencial. El artículo 37 de la Ley le otorga al IFAI, entre otras atribuciones, la capacidad de interpretar la LFTAIPG y la facultad de conocer y resolver los recursos de revisión interpuestos por los particulares en materia de acceso a la información y protección de datos personales en posesión de organismos gubernamentales. Adicionalmente, el artículo 34 de la Ley indica que "el Instituto, para efectos de sus resoluciones, no estará subordinado a autoridad alguna, adoptará sus decisiones con plena independencia". Posteriormente, a raíz de la reforma constitucional al artículo 6 realizada en 2007 la tutela de los derechos de acceso a la información y reserva de datos personales debe ser interpretada bajo el marco de los derechos fundamentales. En este sentido, el IFAI cuenta con un sólido respaldo normativo que le otorga un amplio grado de autonomía institucional y capacidades interpretativas y resolutivas.

Si bien el ejercicio de los derechos de acceso a la información y protección de datos personales pueden entrar en conflicto, la designación de un solo organismo encargado de tutelar ambos derechos evita duplicidad de funciones y facilita la resolución de controversias mediante un solo órgano de decisiones sin generar conflictos con otras agencias.

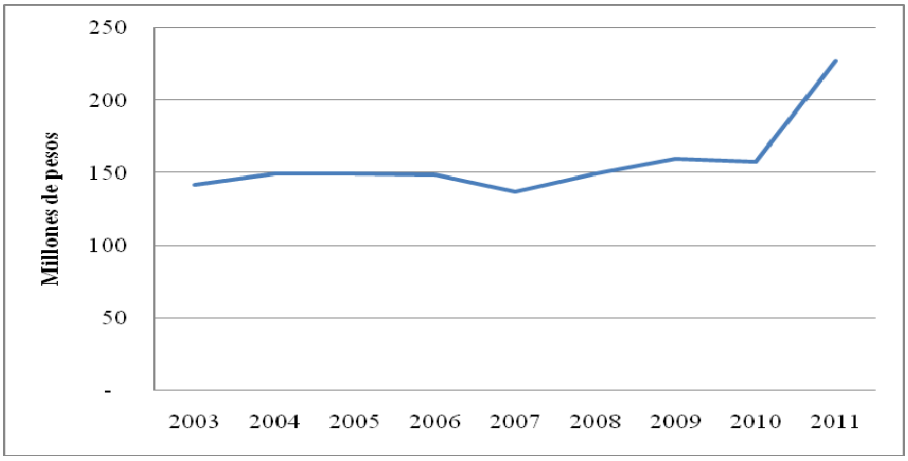
2.1.2 Aspectos internos

Para el ejercicio de sus funciones, el IFAI cuenta con la capacidad de proyectar su propio presupuesto y presentarlo a la Secretaría de Hacienda para su posterior aprobación por el Congreso (Art. 37, frac. XVIII). De acuerdo con las entrevistas realizadas a funcionarios del IFAI, existe un amplio consenso acerca de que el Instituto cuenta con los recursos financieros, materiales y humanos suficientes para cumplir de manera eficaz y eficiente con el mandato de ley.[215] La Figura 2 muestra la asignación presupuestal anual que ha recibido el IFAI entre 2003 y 2011. La gráfica muestra que el presupuesto del Instituto se mantuvo relativamente estable hasta 2011, año en el que tuvo un incremento presupuestal de 44.2% con respecto a 2010. La razón de este incremento radica en la ampliación de atribuciones derivada de la Ley de Protección de Datos Personales en Posesión de Particulares promulgada en Julio de 2010. Para cumplir con las nuevas atribuciones, el IFAI recibió un incremento presupuestal que le permitió incrementar su estructura burocrática y capacidad operativa.

Al respecto, la Figura 3 muestra que el número de plazas en la estructura organizativa del IFAI incrementó en 74.9% en el año 2011. Sin embargo, la proporción del presupuesto anual destinado al pago de salarios se mantuvo relativamente estable. Incluso, en 2011 la proporción de los recursos presupuestales utilizados para salarios se redujo en 11.6 respecto a 2010. Esto indica que a pesar de haber tenido un incremento absoluto en términos presupuestales y de personal en 2011, la capacidad operativa del Instituto es similar a la de años anteriores.

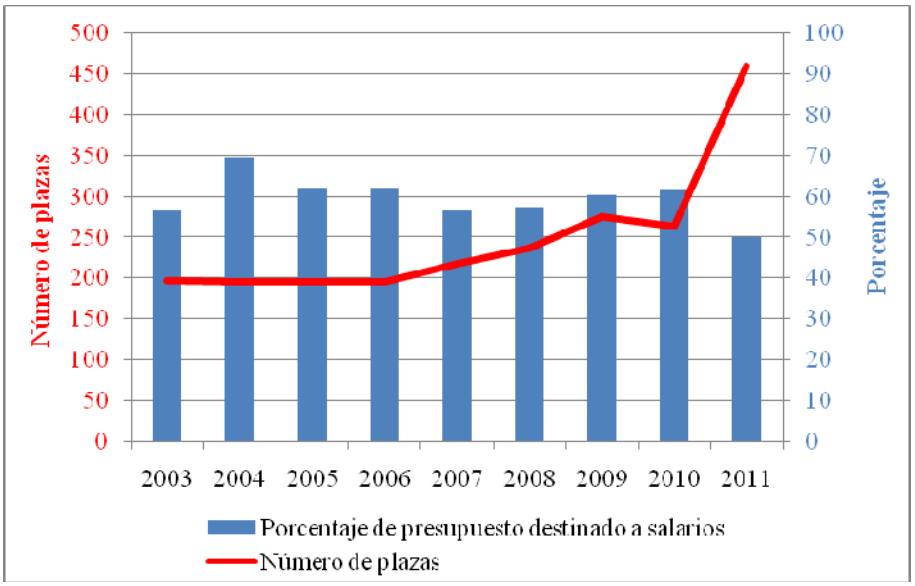
[215] Entrevista a sujetos 1, 5, 6, 8, 9 y 13 efectuadas entre el 9 y 16 de agosto de 2012.

Figura 2. Presupuesto anual del IFAI



Fuente: Gráfica elaborada por el autor con base en datos proporcionados por el IFAI en la solicitud de acceso a la información con folio No. 0673800109612.

Figura 3. Número de plazas y proporción del presupuesto destinado a salarios



Fuente: Gráfica elaborada por el autor con base en datos proporcionados por el IFAI en la solicitud de acceso a la información con folio No. 0673800109612.

La Tabla 1 muestra diferentes indicadores referentes al ejercicio del derecho de acceso a la información y el desempeño del IFAI en la protección de dicho derecho. La Tabla muestra un crecimiento sostenido en el número de solicitudes realizada por la ciudadanía a los diferentes órganos de la administración pública federal. En 2003, las dependencias gubernamentales recibieron 24,097 solicitudes de acceso a la información, cifra que incrementó a 123,293 en 2011. La tabla muestra que, en general, la administración pública otorga a los peticionarios la información solicitada, ya que solamente un pequeño porcentaje de los peticionarios no están de acuerdo con la respuesta de las autoridades gubernamentales y decide recurrirlas ante el IFAI. Entre 2003 y 2011, en promedio solamente fueron recurridas el 5 por ciento de las solicitudes de acceso a la información. Desde su creación, el pleno del IFAI ha recibido un total de 39,538 recursos de acceso a la información. Esto implica que en el 95 por ciento de las solicitudes los peticionarios no se inconforman con la decisión de las autoridades respecto a su solicitud. Esto no necesariamente significa que las dependencias otorguen la información requerida. En algunos casos, las autoridades han negado el acceso a la información argumentando que se encuentra protegida bajo las excepciones de la ley y, por lo tanto, no puede ser entregada. Siempre y cuando los peticionarios se inconformen

respecto a la decisión de la autoridad e interpongan un recurso de revisión ante el pleno del IFAI, su solicitud es considerada dentro del 5 por ciento de solicitudes recusadas.

Adicionalmente, la Tabla 1 muestra que del total de recursos de revisión que recibió el IFAI, el pleno de comisionados solamente emitió resoluciones dictando instrucciones a las autoridades en un promedio de 32 por ciento de los casos entre 2003 y 2011. Las resoluciones con instrucción son aquellas en las que el IFAI revoca o modifica la decisión de la autoridad en relación a la solicitud de acceso a la información recusada por el particular. En estos casos, el IFAI puede ordenar a la dependencia que permita el acceso a la información o a los datos personales solicitados, que reclasifique la información o que se modifiquen los datos referidos. En contraste, el porcentaje promedio de los recursos que no fueron revocados o modificados por el IFAI constituye el 68 por ciento de los recursos de revisión presentados por los particulares. En estos casos, los recursos pudieron haber sido declarados como improcedentes, sobreseído o la decisión de las dependencias pudo haber sido confirmada por el IFAI.

Tabla 1. Solicitudes, recursos y resoluciones.

Año	Solicitudes recibidas por las dependencias	Recursos interpuestos ante el IFAI		Resoluciones del IFAI con instrucción a las dependencias		
		Frecuencia	Porcentaje respectode solicitudes	Frecuencia	Porcentaje respectode recursos	Porcentaje respectode solicitudes
2003	24,097	635	3%	166	26%	0.7%
2004	37,732	1,431	4%	446	31%	1.2%
2005	50,127	2,639	5%	1,125	43%	2.2%
2006	60,213	3,533	6%	1,310	37%	2.2%
2007	94,723	4,864	5%	1,782	37%	1.9%
2008	105,250	6,053	6%	2,003	33%	1.9%
2009	117,597	6,038	5%	2,070	34%	1.8%
2010	122,138	8,160	7%	2,018	25%	1.7%
2011	123,293	6,185	5%	1,684	27%	1.4%
Total	735,170	39,538		12,604		

Fuente: Tabla elaborada por el autor con base en datos contenidos en el Informe de Labores del IFAI, 2012

Finalmente, la columna al extremo derecho de la Tabla 1 muestra la proporción del número de resoluciones con instrucción emitidas por el IFAI respecto al número de solicitudes de acceso a la información recibidas por la administración pública federal. Los datos revelan que en la gran mayoría de los casos (98.3 por ciento en promedio entre 2003 y 2011) no hubo necesidad que el pleno del IFAI interviniera para garantizar el derecho de acceso a la información y protección de datos personales ante las autoridades gubernamentales.

La tendencia general descripta por los datos indica que a lo largo de los últimos nueve años el número de solicitudes de acceso a la información creció de manera sostenida y, en la mayoría de los casos, las dependencias gubernamentales otorgaron la información requerida por los ciudadanos. Solamente un pequeño porcentaje de los particulares recurrieron al IFAI para que revisara las decisiones gubernamentales referentes a sus solicitudes de información. Incluso, entre los pocos recursos presentados para consideración del IFAI, aproximadamente en uno de cada tres casos el pleno de comisionados emitió una resolución revocando o modificando la decisión de las dependencias de gobierno. Sin embargo, puesto en perspectiva, el IFAI solamente intervino para tutelar los derechos de acceso a la información y protección de datos en aproximadamente dos de cada cien solicitudes.

2.1.3 Diferenciación política

De acuerdo al artículo 34 de la LFTAIPG, el IFAI cuenta con un órgano colegiado de decisión, el cual está conformado por cinco comisionados. El Ejecutivo Federal tiene la prerrogativa de nombrar a los comisionados del IFAI y el Senado tiene la posibilidad de objetar dichos nombramientos. Una vez nombrados, los comisionados del IFAI duran siete años en el cargo y no pueden ser removidos del mismo a menos que trasgredan de forma grave la ley, afecten las atribuciones del Instituto o hayan sido sentenciados por un delito grave. La conformación impar del órgano colegiado evita la posibilidad de parálisis o conflicto por votaciones pares y garantiza que las decisiones de los comisionados se tomen por mayoría.

Para el ejercicio de sus funciones, los comisionados del IFAI reciben un sueldo determinado por el escalafón salarial de la administración pública federal.[216] A diferencia de cargos de tipo honorario que no reciben remuneraciones, este esquema salarial permite a los comisionados dedicarse de tiempo completo a las responsabilidades inherentes a su cargo. Durante la tenencia de su nombramiento, los comisionados no pueden tener ningún empleo, cargo o comisión, salvo en instituciones de carácter docente, científico o de beneficencia.

En términos de representación legal, el artículo 36 de la Ley indica que el IFAI es presidido por un comisionado, el cual es electo por el mismo grupo de comisionados. La presidencia del Instituto tiene una duración de dos años y permite la renovación del cargo por una ocasión. El artículo 35 indica los requisitos para ser nombrado comisionado, los cuales incluyen ser ciudadano mexicano; no haber sido condenado por delitos dolosos; tener cuando menos treinta y cinco años de edad; haber desempeñado actividades relacionadas con la materia de la LFTAIPG; no haber tenido cargos de elección popular a nivel federal o estatal o haber sido dirigente de algún partido o asociación política durante el año previo a su nombramiento.

2.2 Diseño institucional para la implementación de la regulación de datos personales

Como se menciona en la sección 1.2, en el caso mexicano el derecho de protección de datos personales en posesión de organismos públicos está regulado por la LFTAIPG. En contraste, la LFPDPPP regula los datos personales en posesión de entidades privadas. El IFAI es la institución encargada de velar por este derecho en sus dos diferentes ámbitos de aplicación. Al respecto, las características de diseño y autonomía institucional, facultades de ley, órgano de toma de decisiones y capacidad de resolución de controversias mencionadas en el apartado 2.1 también aplican para la regulación de datos personales en posesión de entidades públicas.

2.3 Mecanismos para resolución de controversias

2.3.1 Instancias de apelación para que los ciudadanos planteen controversias

La exposición anterior muestra claramente que el acceso a la información y a la protección de datos personales no son derechos absolutos. En lo referente a la información en el sector público, existen múltiples aristas donde ambos derechos pueden entrar en contradicción. En este sentido, el diseño institucional mexicano tiene la ventaja de concentrar la regulación de estos dos derechos bajo una misma normatividad cuya tutela está a cargo de una sola institución. En caso que el conflicto entre ambos derechos sea inevitable, la unificación legal e institucional permite resolver las controversias de manera más eficiente.

En términos procedimentales, el artículo 49 de la LFTAIPG señala que cualquier solicitante que haya recibido una respuesta negativa a su solicitud de acceso a la información podrá interponer un recurso de revisión para que el IFAI analice el sustento con el que la autoridad tomó su decisión. Al respecto, basta con que el solicitante interponga un recurso de revisión ante la unidad de enlace de la dependencia o ante el IFAI dentro de los primeros quince días después de haber recibido la respuesta. Adicionalmente, el artículo 52 señala que "el Instituto subsanará las deficiencias de los recursos interpuestos por los particulares". En este sentido, la ley facilita el uso de recursos de revisión ya que no pone el peso de la justificación o argumentación jurídica en el recurrente. En otras palabras, no es necesario ser un especialista en materia de acceso a la información y protección de datos para interponer un recurso de revisión. Cualquier solicitante puede solicitar al IFAI que analice la negativa de la autoridad para otorgar la información solicitada.

Una vez aceptado, el recurso de revisión es asignado a un comisionado que servirá como ponente del caso y será el encargado de dar trámite, resolver los recursos y, en caso necesario, subsanar las deficiencias de derecho que sean pertinentes siempre en estricto apego a los hechos expuestos por las partes. El comisionado ponente puede llamar a audiencia a la dependencia o al recurrente a fin que presenten pruebas. El solicitante también puede pedir directamente audiencia con el comisionado ponente en el documento de interposición de recurso. El comisionado ponente debe integrar el expediente y presentar un proyecto de resolución ante el pleno dentro de los siguientes treinta días siguientes a la interposición del recurso. Una vez presentado el proyecto, el pleno del IFAI resuelve en definitiva el recurso mediante el voto de cada uno de los cinco comisionados. Finalmente, las resoluciones del pleno del Instituto son hechas del conocimiento público. En caso que la resolución del pleno contenga una instrucción para la dependencia, ésta deberá ser implementada dentro de un plazo no mayor a diez días hábiles a partir de la resolución.

2.3.2 Mecanismos establecidos para la resolución de controversias entre acceso a la información y la protección de datos personales

[216] La siguiente liga dirige al portal de transparencia donde se pueden consultar los datos de contacto y la remuneración de los funcionarios públicos, incluyendo a los comisionados del IFAI:
http://portaltransparencia.gob.mx/pot/directorio/buscarDirectorio.do?method=getBusqueda&_idDependencia=06738

La LFTAIPG considera que los recursos de revisión deben ser discutidos en el pleno del IFAI de forma colegiada y las resoluciones deben ser tomadas mediante la mayoría de votos de los comisionados. Al respecto, la ley no cuenta con un procedimiento especial para resolver las controversias entre los derechos de acceso a la información y protección de datos personales. Los casos en que estos derechos entran en conflicto son resueltos siguiendo el mismo procedimiento que cualquier otro recurso de revisión.

Dada la naturaleza del acceso a la información y la protección de datos personales existe una amplia variedad de instancias en que estos derechos pueden entrar en contradicción. Incluso, uno de los comisionados mencionó que "el conflicto entre estos dos derechos es inevitable; día a día es necesario analizar qué [información] se protege y qué se devela".[217] Al respecto, las opiniones de varios comisionados coinciden en que la complejidad de la confrontación entre estos derechos debe ser analizada caso por caso y mediante el contraste de argumentos en un proceso de debate al interior de un órgano colegiado.[218] De acuerdo a estos testimonios, tratar de implementar un procedimiento específico para la resolución de estos temas resultaría contraproducente ya que podría restringir la flexibilidad analítica necesaria para resolver asuntos tan delicados.

En la resolución de controversias, los comisionados del IFAI se centran en analizar de manera casuística la extensión y límites de los principios de máxima publicidad y la protección de la privacidad. Para ello recurren a estrategias de ponderación jurídica para valorar qué derecho prevalece sobre el otro en cada caso particular.

En algunas circunstancias, el pleno del IFAI ha encontrado los medios para establecer un balance que permita maximizar el principio acceso a la información mientras que salvaguarda el derecho a la privacidad. Esto ha ocurrido en solicitudes de acceso que piden la develación de información de interés general que contiene, entre otros elementos, datos personales. Una solución usualmente recurrida por los comisionados es la generación de *versiones públicas* de documentos que permitan la *armonización* de derechos de forma tal que solicitante pueda conocer a la información de interés público mientras que los datos personales de particulares aparecen testados en los documentos divulgados.

Desafortunadamente, no siempre es posible armonizar derechos fundamentales que se encuentran en conflicto. En estos casos, el pleno del IFAI recurre a la técnica jurídica de ponderación o proporcionalidad de derechos. En esencia, la ponderación consiste en el análisis de la relación costo-beneficio de favorecer un derecho por encima de otro. De esta forma, los comisionados discuten a detalle caso por caso y analizan si el beneficio que recibe la sociedad al favorecer un derecho es mayor que el costo de restringir el otro. Después de comparar ambos derechos en conflicto y determinar si la limitación de uno ese menor a la protección del otro, los comisionados se pronuncian y la decisión se toma por mayoría de votos en el pleno. En algunas ocasiones el dictamen de los comisionados se inclina a favor de la transparencia y el acceso a la información mientras que en otros consideran que es más importante la protección de datos personales.

2.3.3 Mecanismos de cumplimiento de las resoluciones

Una vez que el pleno del IFAI se pronuncia al respecto de un recurso de revisión, su resolución tiene carácter definitivo (artículo 59 de la LFTAIPG). En caso que la resolución contenga una instrucción hacia la autoridad, la dependencia referida tiene la obligación de dar cumplimiento al dictamen del IFAI. Si bien las entidades gubernamentales generalmente cumplen en tiempo y forma con las instrucciones del pleno, existen algunos casos en que los funcionarios públicos se rehúsan a cumplir con los mandatos del Instituto. En caso de incumplimiento, la ley otorga al IFAI la facultad de informar al órgano interno de control de cada dependencia acerca de las infracciones a la Ley (art. 37, frac. X).

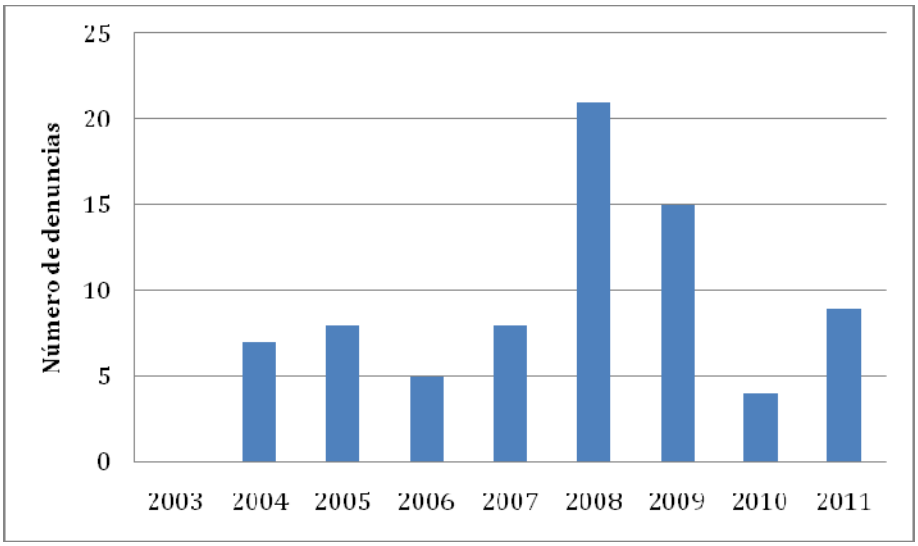
La Figura 4 muestra la tendencia de incumplimiento de las dependencias respecto a las resoluciones emitidas por el IFAI. Los datos indican que de las 12,604 resoluciones con instrucción dictadas entre 2003 y 2011, el IFAI solamente ha iniciado un total de 77 denuncias en contra de funcionarios públicos por incumplimiento de sus resoluciones.

Los datos indican que existe un alto porcentaje de cumplimiento de las instrucciones que emite el IFAI hacia las dependencias gubernamentales, al grado que su incumplimiento es una anomalía. Al respecto, es importante señalar que el IFAI no cuenta con facultades sancionatorias en contra de los funcionarios públicos que se rehúsen a cumplir con las resoluciones dictadas por el pleno. En casos de incumplimiento, lo máximo que puede hacer el IFAI es informar del caso al órgano interno de control de la dependencia. Éste, a su vez, informa a la Secretaría de la Función Pública (SFP). La SFP es el órgano de la administración pública federal encargado de vigilar que los servidores públicos federales se apeguen a la legalidad durante el ejercicio de sus funciones. En caso que el funcionario haya incurrido en responsabilidad, la SFP tiene la facultad de administrar una sanción. Sin embargo, de acuerdo con las entrevistas realizadas a funcionarios del IFAI, la SFP rara vez aplica sanciones en contra de los funcionarios que incumplen las resoluciones del pleno.[219] Del total de denuncias de incumplimiento iniciadas por el

[217] Entrevista a sujeto 9, Comisionado del IFAI, 14 de agosto de 2012.
[218] Entrevistas a sujetos 1, 6, 7 y 9 realizadas entre el 9 y 14 de agosto de 2012.
[219] Entrevistas a sujetos 3 y 4, Directores del IFAI, 10 de agosto de 2012.

IFAI entre 2003 y 2011, la SFP solamente ha sancionado a un funcionario por el incumplimiento de instrucciones dictadas por el IFAI.

Figura 4. Denuncias emitidas por el IFAI en contra de funcionarios públicos por incumplimiento de resoluciones



Fuente: Gráfica elaborada por el autor con base en datos proporcionados por el IFAI en la solicitud de acceso a la información con folio No. 0673800109612.

¿Cómo hace el IFAI para conseguir una tasa tan alta de cumplimiento de sus resoluciones a pesar de carecer de facultades sancionatorias y que la amenaza de sanción por parte de la SFP es poco probable? Parte central del éxito del IFAI para incentivar el cumplimiento de las instrucciones contenidas en recursos de revisión consiste en el monitoreo pormenorizado de cada solicitud de acceso a la información. El IFAI ha desarrollado un sistema interno de seguimiento del cumplimiento de los recursos de revisión con instrucción que indica la fecha límite de cumplimiento marcada por ley y la fecha en que la dependencia cumplió con la instrucción dictada por el IFAI.

Este sistema de monitoreo es utilizado por funcionarios del IFAI para contactar directamente a las unidades de enlace de cada dependencia y dar seguimiento estrecho al cumplimiento de resoluciones con instrucción. A medida que se acerca el plazo límite para el cumplimiento de obligaciones, los funcionarios del IFAI se comunican con sus contrapartes en las instituciones gubernamentales a fin de garantizar que se cumpla en tiempo y forma con las instrucciones dictadas por el pleno. En caso que se venzan las fechas límite, los funcionarios del IFAI redoblan esfuerzos para contactar a las dependencias y garantizar el cumplimiento de la resolución. De acuerdo a las entrevistas realizadas a personal del IFAI, el seguimiento puntual de cada caso desarrolla en los funcionarios públicos la percepción que están siendo monitoreados de manera pormenorizada, lo cual genera incentivos para el cumplimiento de sus obligaciones. El IFAI refuerza este sistema de incentivos al publicar en su sitio de internet la relación de recursos de revisión y su cumplimento.[220] Este mecanismo de difusión sirve para hacer del conocimiento público los casos de incumplimiento de las resoluciones y generar presión por parte de la opinión pública. Adicionalmente, los testimonios recolectados durante las entrevistas a funcionarios del IFAI coinciden en que los órganos internos de control de cada dependencia suelen utilizar esta información de cumplimiento para evaluar el desempeño de sus servidores públicos encargados de dar seguimiento y cumplir con las resoluciones del pleno.[221]

De esta forma, el sistema de monitoreo del IFAI genera incentivos directos e indirectos para el cumplimiento de resoluciones sin la necesidad de recurrir a la amenaza de sanciones administrativas. De manera directa, el IFAI incentiva el cumplimiento de las resoluciones mediante el seguimiento puntual de cada caso ante la dependencia responsable. De manera indirecta, la generación de información pública sobre el grado de cumplimiento favorece la rendición de cuentas por parte de la opinión pública y del órgano interno de control de cada dependencia, lo cual motiva a los funcionarios a obedecer las resoluciones del pleno del IFAI.

[220] La relación del grado de cumplimiento de recursos de revisión con instrucción puede ser consultada en la siguiente liga, dentro de las secciones de "Indicadores" y "Cumplimientos": http://www.ifai.org.mx/Estadisticas/#indicadores
[221] Entrevistas a sujetos 3 y 4, Directores del IFAI, 10 de agosto de 2012.

Tabla 2. Amparos y juicios contenciosos administrativos

Año	Amparos en contra de las resoluciones del IFAI interpuestos por:		Resoluciones de juicios de amparo		Juicios contenciosos administrativos en contra del IFAI interpuestos por:		Resoluciones de juicios contenciosos administrativos	
	Autoridades	Particulares	A favor del IFAI	En contra del IFAI	Autoridades	Particulares	A favor del IFAI	En contra del IFAI
2003	3	12	10	5	0	0	0	0
2004	3	49	42	10	1	0	1	0
2005	4	22	25	1	2	2	4	0
2006	5	43	28	20	1	1	2	0
2007	0	37	22	15	2	1	3	0
2008	0	37	16	21	19	2	20	1
2009	0	34	16	18	9	2	11	0
2010	6	56	47	15	4	1	5	0
2011	2	29	25	6	2	0	2	0
Total	23	319	231	111	40	9	48	1

Fuente: Tabla elaborada por el autor con base en datos contenidos en el Informe de Labores del IFAI, 2012 y los datos proporcionados por el IFAI en la solicitud de acceso a la información con folio No. 0673800109612.

Sin embargo, a pesar de las virtudes de este sistema de incentivos, existe un puñado de casos en el que algunas dependencias o particulares se han rehusado a cumplir con las resoluciones del pleno. La Tabla 2 reporta el número de juicios de amparo y juicios contenciosos administrativos interpuestos por organismos gubernamentales o particulares en contra del IFAI. Entre 2003 y 2011 el IFAI ha tenido que enfrentar un total de 342 juicios de amparo y 49 juicios contenciosos administrativos. A pesar de las resistencias de los promotores de dichos amparos y juicios, el poder judicial se ha declarado a favor del IFAI en el 67.6 por ciento de los juicios de amparo (231 casos) y 98 por ciento de los juicios contenciosos administrativos (48 casos). Los datos muestran que a pesar de los esfuerzos de algunas dependencias o particulares para no cumplir con las instrucciones del pleno, las autoridades judiciales le dan la razón al IFAI en la mayor parte de los juicios.

1. ORGANIZACIONES EN ACCIÓN

3.1 Recolección de datos personales de manera masiva

Esta sección describe la normatividad y procesos que siguen las dependencias gubernamentales relacionadas con materia de salud y programas sociales para la recolección masiva de datos personales, su protección y mecanismos de acceso por parte de los titulares. En particular, se analiza el tratamiento que hace la Secretaría de Salud respecto a los expedientes clínicos y la Secretaría de Desarrollo Social acerca de los padrones de beneficiarios de programas sociales.

3.1.1 Expedientes clínicos

En México, la Secretaría de Salud (SS) es la agencia encargada de proveer los servicios de salud a la población que reside en territorio mexicano y, entre sus varias facultades, cuenta con la prerrogativa de establecer las disposiciones jurídicas y normativas referentes a la prestación de servicios a cargo de las unidades que conforman el Sistema Nacional de Salud.[222] En 1998, la Secretaría de Salud expidió la Norma Oficial Mexicana NOM-168-SSA1-1998 del Expediente Clínico con el fin de sistematizar, homogeneizar y actualizar el manejo de los expedientes clínicos utilizados por el Sistema Nacional de Salud. De acuerdo a la Ley General de Salud,[223] el Sistema Nacional de

[222] La Ley General de Salud se encuentra disponible en la siguiente liga: http://www.salud.gob.mx/unidades/cdi/legis/lgs/index-indice.htm

[223] El documento de la NOM-168-SSA1-1998 se encuentra disponible en la siguiente liga: http://www.medigraphic.com/pdfs/patol/pt-2000/pt004g.pdf

Salud comprende el conjunto de dependencias y entidades públicas a nivel federal y estatal y de los sectores social y privado que prestan servicios de salud en México. En este sentido, el relevamiento de información de los expedientes clínicos ocurre de manera descentralizada y se encuentra a cargo de cada una de las unidades del Sistema Nacional de Salud, quienes deben seguir de manera cuidadosa los lineamientos provistos en la norma dictada por la Secretaría de Salud.
La norma NOM-168-SSA1-1998 definía el expediente clínico como el conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole en los que se registran los reportes, anotaciones y certificaciones de las intervenciones que el personal de salud realiza sobre los usuarios de los servicios de salud. Adicionalmente, el apartado 5.3 de dicha norma consideraba que "los expedientes clínicos son propiedad de la institución y del prestador de servicios médicos".
De acuerdo con el recuento realizado por Gómez Robledo (2010), entre 2004 y 2009 diferentes órganos del Sistema Nacional de Salud recibieron peticiones de particulares para acceder a sus propios expedientes clínicos o los de sus familiares fallecidos. En un gran número de solicitudes las dependencias se negaron a dar acceso a los documentos alegando en algunos casos que era información reservada y en otros que era confidencial. Después que los solicitantes interpusieron recursos de revisión ante el IFAI, el pleno del Instituto analizó caso por caso y revocó las resoluciones de las dependencias y ordenó la entrega de los expedientes clínicos a los solicitantes. En términos generales, las resoluciones del IFAI argumentaban que los lineamientos de una norma de nivel inferior contravenían las disposiciones de una ley federal, por lo tanto la LFTAIPG prevalece sobre la NOM-168-SSA1-1998.

Posteriormente, en septiembre de 2010 la Secretaría de Salud emitió la Norma Oficial Mexicana NOM-024-SSA3-2010 que establece los lineamientos del Sistema de Expediente Clínico Electrónico.[224] Esta nueva normativa hace referencia explícita a la definición de datos personales, con lo cual se sujeta a la regulación de la LFTAIPG en materia de protección y acceso de datos personales en posesión de organismos gubernamentales. De esta forma, queda eliminada la contradicción referente a la pertenencia de los expedientes clínicos contenida en la punto 5.3 de la norma anterior.

Adicionalmente, la norma del expediente clínico electrónico cuenta con una amplia gama de medidas de seguridad de datos que incluye protocolos de acceso a personal autorizado y sistemas de seguridad para la captura, integración, revisión, almacenamiento, consulta, administración e intercambio seguro de datos entre diferentes unidades del Sistema Nacional de Salud.

3.1.2 Listados de beneficiarios de programas sociales

De acuerdo con el artículo 7, fracción XI de la LFTAIPG, las dependencias públicas están obligadas a hacer públicos los padrones de beneficiarios de programas sociales y subsidios, los criterios de acceso, los montos asignados, el diseño y ejecución de dichos programas. Al respecto, la Secretaría de Desarrollo Social (Sedesol) mantiene en su página de internet los datos relacionados con once programas de asistencia[225] incluyendo los padrones de beneficiarios, las reglas de operación y las evaluaciones de programas sociales.[226] El sistema de acceso a la información relacionada con padrones sociales de Sedesol permite hacer consultas pormenorizadas por programa a nivel de estado, municipio y localidad y permite identificar el nombre completo de los beneficiarios de dichos programas. Adicionalmente, el artículo 19 del Reglamento de la LFTAIPG y los Lineamientos para la publicación de las obligaciones de transparencia marcan detalladamente el tipo de información y la periodicidad con la que las autoridades deben actualizar los datos relacionados con programas de estímulos, subsidios y apoyos.

En algunos contextos, la obligación de publicar los padrones de beneficiarios de programas sociales puede resultar controversial ya que su difusión incluye la publicación de datos personales e incluso datos sensibles. Algunos críticos podrían argumentar que la apertura de estos datos al conocimiento público vulnera la privacidad de las personas y podría generar daño derivado de la asociación de los individuos a estigmas sociales o económicos. Sin embargo, en el contexto mexicano, la normatividad otorga mayor peso al interés público, a la transparencia y la rendición de cuentas relacionadas a la asignación y uso de programas sociales que a la protección de la privacidad. En este sentido, los antecedentes de corrupción, desvío de recursos públicos y el uso de programas sociales con fines político-electorales en México incrementan la importancia de favorecer el acceso a la información sobre la protección de datos personales.

[224] El documento de la NOM-024-SSA3-2010 se encuentra disponible en la siguiente liga: http://www.dgis.salud.gob.mx/normatividad/nom024.html
[225] La lista de programas sociales incluye: (i) Programa de 70 y más; (ii) Opciones Productivas; (iii) Programa Hábitat; (iv) Empleo Temporal (PET); (v) Estancias Infantiles para Apoyar a Madres Trabajadoras; (vi) Rescate de Espacios Públicos; (vii) Programa 3x1 para Migrantes; (viii) Programa para el Desarrollo de Zonas Prioritarias (PDZP); (ix) Atención a Jornaleros Agrícolas; (x) Apoyo para Regularizar Asentamientos Humanos (PASPRAH); y (xi) Programa de Prevención de Riesgos en los Asentamientos Humanos.
[226] Los padrones de beneficiarios de los distintos programas sociales de Sedesol están disponibles en la siguiente liga: http://www.sedesol.gob.mx/es/SEDESOL/Padron_de_beneficiarios

3.2 Información personal de funcionarios públicos

La LFTAIPG contempla en su artículo 7 una serie de obligaciones de transparencia con la que deben cumplir las dependencias gubernamentales. Entre los elementos contenidos en este artículo se menciona la obligación de hacer públicos los directorios de servidores públicos, indicando el nombre completo del funcionario, su puesto, el detalle de su remuneración mensual, teléfono de contacto, dirección postal y correo electrónico. Al respecto, la legislación Mexicana considera que es de interés público dar a conocer los nombres y datos de contacto de funcionarios gubernamentales. No obstante, no toda su información personal forma parte de las obligaciones de transparencia ya que el mismo artículo 7 contempla el resguardo de la información confidencial.
Cada una de las dependencias gubernamentales tiene la responsabilidad de relevar y actualizar la información concerniente a sus obligaciones de transparencia, incluyendo los datos de sus funcionarios.[227] Para verificar el cumplimiento de las obligaciones de transparencia, la Dirección General de Coordinación y Vigilancia de la Administración Pública Federal del IFAI desarrolló una metodología para monitorear y evaluar el grado de cumplimiento de las dependencias gubernamentales. Dicha metodología consiste en la conformación de un índice que aglomera información referente a cinco apartados: (i) financiero; (ii) regulatorio y toma de decisiones; (iii) relación con la sociedad; (iv) organización interna; e (v) información relevante. El IFAI monitorea esta información en cada una de las dependencias gubernamentales y reporta el grado de cumplimiento de manera regular.[228]

3.3 Casos emblemáticos

En esta sección se discuten cuatro casos en los que el IFAI ha tenido que resolver acerca del conflicto que existe entre el derecho de acceso a la información y la protección de datos personales. Si bien el común denominador de estos casos es la tensión entre estos dos derechos, cada uno de estos casos llegó a resultados diferentes en términos de la prevalencia de un derecho sobre otro. El primer caso describe las resoluciones del IFAI respecto a dos solicitudes de acceso a la información que pedían conocer el número de averiguaciones previas de altos funcionarios del gobierno federal. En la primera ocasión el pleno del IFAI se inclinó hacia la protección de datos y en la segunda se decidió por abrir la información. El segundo caso muestra la decisión del IFAI de generar una versión pública relacionada con los expedientes clínicos de personas fallecidas mientras se encontraban en reclusión en un penal de máxima seguridad. En esta ocasión, los comisionados del IFAI se manifestaron a favor del acceso a la información mientras que protegieron algunos datos personales. El tercer caso discute la resolución del IFAI de abrir la información relacionada con concesiones de aprovechamiento de recursos naturales, incluyendo algunos datos personales de los concesionarios. Finalmente, esta sección presenta uno de los casos más controversiales a los que se ha enfrentado el IFAI en términos de la tensión entre acceso a la información y protección de datos personales. Este último caso se refiere a la información relacionada con la decisión de la autoridad tributaria de desistir en el cobro de créditos fiscales a contribuyentes deudores. En este caso, la tensión de derechos radica en el interés en conocer la información de personas beneficiarias de la cancelación crediticia en contra de la protección del secreto fiscal que niega la difusión de dicha información. Este asunto comprende cuatro resoluciones del IFAI e involucra a la Comisión Nacional de Derechos Humanos y a la Suprema Corte de Justicia de la Nación. A pesar de la instrucción reiterada del IFAI de abrir la información, la valoración que hizo la Suprema Corte respecto a este asunto favoreció la protección de datos personales sobre el acceso a la información.

3.3.1 Averiguaciones previas de funcionarios públicos de alto nivel

A finales de 2010 un ciudadano solicitó a la Procuraduría General de la República (PGR) que le informara sobre el número de averiguaciones previas que se habían iniciado en contra de 25 servidores públicos de alto nivel durante el año 2010. Dicha lista contenía los nombres de algunos funcionarios[229] que en ese momento se desempeñaban como Secretarios de Estado.[230] Esta solicitud fue registrada con el folio 0001700170710.

En su respuesta, la PGR informó al solicitante que no podía pronunciarse en sentido afirmativo o negativo respecto a esta solicitud ya que la información requerida se encontraba clasificada como reservada y confidencial de

---

[227] Los directorios de todas las dependencias de la administración pública federal pueden ser consultados en la siguiente liga: http://portaltransparencia.gob.mx/buscador/search/search.do?query=&idDependenciaZoom=&method=search&siglasDependencia=&idFraccionZoom=III&searchBy=1

[228] Dichos reportes pueden ser consultados en la siguiente liga dentro de la sección "Indicadores": http://www.ifai.org.mx/Estadisticas/#indicadores

[229] Los funcionarios mencionados en la solicitud incluye los siguientes nombres:
1. José Francisco Blake Mora, 2. Patricia Espinosa Cantellano, 3. General Guillermo Galván, 4. Almirante Mariano Francisco Saynez Mendoza, 5. Bruno Ferrari García de Alba, 6. Heriberto Feliz Guerra, 7. Arturo Chávez Chávez, 8. Genaro García Luna, 9. Salvador Vega Casillas, 10. Juan Francisco Molinar Horcasitas, 11. Javier Lozano Alarcón, 12. Juan Rafael Elvira Quesada, 13. Georgina Kessel Martínez, 14. Francisco Javier Mayorga Castañeda, 15, Alonso Lujambio Irazábal, 16. José Ángel Córdova Villalobos, 17. Gloria Guevara Manzo, 18. Abelardo Escobar Prieto, 19. Rocío de las Mercedes Nieves Bermúdez, 20, Ariel Cano Cuevas, 21. Consuleo Sáizar Guerrero, 22. Daniel Karam Toumeh, 23. Juan José Suárez Coppel, 24. Alfredo Elías Ayub y 25. Alonso García Tamés.

[230] De acuerdo a la estructura de la administración pública federal, las Secretarías de Estado en México son órganos equivalentes a los Ministerios en algunos otros países.

conformidad con la LFTAIPG y con el Código Federal de Procedimientos Penales (CFPP). Por lo tanto, no podía darle la información en relación al número de averiguaciones previas existentes en contra de los servidores públicos mencionados. La respuesta de la PGR se encontraba sustentada, entre otros elementos, en el artículo 14, fracción III de la LFTAPIG que señala como información reservada la relacionada con las averiguaciones previas y en el artículo 16 del CFPP el cual indica que solamente podrán tener acceso a las averiguaciones previas los inculpados, las víctimas o sus respectivos representantes legales.

Ante la negativa de acceso, el solicitante presentó un recurso de revisión al IFAI. Dicho recurso constituye un ejemplo claro del conflicto entre el derecho de acceso a la información y la protección de datos personales. Por una parte, el principio de máxima publicidad de la Ley favorece el acceso a la información que permita a la ciudadanía evaluar el desempeño de las autoridades gubernamentales. En este sentido, el conocimiento acerca de la existencia de averiguaciones previas iniciadas en contra de funcionarios públicos con cargos en las más altas esferas de la administración pública por la presunta comisión de algún delito sirve como un elemento importante para evaluar su desempeño. Por otra parte la LFTAIPG y CFPP protegen los datos personales y la información contenida en expedientes judiciales que no hayan causado estado. Presumiblemente, la difusión de esta información podría afectar el curso de los procedimientos judiciales y la reputación de los titulares de dichos datos personales.

El pleno del IFAI aceptó revisar el caso y le asignó el expediente número 685/11. Tras el análisis pormenorizado del marco normativo, los consejeros del IFAI decidieron por unanimidad confirmar la decisión de la Procuraduría General de la República de catalogar como reservada la información relacionada con el número de averiguaciones previas de 25 funcionarios públicos de alto nivel y no permitir su divulgación. En este caso, la resolución del IFAI se inclinó hacia la protección de la vida privada y los datos personales y determinó que toda aquella información que esté relacionada con la averiguación previa tendrá el carácter de reservada, motivo por el cual no es susceptible de acceso.

El sentido de la resolución del IFAI a favor de la protección de datos personales en esta solicitud, contrasta con la decisión del pleno de este Instituto a favor del acceso a la información en otro caso de características muy similares. Esto es muestra clara que los ámbitos de acción y límites de los derechos de acceso a la información no son absolutos y están sujetos a constante evaluación y reinterpretación.

En octubre de 2011 un ciudadano pidió a la PGR que informara sobre el número de averiguaciones previas en las que se ha denunciado al Secretario de Seguridad Pública Federal, Genaro García Luna. Esta solicitud fue registrada bajo el folio 0001700189811 con fecha del 19 de octubre de 2011. Es importante resaltar que el nombre de este Secretario también había sido mencionado en la lista de los 25 funcionarios de la solicitud número 0001700170710 mencionada anteriormente (ver el octavo nombre listado en la nota al pie número 19 de este documento). La PGR respondió al solicitante con la negativa de dar a conocer cualquier información relacionada con averiguaciones previas dirigidas en contra del Secretario de Seguridad Pública Federal ya que esta información está estrictamente reservada bajo la LFTAIPG y el CFPP. Posteriormente, el particular interpuso un recurso de revisión ante el IFAI, el cual fue aceptado e integrado en el expediente 5984/11.

La naturaleza de este recurso de revisión es muy similar al discutido anteriormente, ya que en ambos se solicitaba información acerca del número de averiguaciones previas de funcionarios públicos de alto nivel. En este sentido, el recurso también implicaba la tensión entre el derecho de acceso a la información y la protección de datos personales. No obstante, el análisis y ponderación que realizaron los comisionados del IFAI tomó un curso diferente.

En concordancia con su resolución anterior, el pleno del Instituto reconoció que la información contenida en las averiguaciones previas corresponde a la definición de dato personal y debe ser catalogado como información reservada, por lo que no es procedente otorgar acceso a ella fuera de los lineamientos que marcan la LFTAIPG y el CFPP. No obstante, consideró que el derecho a la privacidad no es absoluto y admite algunas excepciones. En esta ocasión, el IFAI recurrió a jurisprudencias de la Suprema Corte que enfatizan la preponderancia del principio de máxima publicidad que motiva la LFTAIPG y se encuentra respaldado por el artículo 6° constitucional. De acuerdo a los lineamientos de la corte, en caso de duda entre la publicidad o la reserva de la información, la interpretación de la ley debe favorecer inequívocamente la publicidad de la misma.

El ejercicio de ponderación jurídica que realizó el IFAI en torno a este caso se basó en la prueba de daño. Por una parte, los comisionados sopesaron el daño derivado de limitar el derecho a la privacidad del funcionario cuya información fue solicitada. Por otra, analizaron el beneficio público de difundir dicha información para promover la transparencia y la rendición de cuentas de los gobernantes.

La mayoría de los comisionados estimaron que no había daño sustancial al honor o reputación del funcionario público que ameritara favorecer la protección de datos sobre el acceso a la información. El carácter público de las funciones que voluntariamente desempeñan los servidores implica que ciertos ámbitos de su vida privada sean de interés público. Cuando se trate de funcionarios de alta jerarquía o relevancia, es necesario permitir un mayor escrutinio público sobre su esfera privada en caso que dicha información tenga relevancia para evaluar el ejercicio de sus funciones. Al respecto, el pleno del IFAI consideró que el beneficio público derivado de abrir la información acerca del número de averiguaciones previas iniciadas en contra del Secretario de Seguridad Pública Federal era mayor al daño individual que pudiera derivarse de restringir la protección de sus datos personales. La naturaleza del beneficio público radica en que el acceso a dicha información permite a la ciudadanía hacer una evaluación del desempeño de los servidores públicos y favorece la rendición de cuentas. En consecuencia, la mayoría de los

comisionados del IFAI estuvieron de acuerdo en revocar la decisión de la PGR para clasificar dicha información como reservada y giraron la instrucción para que la Procuraduría entregara los datos al solicitante.

Estos dos casos de solicitudes referentes al número de averiguaciones previas de funcionarios de alto nivel muestra que la tensión entre acceso a la información y la protección de datos personales es un conflicto recurrente en temas similares. La autoridad encargada de tutelar ambos derechos se enfrenta reiteradamente ante la necesidad de definir de manera casuística la extensión y los límites de ambos derechos. Incluso, existe la posibilidad que casos de naturaleza muy similar generen decisiones diametralmente opuestas favoreciendo en algunas ocasiones la protección de datos personales y dando preponderancia al acceso a la información en otras.

3.3.2 Expedientes clínicos de personas muertas en reclusión mientras se encontraban bajo custodia penitenciaria

En 2009, un solicitante pidió a la Secretaría de Seguridad Pública (SSP) que le hiciera entrega de la información relacionada con (i) los nombres de los prisioneros fallecidos en un penal de máxima seguridad y (ii) la copia de los expedientes médicos de dichos prisioneros mientras se encontraban bajo cuidado del estado. Esta solicitud de acceso a la información fue registrada con el folio 000220076509. En su respuesta, la SSP se negó a entregar la información argumentando que dichos datos estaban catalogados como datos personales y se encontraban protegidos bajo las reservas de ley. Dada la negativa de las autoridades para otorgar acceso a la información, el solicitante presentó un recurso de revisión ante el IFAI.

De acuerdo a la valoración de los comisionados del IFAI, dicha petición presentaba un claro conflicto entre los derechos de acceso a la información y la protección de datos personales. Por una parte, es de interés general conocer el tipo y calidad de cuidados médicos que brindan las autoridades gubernamentales a personas que se encuentran en reclusión al haber sido sentenciadas por la comisión de un delito o en prisión preventiva mientras su proceso judicial se encuentra abierto. La sustancia de interés para el público radica en la posibilidad de evaluar el desempeño gubernamental respecto al cumplimiento de sus obligaciones en la prestación de servicios de salud y analizar las circunstancias bajo las cuales pierden la vida las personas que se encuentran bajo cuidado del estado.

Por otra parte, la solicitud de información implicaba la divulgación de datos personales relacionados con información sensible, incluyendo padecimientos de salud y condiciones médicas. La protección de estos datos personales requirió un análisis pormenorizado. En este caso, existe el argumento que los datos personales solicitados no constituyen una afectación a la privacidad de sus titulares debido a que éstos ya habían fallecido. Sin embargo, la interpretación del IFAI extendió el área de protección de datos personales más allá de sus titulares al considerar que la divulgación de ciertos datos podía afectar a los familiares de las personas fallecidas ya que cierta información hacía referencia a padecimientos de tipo hereditario.

La mayoría de los comisionados consideraron que la actividad gubernamental debe ser sujeta de escrutinio público en aras de hacer efectiva la rendición de cuentas. Dicho escrutinio es particularmente importante en la esfera penitenciaria ya que las condiciones de aislamiento y restricción del contacto social en la que se encuentran los presos requieren de canales más amplios que permitan transparentar la actividad gubernamental. Con base en estas consideraciones, la mayoría de los miembros del pleno apoyaron la resolución con folio 3751/09 instruyendo a la SSP para que liberara la versión pública de los expedientes médicos de las personas fallecidas mientras se encontraban resguardadas por las autoridades penitenciarias. La versión pública de los expedientes debía testar el nombre de los titulares de datos personales, así debían eliminar los datos personales de terceras personas tales como su cónyuge u otros familiares. De esta manera, la versión pública de los documentos permitió *armonizar* los derechos de acceso a la información y la protección a la intimidad. La difusión de información acerca del número de decesos y las causas de los mismos permitió transparentar la gestión pública, a la vez que protegió el derecho a la privacidad de los familiares de las personas fallecidas en reclusión.

3.3.3 Aprovechamiento de recursos naturales

En 2010, un particular solicitó a la Comisión Nacional del Agua (Conagua) una serie de documentos relacionados con el título de concesión que la Comisión otorgó a un ciudadano para el aprovechamiento de las aguas de un río que atraviesa un ejido.[231] Esta solicitud fue registrada bajo el folio 1610100011211. Entre los documentos solicitados por el particular se incluía la copia de los pagos oficiales que realizó el concesionario para dicho aprovechamiento de recursos naturales. La Conagua entregó versiones públicas de algunos de los documentos solicitados. Sin embargo, decidió reservar la información referente a los pagos realizados por el concesionario bajo el argumento que era información protegida por el secreto fiscal. El solicitante se inconformó ante la negativa de la autoridad e interpuso un recurso de revisión para que el IFAI revisara el caso.

Este caso presenta nuevamente la tensión entre el derecho de acceso a la información y la protección de datos personales. Por una parte, es de interés público conocer la forma en que las autoridades dan seguimiento al cumplimiento de concesiones de aprovechamiento de recursos naturales y tutelan los derechos ambientales.

[231] El ejido es una forma de propiedad comunal de la tierra en zonas rurales que permite el uso colectivo de los recursos naturales.

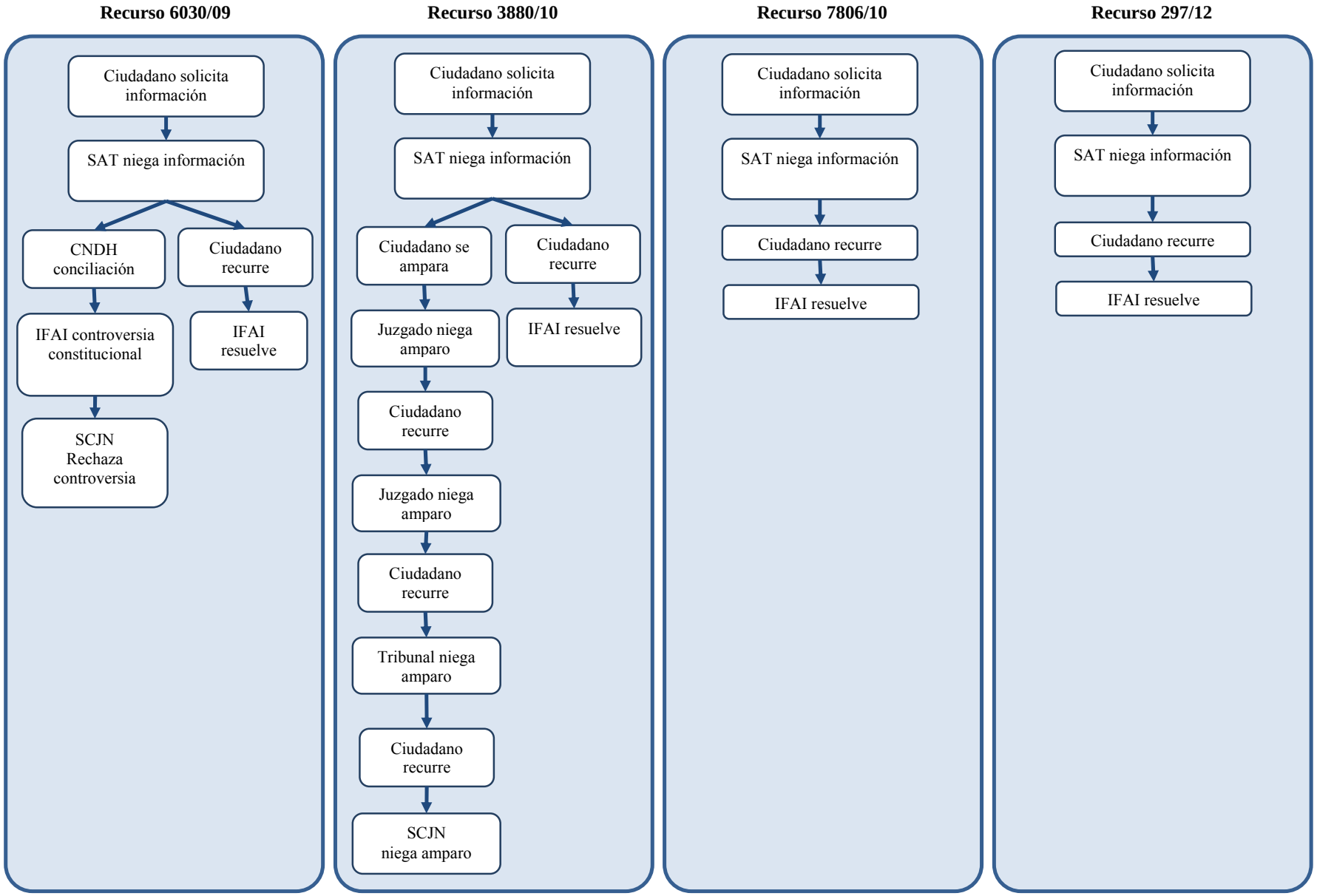
Adicionalmente, dado el carácter comunal de la propiedad de la tierra bajo el sistema ejidal, los miembros de la comunidad tienen un interés intrínseco en conocer la forma en que el estado permite la explotación de sus recursos naturales. Por otra parte, la divulgación de la información relacionada con los pagos de dicha concesión podía vulnerar la esfera de privacidad del concesionario a hacer públicos sus datos personales e información patrimonial. Además, la apertura de información relacionada con el secreto fiscal implicaba generar un precedente de consecuencias muchos mayores para futuros litigios relacionados con el secreto fiscal.

Finalmente, el pleno del IFAI realizó un ejercicio de ponderación de ambos derechos y la mayoría de los comisionados consideraron que el interés público por conocer el cumplimiento de las condiciones de explotación de recursos naturales es superior a la necesidad de proteger la información sobre los pagos de concesión bajo el secreto fiscal. Por lo tanto, ordenó a la Conagua que entregara la información relacionada con el pago de derechos de aprovechamiento de agua.

3.3.4 Cancelación del cobro de créditos fiscales

La cancelación del cobro de créditos fiscales por parte de la autoridad tributaria es uno de los casos más controversiales y complejos que ha enfrentado el IFAI en términos de la tensión entre el derecho de acceso a la información y la protección de datos personales. A diferencia de los ejemplos mencionados anteriormente donde el derecho al acceso a la información prevaleció sobre la protección de datos personales o fue armonizado en una versión pública, el caso de la cancelación de cobro de créditos fiscales se inclinó a favor de la protección de datos personales y en contra del acceso a la información. La discusión de este caso incluye cuatro solicitudes de acceso y sus correspondientes recursos de revisión dentro de un periodo de cuatro años. Además del solicitante, el sujeto obligado y el IFAI, este caso involucra la actuación de otras instituciones como la Comisión Nacional de Derechos Humanos (CNDH) y la Suprema Corte de Justicia de la Nación (SCJN). La Figura 5 muestra el diagrama con la evolución de cado uno de los cuatro recursos de revisión (6030/09, 3880/10, 7806/10 y 297/12) relacionadas con el tema.

Figura 5. Cancelación de cobro de créditos fiscales



3.3.4.1 Recurso de revisión 6030/09.

En noviembre de 2009 un ciudadano solicitó al Sistema de Administración Tributaria (SAR) información acerca de la relación de personas cuyo cobro de créditos fiscales fue cancelado debido a la imposibilidad práctica de cobro o incosteabilidad durante el año 2007.
Esta solicitud fue registrada con el folio 0610100169509. De acuerdo al artículo 4° del Código Fiscal de la Federación (CFF), los créditos fiscales son los créditos que el estado tiene derecho a exigir por parte de los contribuyentes.[232] De manera sumamente simplificada, se trata de créditos que los contribuyentes deben pagar al estado. En este sentido, el particular solicitó los datos de las personas morales a las que el SAT decidió cancelar el cobro de los montos adeudados por obligaciones crediticias con la Secretaría de Hacienda y Crédito Público debido a la imposibilidad práctica de cobrarlos o porque su cobro resultaba incosteable. La imposibilidad práctica del cobro ocurre cuando el deudor no tiene bienes que puedan ser embargados, ha fallecido, desapareció sin dejar nombre o cuando ha sido declarado en quiebra. La incosteabilidad del cobro ocurre cuando el SAT considera que es más costoso procurar el cobro de la deuda que recuperar el monto de la misma. Esto se define de acuerdo al monto del crédito, los costos de las acciones de recuperación, la antigüedad del crédito y la probabilidad del cobro.
En diciembre de 2009, el SAT respondió a la solicitud negando la entrega de la información bajo el argumento que esta información se encuentra reservada en virtud de la protección que brinda el secreto fiscal, el cual obliga a la autoridad tributaria a guardar en absoluta reserva lo concerniente a las declaraciones y datos suministrados de los contribuyentes. Inconforme con esta respuesta, el solicitante recurrió al IFAI para que revisara el caso. De acuerdo al artículo 69 del Código Fiscal de la Federación, las autoridades tributarias tienen la obligación de guardar reserva absoluta en relación con toda la información suministrada por los contribuyentes o captada por ellas en uso de sus facultades de comprobación.
El IFAI recibió el recurso de revisión interpuesto por el particular y le asignó el número de expediente 6030/09. En su resolución, el pleno del IFAI decidió favorecer el acceso a la información por encima de la protección de datos personales resguardada bajo el secreto fiscal. El IFAI consideró que la entrega de información transparenta la gestión y la rendición de cuentas. La rendición de cuentas va más allá de transparentar información, implica justificar las decisiones de gobierno. El SAT ejerce parte de sus atribuciones decidiendo a que personas físicas y morales cancela el cobro de créditos fiscales y a quienes no. Por lo tanto el sujeto obligado debe informar no sólo el mecanismo para tomar la decisión misma, sino la decisión misma, es decir, informar quiénes fueron beneficiados por el no cobro de obligaciones crediticias. De acuerdo con el IFAI, la cancelación del cobro de créditos fiscales constituye una transferencia de recursos negativos en sentido negativo. Por lo tanto es una decisión de no acción que debe ser sujeta a rendición de cuentas.
Adicionalmente, el IFAI consideró que el secreto fiscal no es absoluto y debe estar sujeto a las determinaciones de este organismo. Este secreto no puede aplicarse a personas físicas y morales a las que les fueron cancelados el cobro de créditos fiscales ya que el secreto fiscal protege a los “contribuyentes”. Para que una persona física o moral tenga la categoría de “contribuyente” debe mediar la acción de contribuir al erario público mediante el pago de sus obligaciones fiscales. Sin embargo, dado que el SAT decidió no ejercer el cobro de créditos fiscales, las personas beneficiarias de esta decisión no realizaron el pago de sus contribuciones, por lo tanto, no pueden ser catalogadas como “contribuyentes” y, en consecuencia, no se encuentran bajo la protección del secreto fiscal.
Incluso bajo el supuesto que el secreto fiscal fuera aplicable en este caso, los comisionados del IFAI realizaron un ejercicio de ponderación de derechos entre el acceso a la información y la protección de datos personales. En el análisis, el pleno del IFAI identificó que el monto total de los créditos cancelados por el SAT asciende a 73,960.4 millones de pesos, lo cual corresponde aproximadamente a 5,698.3 millones de dólares. Dada la magnitud del monto que la autoridad tributaria decidió no cobrar, el IFAI consideró que el interés público de conocer el nombre de los beneficiarios de esta decisión gubernamental es mucho mayor al daño que pudiera causar la divulgación de datos personales. El 10 de marzo de 2010, el IFAI revocó la decisión del SAT de catalogar la información como reservada e instruyó al SAT a entregar la información solicitada. A pesar de la resolución del IFAI, el SAT se negó a entregar la información argumentando que al hacerlo infringiría la ley y violaría el secreto fiscal.

3.3.4.2 Recurso de revisión 3880/10.

En marzo de 2010 un particular solicitó al SAT información sobre el listado de beneficiarios de la cancelación de créditos fiscales por 148,155 millones de pesos (entre 2007 y 2008) y los procesos de baja aprobados por el congreso en 2009 por 40,539 millones de pesos. Dicha solicitud fue registrada bajo el folio 0610100041310.
En abril del mismo año el SAT respondió a la solicitud declarando que parte de la información es inexistente y otra parte está protegida bajo el secreto fiscal. Además, el SAT señaló que no es procedente afirmar que existen personas "beneficiadas" dado que, de acuerdo al art 146-A del Código Fiscal de la Federación, la cancelación del

[232] El Código Fiscal de la Federación está disponible en la siguiente liga:
http://www.diputados.gob.mx/LeyesBiblio/pdf/8.pdf

cobro de créditos fiscales no libera al contribuyente de la obligación de pagar la deuda. De acuerdo a este argumento, la cancelación de créditos fiscales solamente implica la decisión por parte de la autoridad tributaria de no cobrar los créditos fiscales, pero eso no extingue la obligación de pago por parte de los contribuyentes. El solicitante se inconformó por la respuesta del SAT y presentó el recurso de revisión ante el IFAI, quien recibió el caso bajo el folio 3880/10.
El 20 de septiembre de 2010, la mayoría del pleno del IFAI resolvió revocar la respuesta del SAT y lo instruyó a entregar la relación de personas físicas y morales a las que fueron cancelados los créditos fiscales requeridos en la solicitud de acceso a la información. En su justificación, el IFAI retomó varios de los argumentos presentados en la resolución 6030/09 en el sentido que es mayor el interés general de conocer la información solicitada que la protección de datos personales bajo el secreto fiscal, ya que la difusión de esta información transparenta la gestión de la autoridad tributaria y favorece la rendición de cuentas.
A pesar que el IFAI resolvió hacer pública la información solicitada, el SAT se negó a la divulgación de dichos datos. Ante la negativa de acceso a la información, el solicitante promovió un amparo por la vía judicial argumentando que la decisión del SAT violentaba el derecho de acceso a la información garantizado por la Constitución. Dado que la resolución de este proceso judicial culminó hasta 2012, la descripción de eventos relacionados con la misma es presentada en la última sección de este apartado.

3.3.4.3 Recurso de revisión 7806/10.

En Octubre de 2010 un ciudadano emitió una nueva solicitud de acceso a la información solicitando al SAT que diera a conocer la relación de todas las personales morales a las que canceló una deuda fiscal entre 2008 y 2010, especificando el nombre de la persona y el total de la cancelación crediticia. Esta solicitud fue registrada bajo el folio 0610100165910. En noviembre del mismo año el SAT respondió a la solicitud negando su acceso e indicando que está clasificada como información reservada y está protegida por el secreto fiscal. Posteriormente, el solicitante se inconformó y presentó un recurso de revisión ante el IFAI, quien recibió la inconformidad del particular e inició el expediente con número 7806/10.
En marzo de 2011, el IFAI emitió su resolución. En ella consideró que el único mecanismo por medio del cual la ciudadanía puede verificar si el SAT está cumpliendo o no con su atribución de recaudar impuestos de manera eficiente, evitando la evasión y elusión fiscal, es mediante el conocimiento de las personas morales a quienes les ha cancelado el cobro de adeudos, así como el monto de dichas cancelaciones. No dar a conocer esta información propiciaría que el SAT no rindiera cuentas de sus actos.
Nuevamente el IFAI rechazó el argumento de reservar esta información bajo el secreto fiscal. De acuerdo a la mayoría del pleno, el secreto fiscal no tiene carácter de permanente y se opone al principio de transparencia. Por tal razón, el secreto fiscal como información confidencial no está incluido dentro de la FLTAIPG como causal de reserva.
Adicionalmente, el IFAI calificó que cancelar el cobro de un crédito fiscal constituye un beneficio para los deudores ya que, después de la cancelación y con el paso del tiempo, dicho crédito prescribe y se libera al deudor de la obligación fiscal de pago. La cancelación representa un beneficio puesto que aunque el particular sigue siendo deudor, no enfrenta ninguna consecuencia por el incumplimiento de sus obligaciones fiscales. Es más, el transcurso del tiempo favorece al beneficiario ya que da lugar a la extinción del crédito fiscal y anula la obligación de pago. En este sentido, el contribuyente al que el SAT canceló un crédito fiscal recibe un trato diferenciado respecto al de otros contribuyentes y dicho trato diferenciado constituye un beneficio.
En la evaluación de la prueba de daño, el IFAI consideró que aún en el supuesto que las personas morales contaran con la protección del secreto fiscal, el daño a su privacidad no sería mayor al interés público por transparentar la manera en que el SAT determina la cancelación del cobro de créditos fiscales. En consecuencia, el IFAI revocó la decisión del SAT de catalogar la información como reservada bajo el secreto fiscal y lo instruyó a dar acceso a la misma. En este sentido, el Instituto consideró que la divulgación de la información transparentaría la gestión del SAT y permitiría la rendición de cuentas respecto a su decisión de cancelar el cobro de créditos fiscales.

3.3.4.4 Intervención de la Comisión Nacional de Derechos Humanos.

A raíz de la resolución 6030/09 del IFAI realizada en marzo de 2010, diversos particulares presuntamente beneficiados por la cancelación de créditos fiscales realizada por el SAT solicitaron la intervención de la Comisión Nacional de Derechos Humanos (CNDH) bajo el argumento que la difusión de la información solicitada ordenada por el IFAI representaría una violación a su derecho a la privacidad consagrado bajo el artículo 6° constitucional. La CNDH recibió el caso bajo el expediente CNDH/2/2010/1825/Q. En agosto de 2010, la Comisión Nacional de Derechos Humanos emitió una propuesta de conciliación para salvaguardar el derecho a la privacidad y a la protección de datos personales que se encuentran en control del SAT. El acto de conciliación consistió en pedirle al SAT que publicara en su sitio web el detalle del monto de cada una de los créditos cuyo cobro fue cancelado pero sin revelar en nombre de las personas que se beneficiaron de la cancelación de créditos. La CNDH

consideró que la revelación de los nombres de quienes fueron cancelados sus créditos fiscales implica una violación a los derechos a la privacidad y protección de datos personales que se encuentran consagrados en el artículo 6 de la Constitución. La Comisión señaló que para evaluar el desempeño del SAT respecto a la aplicación de parámetros para la cancelación de créditos fiscales no es necesario revelar los datos personales; en específico, el nombre de los sujetos a los que se les canceló un crédito.
El IFAI consideró que la actuación de la CNDH contradecía de manera directa la resolución de este Instituto emitida en 2010, instruyendo al SAT que entregara la información detallada sobre los beneficiarios de la cancelación de créditos fiscales. Por tal motivo, el IFAI promovió ante la Suprema Corte de Justicia de la Nación (SCJN) una controversia constitucional acusando a la CNDH de invasión de funciones.
En marzo de 2011, la Segunda Sala de la SCJN consideró como procedente el recurso de reclamación interpuesto por el IFAI. Sin embargo, declaró infundada la controversia constitucional ya que el IFAI carece de legitimación activa para promoverla. La SCJN argumentó que el IFAI fue creado mediante decreto presidencial como un organismo descentralizado de tipo no sectorizado con autonomía de gestión y patrimonio. Sin embargo, a pesar de su autonomía, el IFAI conserva su naturaleza de órgano descentralizado y, de acuerdo al artículo 105, fracción I de la Constitución, este tipo de órganos carecen de legitimación activa para promover controversias constitucionales. Al declarar infundada la controversia constitucional, la Suprema Corte no entró a la discusión de fondo acerca del alegato del IFAI respecto a la invasión de competencias legales por parte de la CNDH.

3.3.4.5 Recurso de revisión 297/12.

En noviembre de 2011 un ciudadano solicitó al SAT los nombres de las personas morales a quienes se les canceló el cobro de créditos fiscales, los números de crédito y las causas de generación y cancelación de dichos créditos. La solicitud fue registrada bajo el folio 0610100205711. El SAT negó el acceso a la información argumentando que su divulgación afectaría el derecho a la protección de datos personales y el secreto fiscal. En enero de 2012, el solicitante interpuso un recurso de revisión ante el IFAI, el cual quedó registrado baje el expediente número RDA 297/12.
El IFAI argumentó nuevamente que la decisión discrecional del SAT de cancelar el cobro de créditos fiscales está sujeta a los requisitos de fundamentación, motivación, congruencia y exhaustividad exigidos por la Constitución. Por lo tanto, el acceso a la información relacionada con este caso debe favorecer el interés público, la transparencia y la rendición de cuentas del SAT. El pleno del IFAI consideró que es de interés público transparentar las decisiones del SAT a fin que exista mayor control por parte de la ciudadanía que permita evitar corrupción, así como actos de favoritismo, y verificar que su desempeño se apega a los principios de eficacia, eficiencia, justicia tributaria, generalidad e igualdad en la recaudación tributaria.
De acuerdo con el IFAI, la rendición de cuentas va más allá de transparentar la información e implica justificar las decisiones de gobierno. Dado que el SAT ejerce parte de sus atribuciones decidiendo sobre la cancelación de créditos fiscales, dicha decisión debe ser sujeta de escrutinio público. Por lo tanto, el SAT debe informar no sólo el mecanismo para decidir, sino la decisión misma; es decir, debe dar a conocer la relación de quienes fueron beneficiados por no pagar impuestos por un monto de 73,960.4 millones de pesos.
Si bien la normatividad referente a la cancelación de los créditos fiscales no libera a los deudores del pago de los mismos, lo cierto es que el Estado asume los costos de ese dinero que no ingresó al erario público por la decisión de no recaudarlos. La cancelación del crédito fiscal no extingue la obligación del deudor de pagar el crédito, pero dado que el Estado desiste de su esfuerzo por cobrar, la condición jurídica de cancelación deja a voluntad de los deudores el pago de los créditos cancelados. En este caso los deudores pueden pagar el crédito por iniciativa propia o dejar que pase el tiempo para que prescriban las facultades de cobro del SAT. De esta forma, la cancelación de créditos es equiparable a la obtención de recursos públicos en sentido negativo. Por lo tanto, el IFAI consideró que es de interés público conocer la relación de las personas beneficiadas por la cancelación de créditos incluyendo el nombre, el número de crédito, el monto y los motivos de cancelación del crédito. Sin embargo, pese a la resolución del IFAI de abrir la información, el SAT nuevamente se negó a cumplir con la instrucción del pleno y otorgar acceso a la información.

3.3.4.6 Intervención de la Suprema Corte de Justicia de la Nación.

Como consecuencia de la negativa del SAT de acatar la resolución del 7806/10 del IFAI y de entregar la información requerida, el solicitante promovió en diciembre de 2010 un juicio de amparo directo en contra del artículo 69 del Código Fiscal de la Federación y contra la respuesta del SAT que le niega el acceso a la información. El argumento central del quejoso consistió en que la negativa del SAT de entregar la información vulnera el derecho de acceso a la información consagrado en el artículo 6° constitucional como un derecho fundamental. En consecuencia, consideró que el artículo 69 del Código Fiscal es inconstitucional porque impone una absoluta opacidad sobre las decisiones tributarias y, en consecuencia, impide a los ciudadanos el acceso a la información relacionada con esta área de la administración de recursos públicos.

El Juzgado Séptimo de Distrito en Materia Administrativa del Distrito Federal recibió el amparo interpuesto por el quejoso. Sin embargo, el juez a cargo de analizar este caso determinó que el artículo 69 del código fiscal no es inconstitucional y puede ser interpretado de conformidad con la Constitución. Por lo tanto, se negó a otorgar el amparo al ciudadano. Inconforme con la resolución del juez, el ciudadano interpuso un recurso de revisión.
En enero de 2011, el juzgado Quinto de Distrito del Centro Auxiliar de la Primera Región recibió el caso y en marzo del mismo año dictó sentencia negando nuevamente el amparo. Haciendo uso de los recursos que le otorga la ley, el ciudadano recurrió de nueva cuenta la decisión del juzgado. En mayo de 2011, el Quinto Tribunal Colegiado en Materia Administrativa del Distrito Federal admitió el recurso de revisión y lo registró con el número 245/2011. En septiembre del mismo año, el Tribunal Colegiado remitió el caso a la Suprema Corte de Justicia de la Nación, quien admitió el caso en octubre de 2011 y le asignó el folio 699/2011. El asunto quedó radicado en la Primera Sala y fue turnado a la ponencia del Ministro Arturo Zaldívar Lelo de Larrea en noviembre de 2011.
En julio de 2012, la Suprema Corte determinó por mayoría de ocho votos a favor y dos en contra que el artículo 69 del Código Fiscal de la Federación es constitucional y negó el amparo al demandante. De acuerdo a la resolución de la corte, el alcance de la protección de datos personales que otorga el artículo 69 del Código Fiscal a los contribuyentes no es absoluto. Cuando el derecho a la protección de datos personales se contrapone al de acceso a la información debe realizarse un ejercicio de ponderación que ponga en la balanza el interés público que se promovería con la divulgación de los datos personales y el interés público de mantener la privacidad de esa información. Al respecto, la Suprema Corte consideró que se promueve el interés público cuando la apertura de la información contribuye al escrutinio del desempeño gubernamental con la finalidad de favorecer la transparencia, la rendición de cuentas y la buena administración de los recursos públicos. En contraste, no deben considerarse como casos de interés público aquellos en los que la información no tenga relevancia directa para evaluar la actuación de las autoridades o únicamente tienda a satisfacer la curiosidad de las personas sobre aquellos afectados con la divulgación de los datos. En este caso particular, la mayoría de los ministros de la Suprema Corte consideraron que la solicitud de conocer la relación de todas las personales morales a las que el SAT canceló créditos fiscales, especificando el nombre de la personal y el total de la cancelación crediticia no tiene relevancia directa para evaluar la actuación de las autoridades tributarias. En consecuencia, la Suprema Corte estimó que los agravios argumentados por el demandante son infundados y negó el amparo.
En este caso la Suprema Corte no entró a la discusión de fondo del asunto planteado en la demanda de amparo, es decir, no determinó si la información solicitada sobre la cancelación de los créditos fiscales debía o no ser revelada por la autoridad tributaria. A la fecha de elaboración de este estudio, el SAT se mantenía en incumplimiento de cuatro resoluciones del IFAI que le instruían abrir la información relacionada con el nombre de beneficiarios de la cancelación de créditos fiscales, número de créditos y el monto de los mismos.

4. CONCLUSIÓN

Este estudio analiza las características normativas y de diseño institucional relacionadas con la protección de los derechos de acceso a la información y protección de datos personales en posesión de entidades públicas. La coexistencia de estos dos derechos implica la posibilidad que en algunas cosas ocasiones ambos derechos entren en conflicto. Al respecto, este estudio describe los mecanismos para la resolución de conflictos en México y presenta algunos casos emblemáticos que dan muestra de la complejidad y tensiones que surgen entre el acceso a la información y la protección de datos personales.

El análisis del marco normativo muestra que el caso mexicano cuenta con una robusta regulación para salvaguardar el derecho de acceso a la información y la protección de datos personales. El entarimado normativo respecto a estos dos derechos se encuentra respaldado a nivel constitucional como derechos humanos. La operacionalización de estos dos derechos está contemplada en dos leyes federales, la LFTAIPG regula el acceso a la información y la protección de datos personales en posesión de entidades gubernamentales y la LFPDPPP regula los datos personales en posesión de particulares. Además, dichas leyes cuentan con un amplio cuerpo de reglamentos que regulan aspectos detallados de su aplicación. Finalmente, la regulación considera al IFAI como el órgano encargado de velar por el cumplimiento de ambas leyes.

Sin embargo, la evolución del marco normativo no ocurrió de manera jerárquica iniciando con la Constitución y, a partir de ella, bajando a leyes secundarias. Más bien, la evolución normativa de estos derechos inició por el reconocimiento e instrumentación del derecho de acceso a la información en el sector gubernamental; posteriormente fue elevado en la Constitución con carácter de derecho fundamental; y finalmente fue extendido a la protección de datos personales en el sector privado.

Dada las características regulatorias del derecho de acceso a la información y el de protección de datos personales, la tensión entre estos dos derechos existe solamente en el ámbito de la información que se encuentra resguardada por las entidades públicas. Mientras que en el sector privado no existe dicha tensión ya que a el acceso a la información obliga solamente al Estado y no a los particulares.

El análisis institucional da muestra de las características de diseño, atribuciones y recursos humanos y financieros con los que cuenta el IFAI para garantizar el ejercicio de ambos derechos. El IFAI cuenta con un cuerpo colegiado conformado por cinco comisionados que tienen a su cargo la toma colectiva de decisiones del Instituto. Todos los recursos de revisión son discutidos en el pleno del IFAI de forma colegiada y las resoluciones son tomadas mediante la mayoría de votos de los comisionados. Existe un amplio consenso acerca de que el Instituto cuenta con los recursos financieros, materiales y humanos suficientes para cumplir de manera eficaz y eficiente con el mandato de ley. A la fecha, el profesionalismo de los funcionarios públicos adscritos al IFAI y el uso eficiente de dichos materiales y financieros han sido utilizados para hacer frente al crecimiento sostenido en el número de solicitudes realizada por la ciudadanía a los diferentes órganos de la administración pública federal.

De acuerdo con el análisis de desempeño realizado en este estudio, en la mayoría de los casos la administración pública otorga a los peticionarios la información solicitada. Solamente un pequeño porcentaje de los peticionarios no están de acuerdo con la respuesta de las autoridades gubernamentales y decide interponer recursos de revisión ante el IFAI. Entre 2003 y 2011, en promedio solamente fueron recurridas el 5 por ciento de las solicitudes de acceso a la información. Del total de recursos de revisión que recibió el IFAI, el pleno del Instituto sólo emitió resoluciones con instrucción en un promedio de 32 por ciento de los casos. Esto muestra que en la gran mayoría de las solicitudes realizadas a la administración pública no fue necesaria la intervención del IFAI para garantizar el derecho de acceso a la información y protección de datos personales ante las autoridades gubernamentales.

Los datos indican que de las 12,604 resoluciones con instrucción dictadas entre 2003 y 2011, el IFAI solamente ha iniciado un total de 77 denuncias en contra de funcionarios públicos por incumplimiento de sus resoluciones. Esto es muestra del alto porcentaje de complimiento de las instrucciones que emite el IFAI a pesar que el Instituto no cuenta con facultades sancionatorias en contra de los funcionarios públicos que se rehúsen a cumplir con sus resoluciones. En casos de incumplimiento, lo más que puede hacer el IFAI es informar del caso al órgano interno de control de la dependencia o a la Secretaría de la Función Pública. Para maximizar el grado de cumplimiento de sus resoluciones sin necesidad de implementar sanciones directas en contra de dependencias que incurran en incumplimiento, el IFAI ha desarrollado un sistema de monitoreo pormenorizado que genera incentivos directos e indirectos para el cumplimiento de sus resoluciones.

En caso de controversia entre acceso a la información y la protección de datos personales los recursos de revisión son analizados de manera casuística por el pleno del IFAI. En la resolución de controversias, los comisionados analizan la extensión y límites de los principios de máxima publicidad y la protección de la privacidad mediante estrategias de ponderación jurídica que los ayudan a valorar caso por caso qué derecho debe prevalecer sobre el otro. En algunas ocasiones el IFAI consigue armonizar la coexistencia de ambos derechos mediante la divulgación de versiones públicas de documentos que revelan información de interés general mientras que protegen datos personales. Sin embargo, en algunas ocasiones la tensión entre estos dos derechos es irreductibles y los comisionados tienen que realizar pruebas de proporcionalidad de los beneficios de abrir la información o protegerla.

La discusión de casos muestra diversas aristas de la tensión entre el derecho de acceso a la información y la protección de datos personales. Respecto a la recolección y manejo masivo de datos en el sector salud, este estudio muestra la forma en que la regulación referente a los expedientes clínicos se ha ido adaptando a la protección de datos personales. Por su parte, la descripción del tratamiento que da la ley a los padrones de beneficiarios de programas sociales revela que los antecedentes de corrupción y uso clientelista de recursos públicos justifican la publicación de los nombres los beneficiarios a pesar que se trate de datos personales. De manera similar, la normatividad favorece la transparencia y el acceso a la información de ciertos datos personales de funcionarios públicos, incluyendo sus datos de contacto y salario.

Este estudio presenta también un conjunto de casos controversiales en los que el pleno del IFAI ha tenido que analizar la tensión entre el derecho de acceso a la información y la protección de datos personales y decidir acerca de la prevalencia de un derecho sobre el otro. El primer caso se refiere al número de averiguaciones previas de altos funcionarios públicos respecto a los cuales el IFAI se inclinó inicialmente a favor de la protección de datos personales y posteriormente a favor de la divulgación de dicha información. El segundo caso está relacionado con los expedientes clínicos de personas fallecidas mientras se encontraban en prisión. Al respecto el IFAI instruyó a la autoridad que generara versiones públicas de los expedientes que permitieran evaluar el cuidado de salud que brinda el Estado a personas en reclusión mientras que salvaguardaran los datos personales de los fallecidos ya que su divulgación podría afectar a sus familiares. El tercer ejemplo se relaciona con la protección de derechos ambientales en el que el IFAI consideró que el interés público de conocer las condiciones de aprovechamiento de recursos acuíferos es mayor al daño causado a un particular por la divulgación de cierta información personal referente al pago de derechos de concesión. Por último, el estudio presentó los diferentes componentes del caso de la cancelación del cobro de créditos fiscales con los que la autoridad tributaria decidió beneficiar a algunos deudores. La tensión de fondo en este caso radica en el argumento de dar a conocer la

información de las personas beneficiadas de la cancelación de créditos fiscales que se opone al argumento de no divulgar esta información ya que se trata de datos personales protegidos bajo el secreto fiscal. A pesar que el IFAI reiteró en cuatro ocasiones su instrucción para que la autoridad tributaria diera a conocer la lista de beneficiarios, la Suprema Corte favoreció la protección de datos personales bajo el secreto fiscal.

El análisis del caso mexicano muestra las ventajas de contar con un marco normativo robusto en materia de acceso a la información y protección de datos, así como un órgano garante con sólidas atribuciones legales y suficientes recursos humanos y materiales. Sin embargo, la coexistencia de ambos derechos es tan dinámica y compleja que el IFAI recurrentemente se ve en la necesidad de recurrir a estas herramientas legales y estructuras institucionales para analizar las tensiones entre el acceso a la información y la protección de datos personales. Si bien el caso mexicano presenta varias características que pueden ser de utilidad para otros países en su esfuerzo de reducir la tensión entre estos dos derechos, lo cierto es que el derecho a saber y el derecho a la privacidad no son absolutos y su coexistencia implica diversas instancias potenciales de conflicto.

5.REFERENCIAS

Alderman, Ellen y Carolina Kennedy. 2007. *The Right to Privacy,* Vintage Books. New York.

Cámara de Diputados. 2007. "Dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, con proyecto de decreto por el que se reforma el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos".

Código Fiscal de la Federación, http://www.diputados.gob.mx/LeyesBiblio/pdf/8.pdf

Gaceta Parlamentaria, No. 2207-II, 6 de marzo de 2007.

De la O, Ana. 2012. "Do Conditional Cash Transfers Affect Electoral Behavior? Evidence from a Randomized Experiment in Mexico" aceptado en *American Journal of Political Science.*

Fundar. Centro de Análisis e Investigación, 2012, "Amparo indirecto interpuesto en contra de la reserva de información por el llamado 'Secreto fiscal'. Ficha informativa. Mayo 2012".https://docs.google.com/a/nd.edu/file/d/0B7FMdBl-8xqIY1NYcWpmU3NzZ1U/edit?pli=1

Fundar. Centro de Análisis e Investigación, 2012, "De reservas absolutas y créditos fiscales cancelados en 2007". http://fundar.org.mx/mexico/?p=7424

Fundar. Centro de Análisis e Investigación, 2012, "El 'Secreto fiscal' en la SCJN: ¿ganará el interés público o vencerá la opacidad?" http://fundar.org.mx/mexico/?p=7340

Gómez Robledo, Alonso. 2010. "El acceso al expediente clínico como derecho humano fundamental" en *Homenaje al Doctor Emilio O. Rabasa*, Jorge Carpizo y Carol B. Arriaga (Coord.). Universidad Nacional Autónoma de México- Instituto de Investigaciones Jurídicas - Facultad de Derecho. México DF. Pp. 825-838.

Guerrero Gutiérrez, Eduardo. 2010. *Transparencia y seguridad nacional*. Instituto Federal de Acceso a la Información. Cuadernos de transparencia N0. 18. México DF.

Instituto Federal de Acceso a la Información. 2007. *Reforma al artículo 6° constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos*. Instituto Federal de Acceso a la Información. México DF.

Instituto Federal de Acceso a la Información. 2009. 7° *Informe de labores al H. Congreso de la Unión, 2009*. Instituto Federal de Acceso a la Información y Protección de Datos, México DF.

Instituto Federal de Acceso a la Información. 2011. 8° *Informe de labores al H. Congreso de la Unión, 2010*. Instituto Federal de Acceso a la Información y Protección de Datos, México DF.

Instituto Federal de Acceso a la Información. 2012. 9° *Informe de labores al H. Congreso de la Unión, 2011*. Instituto Federal de Acceso a la Información y Protección de Datos, México DF.

Instituto Federal de Acceso a la Información y Protección de Datos, 2012, Directorio de servidores públicos.
http://portaltransparencia.gob.mx/pot/directorio/buscarDirectorio.do?method=getBusqueda&_idDependencia=06738

Instituto Federal de Acceso a la Información y Protección de Datos, 2012, Cumplimientos 2003 – 2010, http://www.ifai.org.mx/Estadisticas/#indicadores

Instituto Federal de Acceso a la Información y Protección de Datos, 2012, "Indicadores de respuesta a solicitudes de información" http://www.ifai.org.mx/Estadisticas/#indicadores

Ley General de Salud, http://www.salud.gob.mx/unidades/cdi/legis/lgs/index-indice.htm

López Ayllón, Sergio (Coord.). 2007. *Código de buenas prácticas y alternativas para el diseño de leyes de transparencia y acceso a la información pública en México*. Instituto Federal de Acceso a la Información. México DF.

López Ayllón, Sergio. 2009. *El acceso a la información como un derecho fundamental: la reforma al artículo 6° de la Constitución mexicana*. Instituto Federal de Acceso a la Información. Cuadernos de transparencia N0. 17. México DF.

Magaloni, Beatriz. 2006. *Voting for Autocracy: Hegemonic Party Survival and its Demise in Mexico*. Cambridge University Press. Cambridge, MA.

Norma Oficial Mexicana NOM-168-SSA1-1998,

http://www.medigraphic.com/pdfs/patol/pt-2000/pt004g.pdf

Norma Oficial Mexicana NOM-024-SSA3-2010,

http://www.dgis.salud.gob.mx/normatividad/nom024.html

Secretaría de Desarrollo Social, 2012, Padrones de beneficiarios de programas sociales, http://www.sedesol.gob.mx/es/SEDESOL/Padron_de_beneficiarios

Suprema Corte de Justicia de la Nación, 2012, "Amparo en Revisión 699/2011". http://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=132394&SeguimientoID=472

Caso de estudio peruano

Por Carlos J. Zelada

Introducción

Quizás por su antigüedad como preocupación legislativa, el acceso a la información es una suerte de derecho "rey", al menos en lo formal, si lo comparamos con la protección de los datos personales. Pese al "boom" que favoreció su regulación más específica al finalizar el gobierno fujimorista hace ya una década, el acceso a la información en el Perú cuenta todavía con serios problemas de implementación y, a la fecha, carece de una autoridad nacional que regule y facilite su alcance al ciudadano de a pie.

La situación de la protección de los datos personales en el Perú no difiere demasiado tampoco. Con una ley reciente pero sin reglamento, y con una autoridad nacional que en la práctica no opera, poco se ha podido avanzar en su implementación a pesar de la fuerte presión existente por la coyuntura que imponen las obligaciones pactadas en los tratados de libre comercio recientemente suscritos con otros Estados.

La cuestión no es mejor si a ambos derechos se les aprecia bajo un mismo lente: el tratamiento de las tensiones entre el acceso a la información y la protección de los datos personales es todavía incipiente en el Perú. De hecho existen los conflictos, como lo demuestran los casos de estudio, pero poco o nada se ha hecho para establecer líneas jurisprudenciales que permitan esclarecerlos o, lo que sería mejor, para elaborar criterios desde la propia administración pública que permitan resolver tales tensiones sin acudir a la vía judicial.

En el marco de esta consulta pudimos comprobar entonces, no solamente la desconexión existente entre ambos derechos desde una perspectiva gubernamental sistemática, sino también los prejuicios existentes en la judicatura y en las entidades estatales casi siempre en detrimento del acceso a la información pública sin mayor raciocinio.

Se realizaron cuatro entrevistas con expertos a lo largo de esta consultoría para conocer un poco más de cerca esta realidad:

> (1) Erick Iriarte. Experto en temas de protección de datos personales y consultor del proyecto que luego se transformó en la actual Ley de Protección de Datos Personales. La entrevista se llevó a cabo el 15 de junio de 2012;
> (2) Javier Casas. Experto en temas de acceso a la información pública y actual director de la organización no gubernamental Suma Ciudadana. La entrevista se llevó a cabo el 26 de junio de 2012;
> (3) Fernando Castañeda. Experto en temas de acceso a la información y Adjunto para Asuntos Constitucionales de la Defensoría del Pueblo. La entrevista se llevó a cabo el 26 de octubre de 2012; y
> (4) José Álvaro Quiroga. Director de la Dirección Nacional de Protección de Datos Personales. José Álvaro Quiroga no nos atendió personalmente a pesar de haberse concertado la cita, sin embargo, dos abogadas de su equipo absolvieron mis preguntas. Ellas, sin embargo, no permitieron que se grabe la entrevista. La entrevista se llevó a cabo el 20 de noviembre de 2012.

Asimismo, se presentaron cinco solicitudes a diferentes entidades públicas o mixtas como parte de los casos de estudio. El resultado de lo visto y apreciado durante estos meses ha permitido elaborar este documento.

1. Relevamiento normativo

1.1. Normativa sobre acceso a la información pública

En el Perú, el acceso a la información pública es un derecho fundamental desde 1993. El artículo 2 numeral 5 de la Constitución Política vigente (1993) señala que toda persona 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 afecten la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional"[233].

[233] El artículo 61 numeral 1 del Código Procesal Constitucional establece a su vez que: "El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5 y 6 del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: 1. Acceder a información que obre en poder de cualquier entidad pública, ya sea se trate

Sin embargo, fue recién durante el período 2002-2003 que la legislación peruana contó con una ley y un reglamento cuyo eje central fuera el acceso a la información pública[234].

En cuanto a la ley, la norma ha pasado por tres momentos:

(1) El 13 de julio de 2002 el Congreso aprobó la Ley No. 27806 (Ley de Transparencia y Acceso a la Información Pública, en adelante "Ley de Acceso"). La norma fue publicada en el diario oficial el 3 de agosto de 2002.
(2) El 13 de enero de 2003 el Congreso aprobó la Ley No. 27927 (Ley que modifica la Ley No. 27806, Ley de Transparencia y Acceso a la Información Pública). La norma fue publicada en el diario oficial el 4 de febrero de 2003[235].
(3) Ambos textos fueron subsumidos y presentados en versión actualizada a través del Decreto Supremo No. 043-2003-PCM (Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, en adelante "TUO") (Ver Anexo 1), publicado en el diario oficial el 24 de abril de 2003.

La ley que regula el derecho al acceso a la información pública en el Perú cuenta a su vez con un reglamento que fue aprobado mediante el Decreto Supremo No. 072-2003-PCM (Reglamento de la Ley de Transparencia y Acceso a la Información Pública, en adelante "Reglamento") (Ver Anexo 2) y publicado en el diario oficial el 7 de agosto de 2003.

1.1.1 Finalidad

Como se indicó líneas arriba, la Ley de Acceso y su Reglamento aparecen en el período 2002-2003, momento en el que consolidaba la transición democrática luego del oncenio presidencial fujimorista. Es decir, ambas normas se aprobaron en un contexto de "predisposición nacional" para la articulación de un marco jurídico cuyo norte fuera la transparencia y el *accountability* desde las instancias del Estado así como la reversión de la "cultura del secreto" para entonces y todavía tan enraizada en el Perú. La exposición de motivos de la Ley No. 27806 es bastante elocuente al señalar que en dicho momento el Perú ocupaba el último puesto en la medición de los niveles de transparencia y acceso a la información pública en América Latina.

El artículo 1 del TUO señala que la finalidad de la norma es "promover la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información consagrado en el numeral 5 del Artículo 2 de la Constitución Política del Perú".

1.1.2 Sujetos

El artículo 2 del TUO dispone que los sujetos "obligados a informar" son las "entidades de la Administración Pública" definidas como tales "en el artículo I del Título Preliminar de la Ley No. 27444, Ley del Procedimiento Administrativo General".

En términos prácticos, ello implica la cobertura de todo el aparato estatal:

(1) Poder Ejecutivo (incluyendo ministerios y organismos públicos descentralizados),
(2) Poder Legislativo,
(3) Poder Judicial,
(4) Gobiernos regionales,

---

de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material".

[234] Un detalle más preciso de la historia legislativa previa del acceso a la información en el Perú puede encontrarse en: Defensoría del Pueblo. *El derecho de acceso a la información pública. Normativa, jurisprudencia y labor de la Defensoría del Pueblo. Serie Documentos Defensoriales – Documento No. 9*. 3ª edición (2011), pp. 30-34.

[235] Si bien la mayor parte de los preceptos incluidos en la Ley No. 27806 eran considerados positivos, algunas organizaciones denunciaron que ciertas restricciones que allí se establecían no eran compatibles con los estándares comparados sobre la materia. La Defensoría del Pueblo interpuso una acción de inconstitucionalidad contra tales secciones de la Ley de Acceso. Sin embargo, antes de que terminase dicho proceso, el Congreso aprobó la Ley No. 27927, subsanando los defectos que la demanda de inconstitucionalidad exponía. Entrevista con Fernando Castañeda, Comisionado de Asuntos Constitucionales de la Defensoría del Pueblo de Perú, XX de noviembre de 2012.

(5) Gobiernos locales,
(6) Organismos a los que la Constitución Política y las leyes confieren autonomía,
(7) Entidades y organismos así como proyectos y programas del Estado cuyas actividades se realizan en virtud de potestades administrativas,
(8) Personas jurídicas del régimen privado que presten servicios públicos o que ejerzan función administrativa en virtud de concesión, delegación o autorización del Estado, y
(9) Empresas del Estado.

Por otra parte, el Tribunal Constitucional ha establecido que el sujeto activo de este derecho es toda persona natural o jurídica, sin requerir que se acredite la inscripción en registro alguno (Exp. No. 4877-2006-HD/TC).

1.1.3 Principales definiciones conceptuales

El TUO no cuenta con un glosario de definiciones, pero éstas pueden deducirse de su articulado, en especial en cuanto a las excepciones al principio de publicidad (Ver sección 1.1.4). Así, la ley distingue tres tipos de información en este ámbito:

Información secreta: Detallada en el artículo 15 del TUO y referida esencialmente al ámbito militar y de inteligencia.

Información reservada: Detallada en el artículo 16 del TUO y referida esencialmente al ámbito policial y de las relaciones exteriores.

Información confidencial: Detallada en el artículo 17 del TUO y referida esencialmente al ámbito de la vida íntima, el secreto bancario y la reserva tributaria. En términos de esta consulta, ésta es la excepción más relevante. En particular, el inciso 5 del artículo 17 del TUO establece que es confidencial: "la información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución".

1.1.4 Principios

El TUO establece que su principio motor es la publicidad. A partir de este principio, el artículo 3 del TUO dispone que:

(1) Toda información que posea el Estado se presumirá pública, salvo las excepciones expresamente previstas por el artículo 15 del TUO[236],
(2) El Estado adopta medidas básicas que garanticen y promuevan la transparencia en la actuación de las entidades de la Administración Pública, y
(3) El Estado tiene la obligación de entregar la información que demanden las personas.

Con este principio como norte, el Tribunal Constitucional ha deducido, por ejemplo, que las entidades públicas deben entregar la información que solicitan los ciudadanos sin necesidad de que éste exponga las razones por las cuales realiza el pedido (Exp. No. 3278-2003-HD/TC).

Tampoco debe dejarse de lado que el artículo 13 del TUO establece que, en caso de negativa de entregar la información, ésta debe ser "debidamente fundamentada en las excepciones de los artículos 15 a 17 (…), señalándose expresamente y por escrito las razones por las que se aplican estas excepciones y el plazo por el que se prolongará dicho impedimento".

1.2 Relevamiento normativo para la protección de los datos personales

En el Perú, la protección de datos personales es un derecho fundamental. El artículo 2 numeral 6 de la Constitución Política de 1993 señala que toda persona tiene derecho: "A que los servicios informáticos,

[236] El texto completo de las excepciones previstas en el artículo 15 del TUO puede leerse en el Anexo 1. El artículo 15 habla de la información denominada "secreta". Cabe señalar que los artículos 16 y 17 tratan también de excepciones al acceso bajo el título de información "reservada" y "confidencial", respectivamente. Por lo tanto, las excepciones al principio de publicidad incluyen además los supuestos de los artículos 16 y 17 del TUO.

computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"[237].

La legislación peruana cuenta con una ley cuyo eje central es la protección de datos personales. El 21 de junio de 2011 el Congreso aprobó la Ley No. 29733 (Ley de Protección de Datos Personales). La norma fue publicada en el diario oficial el 3 de julio de 2011 (Ver Anexo 3).

Hemos tomado conocimiento del inicio de un proceso interno, a cargo del Ministerio de Justicia y Derechos Humanos, para la elaboración de un reglamento de la Ley No. 29733. El Proyecto de Reglamento de la Ley No. 29733 fue publicado en el diario oficial el 22 de septiembre de 2012 (Ver Anexo 4). En los últimos meses del año circularon noticias que señalaban que la norma sería aprobada con ocasión del primer año de vigencia de la Ley No. 29733. Sin embargo, a la fecha de cierre de este informe no se ha conocido mayor reacción sobre la propuesta desde el Poder Legislativo.

1.2.1 Finalidad

A diferencia de la Ley de Acceso y su Reglamento, la Ley de Protección de Datos Personales aparece en un contexto de ratificación de instrumentos bilaterales denominados "tratados de libre comercio" o TLCs que exigían la implementación de un marco normativo de protección más garantista del derecho a la vida privada, en especial del TLC suscrito con los Estados Unidos[238].

La propia Ley No. 29733 señalaba en su exposición de motivos que el Perú requería contar con "una ley acorde al mundo globalizado y a la revolución tecnológica", además de señalar los compromisos para "legislar el tema del derecho a la intimidad y el acceso a datos personales" adquiridos a través de la ratificación de tales instrumentos internacionales.

El artículo 1 de la Ley No. 29733 establece así que su finalidad es "garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".

Asimismo, el artículo 3 dispone que la norma se aplique "a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en el territorio nacional". El texto agrega que son objeto de especial protección "los datos sensibles".

1.2.2 Sujetos

La Ley No. 29733 es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales en manos de la administración pública o de administración privada, y cuyo tratamiento se realice en el territorio peruano.

Ahora bien, la Ley No. 29733 dispone una serie de obligaciones para los "encargados" y los "titulares" de bancos de datos personales.

De acuerdo con el artículo 2 de la Ley No. 29733, un "encargado" es toda "persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales". A su vez, el "titular" es definido en el mismo artículo como toda "persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de éstos y las medidas de seguridad".

---

[237] El artículo 61 numeral 2 del Código Procesal Constitucional establece a su vez que: "El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5 y 6 del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: 2. Conocer, actualizar, incluir, suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

[238] Entrevista con Erick Iriarte.

El artículo 2 de la Ley No. 29733 establece además que serán "entidades públicas" las definidas como tales "en el artículo I del Título Preliminar de la Ley No. 27444, Ley del Procedimiento Administrativo General". A éstas ya hicimos referencia en la sección 1.2.

1.2.3 Principales definiciones conceptuales

A diferencia de la Ley de Acceso y el Reglamento, la Ley No. 29733 cuenta con un glosario de términos todos detallados en su artículo 2 y que a continuación se transcriben. A efectos de esta consulta, especial atención merece la definición de los llamados "datos sensibles".

Banco de datos personales: Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

Banco de datos personales de administración privada: Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.

Banco de datos personales de administración pública: Banco de datos personales cuya titularidad corresponde a una entidad pública.

Datos personales: Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

Datos sensibles: Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Encargado del banco de datos personales: Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

Flujo transfronterizo de datos personales: Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.

Fuentes accesibles para el público: Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.

Nivel suficiente de protección para los datos personales: Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.

Procedimiento de anonimización: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de éstos. El procedimiento es irreversible.

Procedimiento de disociación: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de éstos. El procedimiento es reversible.

Titular de datos personales: Persona natural a quien corresponden los datos personales.

Titular del banco de datos personales: Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.

Transferencia de datos personales: Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

Tratamiento de datos personales: Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

1.2.4 Principios

Los artículos 4 a 12 de la Ley No. 29733 establecen un conjunto de "principios rectores y de interpretación" para el marco de protección de los datos personales que a continuación se detallan:

Principio de legalidad: El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

Principio de consentimiento: Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

Principio de finalidad: Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Principio de proporcionalidad: Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Principio de calidad: Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopiladas. Deben conservarse de forma tal que se garantice su seguridad y sólo por el tiempo necesario para cumplir con la finalidad del tratamiento.

Principio de seguridad: El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Principio de disposición de recurso: Todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Principio de nivel de protección adecuado: Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia.

1.3 ¿Cuál es la relación entre las dos normativas?

En el Perú, entonces, el acceso a la información pública y la protección de datos personales cuentan con normas legales independientes.

La Ley de Acceso y la Ley No. 29733 han respondido, como ya se precisó, a dos momentos históricos bastante diferenciados. La Ley de Acceso surge en un contexto proclive a la mejora de la transparencia y la credibilidad de la administración pública luego del gobierno fujimorista. Por su parte, la Ley No. 29733 surge casi una década después a raíz de los compromisos internacionales asumidos por el Estado Peruano en el marco de los TLCs y, en especial, el suscrito con los Estados Unidos.

En realidad, ambas normas se relacionan tan sólo desde la perspectiva de las excepciones al ejercicio de cada derecho, es decir, su complementariedad parte de una perspectiva altamente restrictiva. Ninguna de estas normas ha sido pensada para cumplir una lógica coadyuvante o de reciprocidad que pudiera servir para discutir eventuales casos de conflicto entre el acceso a la información pública y la protección de datos personales.

La distancia temporal de casi una década entre ambas es además un fiel reflejo de dicha discordancia.

1.4 ¿La ley de acceso a la información pública, considera la gestión de los datos personales en las excepciones o en alguna otra sección del documento?

La Ley de Acceso solamente considera la gestión de los datos personales en la sección de excepciones, específicamente en el artículo 17 inciso 5 al calificarlos como "información confidencial". Sin embargo, el inciso no hace mayor detalle de la lógica de dicha excepción (Ver Anexo 1).

1.5 ¿La ley que protege los datos personales, brinda lineamientos acerca de la divulgación de los datos personales? ¿Hace alguna distinción en relación al interés general que algunos datos pudieran tener?

De acuerdo con el artículo 13 de la Ley No. 29733, los datos personales sólo pueden ser objeto de tratamiento con consentimiento de su titular, a menos que exista una ley que autorice su revelación. El consentimiento, se exige, debe ser previo, informado, expreso e inequívoco.

En el caso de los datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Si no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

El mismo artículo 13 señala además que el tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas sólo puede ser efectuado por las entidades públicas competentes o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no podrán ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público.

Por otra parte, el artículo 14 de la Ley No. 29733 dispone que el consentimiento puede exceptuarse cuando se trate de datos personales relativos a la salud y cuando sea necesario, en circunstancias de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular y siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional.

Es interesante destacar que el mismo artículo también dispone la excepción del consentimiento para los datos sensibles relativos a la salud cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública. No obstante, ambas razones deben ser calificadas como tales por el Ministerio de Salud a través de procedimientos de disociación.

2. Diseño institucional

2.1 Diseño institucional para la implementación de la regulación del derecho de acceso a la información.

El Perú no cuenta con un órgano autónomo encargado de implementar la regulación del derecho de acceso a la información. El diseño institucional peruano ha previsto que cuando la información no es entregada por la entidad estatal requerida, la vía disponible para el ciudadano afectado es la judicialización de su solicitud. En estos casos, la tutela es ejercida a través del proceso constitucional de hábeas data (que como ya se precisó, también se utiliza para la protección de los datos personales) (Ver pie de página 5).

La Defensoría del Pueblo cuenta con estadísticas que señalan que entre 2009 y 2012 se registraron cerca de 5600 quejas de la población vinculadas a solicitudes de información no resueltas debidamente por las instancias gubernamentales, antes de la judicialización. Esta problemática radicaría, entre otras razones, en la no entrega de la información en tiempo oportuno, la no designación de funcionarios responsables en cada entidad para atender las solicitudes de la ciudadanía y la falta de justificación técnica cuando se produce una denegatoria al solicitante[239].

Por otro lado, una investigación reciente a cargo de la organización no gubernamental Suma Ciudadana precisa que entre 2003 y 2011 se publicaron en el diario oficial 206 sentencias de hábeas data "que, con las debidas reservas, podrían reflejar el ejercicio cotidiano del derecho al acceso a la información pública, desconectado de

[239] Entrevista a Fernando Castañeda.

hechos excepcionales"[240]. De acuerdo con el mismo estudio, solamente 30 de estas decisiones versaron sobre asuntos en los que se solicitaron "datos personales". Cabe señalar que bajo dicho rubro, las solicitudes buscaban dar a conocer las remuneraciones, currículos y planillas de pago de funcionarios públicos"[241].

Ahora bien, el Código Procesal Constitucional vigente (2004) establece las instancias encargadas de resolver estos recursos son el Poder Judicial y el Tribunal Constitucional. Si bien la gran mayoría de demandas de hábeas data solicitando información son declaradas fundadas por estos órganos, también se verifica que la excesiva duración de los procesos así como el uso indebido de las excepciones procesales por parte de los procuradores de las entidades públicas requeridas se han convertido en "desincentivos importantes para acudir a la vía judicial"[242].

De otro lado, expertos señalan que el impacto de estas sentencias en la gestión general de la administración pública es virtualmente mínimo[243]. En efecto, existe una importante cantidad de sentencias declaradas fundadas pero los órganos de la administración pública "persisten en la negativa de brindar información utilizando argumentos que ya han sido rebatidos repetidamente en sede judicial"[244].

El 9 de noviembre de 2012, la Defensoría del Pueblo presentó al Congreso un Anteproyecto de Ley con la finalidad de crear una "Autoridad Nacional para la Transparencia y el Acceso a la Información Pública como ente rector de un Sistema Nacional en la Materia" (Ver Anexo 5). La Defensoría del Pueblo ha propuesto así la creación de un "Sistema Nacional de Transparencia y Acceso a la Información Pública" bajo la dirección de una Autoridad Nacional. La propuesta enfatiza la necesidad de contar con un organismo especializado "con autonomía técnica, funcional, administrativa, normativa y económica", en el marco del Poder Ejecutivo (adscrita a la Presidencia del Consejo de Ministros), y cuyas principales funciones serían:

(1) Fiscalizar y sancionar en sede administrativa los incumplimientos de la ley,
(2) Resolver controversias en sede administrativa, sentando criterios vinculantes (y reduciendo la carga procesal en vía judicial sobre la materia),
(3) Promover y difundir el derecho de acceso a la información pública entre la población,
(4) Capacitar a los funcionarios públicos, y
(5) Asesorar técnicamente a las instituciones del Estado sobre esta materia.

A la fecha de cierre de este reporte no se han registrado mayores reacciones desde el Congreso o el Poder Ejecutivo en torno a esta propuesta.

2.2 Diseño institucional para la implementación de la regulación de datos personales

El Perú cuenta "formalmente" con un órgano autónomo encargado de implementar la regulación de la protección de los datos personales. El Título VI de la Ley No. 29733 (artículos 32 al 36) establece que existe una Autoridad Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos[245]. En el proceso de elaboración de este informe pudimos percibir un malestar en torno a la inclusión de la Autoridad Nacional para la Protección de Datos Personales en el Ministerio de Justicia y Derechos Humanos. Se nos indicó que hubiera sido preferible, a efectos de darle mayor autonomía funcional, técnica y presupuestaria, que se

[240] De hecho, el número de sentencias publicadas subiría a 495 de añadirse estas "otras" decisiones. Suma Ciudadana. El derecho de acceso a la información en el Perú. Lima: Pontificia Universidad Católica del Perú (2012), p. 19.
[241] Suma Ciudadana. El derecho de acceso a la información en el Perú. Lima: Pontificia Universidad Católica del Perú (2012), p. 21. Cabe señalar que en dicha estadística, los datos personales fueron el segundo tipo de información más solicitada.
[242] Entrevista a Javier Casas.
[243] Entrevistas a Javier Casas y Fernando Castañeda.
[244] Entrevista a Javier Casas.
[245] La Dirección Nacional de Protección de Datos Personales, que es la que hace las veces de Autoridad Nacional en dicha materia, cuenta con un enlace oficial en la web oficial del Ministerio de Justicia y Derechos Humanos. Disponible en: http://www.minjus.gob.pe/proteccion-de-datos-personales/. De acuerdo con la información del sitio web, la Dirección General de Protección de Datos Personales "se encarga de supervisar la administración y actualización del Registro Nacional de Protección de Datos Personales, así como resolver las reclamaciones formuladas por los titulares de datos personales en tutela de sus derechos de acceso, rectificación, cancelación y oposición. Asimismo, emite opinión técnica vinculante respecto de los proyectos de normas que regulen los datos personales y emite las directivas para la adecuada aplicación de la Ley de Protección de Datos Personales y su Reglamento. La Dirección General de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras a través de las siguientes unidades orgánicas: (1) Dirección de Registro Nacional de Protección de Datos Personales, (2) Dirección de Supervisión y Control, (3) Dirección de Sanciones y (4) Dirección de Normatividad y Asistencia Legal".

inscriba –como se ha propuesto para el caso de la Autoridad Nacional para la Transparencia y el Acceso a la Información Pública- en el marco de la Presidencia del Consejo de Ministros[246].

Precisamente, una de las principales funciones de la Autoridad Nacional de Protección de Datos Personales es "conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de derechos de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento" y "velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores" (numerales 16 y 17 del artículo 33 de la Ley No. 29733). La no aprobación del Reglamento de la Ley No. 23799 viene limitando el desarrollo de las actividades de la Autoridad Nacional de Protección de Datos Personales[247].

Durante el período de elaboración de este informe se intentó coordinar una entrevista con el Director de la Autoridad Nacional de Protección de Datos Personales, pero en su lugar, nos recibieron dos abogadas de su equipo. En realidad, la jefatura y las competencias de dicha Autoridad Nacional las desarrolla el equipo de la Dirección de Justicia del Ministerio de Justicia y Derechos Humanos[248]. Por ello, además, es el Director Nacional de Justicia en Perú, José Álvaro Quiroga, el que hace las veces de "jefe" temporal de dicho órgano.

En consecuencia, más allá de la nominación y de las coordinaciones para la elaboración de un reglamento para la Ley No. 29733, la Autoridad Nacional de Protección de Datos Personales no ejerce todavía función alguna ni la ejercerá hasta que se apruebe el reglamento de la Ley No. 29733[249]. En realidad, la Ley No. 29733 tampoco ha sido implementada en el Perú debido a que su reglamento todavía no ha sido aprobado. Otra evidencia de ello es que tampoco se ha podido crear el Registro Nacional de Protección de Datos Personales, principal base de datos que la Autoridad Nacional de Protección de Datos Personales debe administrar y actualizar (numeral 3 del artículo 33 de la Ley No. 29733).

Curiosamente, durante 2012 la organización no gubernamental Suma Ciudadana presentó una solicitud ante la Autoridad Nacional de Protección de Datos Personales buscando aclarar la procedencia de los datos personales de varios ciudadanos peruanos publicados en una página web que aparentemente estaría vinculada con el Estado. La Autoridad Nacional habría respondido señalando que por el momento no contaba con la capacidad para responder a dichos asuntos[250].

En todo caso, el diseño institucional peruano ha previsto que cuando se afectan los datos personales, la vía disponible para el ciudadano afectado es la judicialización de su solicitud. En estos casos, la tutela es ejercida a través del proceso constitucional de hábeas data (que como ya se precisó, también se utiliza para la protección del acceso a la información pública) (Ver pie de página 1).

En resumen, y de conformidad con la matriz entregada para la elaboración de esta consulta, la Autoridad Nacional de Protección de Datos Personales en el Perú puede describirse a través de estos indicadores:

Dimensión	Indicador
Aspectos externos	**Contexto en el que surge la agencia:** Implementación del marco normativo para la protección de la vida privada en el contexto de los TLCs celebrados por el Estado peruano, en especial el TLC suscrito con los Estados Unidos. **Tipo de legislación que crea la agencia:** Ley No. 29733, Ley de Protección de Datos Personales, aprobada el 21 de junio de 2011, casi una década después de la aprobación de la Ley de Transparencia y Acceso a la Información. **Posición de la agencia en el organigrama / cobertura territorial:** Dependiente de la Dirección Nacional de Justicia del Ministerio de Justicia. En la práctica no goza de autonomía técnica, funcional o administrativa. Su cobertura es nacional.

[246] Entrevistas a Erick Iriarte y a Fernando Castañeda.
[247] Entrevista a José Álvaro Quiroga.
[248] La Dirección Nacional de Justicia está encargada principalmente de supervisar los procesos de conciliación y la calidad del servicio de prácticas pre profesionales en Derecho en las instituciones del Estado a nivel nacional.
[249] Entrevista a José Álvaro Quiroga.
[250] Entrevista a Javier Casas. Ver además: http://redaccion.lamula.pe/2012/03/09/piden-informacion-al-gobierno-sobre-pagina-web-que-publica-datos-personales/lauraramirez.

	Atribuciones: - Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales. - Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento. - Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores. Existencia de organizaciones rivales: Ninguna.
Aspectos internos	Presupuesto: No cuenta todavía con presupuesto asignado. Personal: Su personal pertenece a la Dirección Nacional de Justicia del Ministerio de Justicia. La Autoridad Nacional de Protección de Datos Personales no cuenta propiamente con personal, comisionados o representantes.
Diferenciación política	Reglas para la designación y remoción: No han sido establecidas. Duración de mandatos: No han sido establecidos.

2. 3 Mecanismos para resolución de controversias

Instancias de apelación para que los ciudadanos planteen controversias

En principio, los ciudadanos que vean desprotegidos sus derechos de acceso a la información pública o de protección de datos personales tienen habilitada la vía judicial para su reclamo a través del proceso constitucional de hábeas data.

El proceso de hábeas data se inicia en el Poder Judicial y culmina en instancia definitiva en el Tribunal Constitucional. El artículo 62 del Código Procesal Constitucional requiere que en este proceso el demandante previamente haya reclamado, "por documento de fecha cierta, el respeto de los derechos (…) y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del derecho reconocido por el artículo 2 inciso 5) de la Constitución (acceso a la información pública), o dentro de los dos días si se trata del derecho reconocido por el artículo 2 inciso 6) de la Constitución (protección de datos personales). Excepcionalmente se podrá prescindir de este requisito cuando su exigencia genere el inminente peligro de sufrir un daño irreparable, el que deberá ser acreditado por el demandante. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir".

Mecanismos establecidos para la resolución de controversias entre el acceso a la información y la protección de los datos personales

No existen mecanismos ni criterios establecidos para la resolución de controversias entre el acceso a la información y la protección de los datos personales. En las disposiciones legislativas que regulan ambos derechos no existen mecanismos de coordinación ni criterios específicos que orienten las respuestas de la administración estatal o de los magistrados que resuelven los casos que alcanzan a judicializarse.

Para abonar a esta preocupación, en un informe reciente de la organización no gubernamental Suma Ciudadana se señaló lo siguiente:

> Desde su creación, el Tribunal Constitucional ha expedido hasta la fecha de elaboración de este informe (2012), 411 sentencias en procesos de hábeas data, pronunciándose sobre diversos aspectos del derecho de acceso a la información y del derecho a la autodeterminación informativa. Esta jurisprudencia es valiosa porque el máximo intérprete de la Constitución vierte criterios que sirven de guía a jueces y vocales e incluso a funcionarios públicos encargados de brindar información.
>
> No obstante, no todos los jueces utilizan como referencia a las sentencias del Tribunal Constitucional ya que de las 495 sentencias judiciales que fueron objeto de este estudio, únicamente en 84 se citan sentencias del Tribunal Constitucional; mientras que de éstas 84 citas casi siempre se trata de las

mismas sentencias. Ello evidencia la falta de fuentes confiables para acudir a jurisprudencia completa tanto del Tribunal Constitucional e incluso del Poder Judicial[251].

Mecanismos de cumplimiento de las resoluciones

No hemos podido acceder a información que nos permita acreditar el nivel de cumplimiento de las resoluciones emitidas por el Poder Judicial o el Tribunal Constitucional para conceder las solicitudes de información pública o de protección de datos de los ciudadanos. La única estadística existente es la que señala el Poder Judicial indicando que entre 2003 y 2011 se iniciaron 9781 procesos de hábeas data en todo el país, de los cuales 2494 habrían concluido en el mismo Poder Judicial. La Base de Datos del Sistema Integrado Judicial (SIJ), perteneciente al Poder Judicial, señala, no obstante, que solamente 6876 procesos estarían todavía en trámite en dicha instancia[252]. Como se puede apreciar, el registro oficial no es confiable.

3. Organizaciones en acción

Relevar mecanismos y bases de datos mediante los cuales los organismos recolectan datos personales de manera masiva

A fin de desarrollar este punto de la consulta, se presentaron solicitudes de información en el marco de dos cuestiones en donde se manifestara la tensión entre el acceso a la información pública y la protección de los datos personales: (1) historias clínicas y (2) listados de beneficiarios de un programa social.

2.2.1 Historias clínicas

Para este extremo se eligió solicitar la información del estado de salud del actual alcalde del distrito de San Isidro en Lima, Raúl Cantella Salaverry. En breve, la historia es la siguiente: en octubre de 2011 el alcalde Cantella solicitó la vacancia de su cargo ante su Concejo Municipal. Para ello presentó un certificado de salud que señalaba que padecía "una hipertensión arterial y una microangiopatia isquémica" que constituían "impedimento físico que lo imposibilitaba de manera permanente de continuar con sus funciones" (Ver Anexo 6). El Concejo Municipal atendió la solicitud y nombró interinamente a una regidora como alcaldesa. En octubre de 2011, el para entonces ex alcalde Cantella presentó una solicitud de reincorporación al cargo ante el Concejo Municipal. Para ello adjuntó un nuevo certificado, firmado por el mismo médico, pero que señalaba que éste "había mejorado físicamente pudiendo desempeñar con normalidad sus funciones" (Ver Anexo 7). Lo que siguió fue una batalla legal, ampliamente cubierta por la prensa local, entre la nueva alcaldesa y el entonces ex alcalde que culminó con una resolución inapelable del Jurado Nacional de Elecciones de diciembre de 2011 en la que se reponía a Cantella en el cargo.

Se logró averiguar que dos entidades privadas poseían los respaldos médicos de los diagnósticos presentados por el alcalde Cantella: la Clínica San Pablo y la Clínica San Felipe. En la medida que ambas instituciones privadas prestan un servicio de naturaleza pública, estarían también obligadas a entregar la información solicitada (de interés público) ante la solicitud de cualquier ciudadano. Se presentaron entonces dos solicitudes (Ver Anexos 8 y 9) durante los primeros días de septiembre de 2012 buscando conocer los segmentos de la historia clínica del alcalde que respaldaban ambos diagnósticos. La Clínica San Pablo nunca contestó la solicitud. La Dirección Médica de la Clínica San Felipe contestó nuestra solicitud el 17 de septiembre de 2012 pero denegando el pedido (Ver Anexo 10). De acuerdo con la respuesta, no era posible que me entreguen copia de la historia clínica de ningún paciente pues todos los actos médicos eran "carácter reservado", siendo ellos además "una institución privada" que por tanto no se encontraba obligada por la Ley de Transparencia y Acceso a la Información. La respuesta cierra con este párrafo:

> Consideramos que en el presente caso, nos encontramos dentro de los supuestos de excepción previstos en la Constitución, en la medida que el entregarle copia de la historia clínica del Dr. Cantella, vulneraría su derecho a la intimidad personal, y debido a que existe una Ley expresa que nos prohíbe divulgar información vinculada con actos médicos.

[251] Suma Ciudadana. El derecho de acceso a la información en el Perú. Lima: Pontificia Universidad Católica del Perú (2012), pp. 25-26.
[252] Suma Ciudadana. El derecho de acceso a la información en el Perú. Lima: Pontificia Universidad Católica del Perú (2012), pp. 11-12.

Listado de beneficiarios de un programa social

Para este extremo se decidió solicitar información al Ministerio de la Mujer y Desarrollo Social para conocer (Ver Anexo 11):

(1) El contenido de los beneficios otorgados a través del Programa de Complementación Alimentaria de la Modalidad de Hogares y Albergues, en la Asociación Impedidos Físicos FAP de la provincia Constitucional del Callao,
(2) Si había existido alguna evaluación que acredite la condición de los beneficiarios y su inclusión en el respectivo registro, y
(3) Conocer la evaluación de 10 personas que se detallaban en el pedido.

La solicitud fue presentada el 10 de octubre de 2012. El Ministerio de la Mujer y Desarrollo Social entregó la información el mismo día de la solicitud apenas ésta fue tramitada. En realidad, de la experiencia de esta consulta, ésta ha sido la única entidad pública que ha entregado la información además de hacerlo en tiempo más que oportuno.

3.4 Relevar el modo en que se gestiona la información personal de funcionarios públicos

Para este extremo se eligió solicitar información en dependencias públicas de funcionarios diversos en relación con:

(1) Curriculum vitae,
(2) Salario,
(3) Declaraciones juradas,
(4) Sanciones administrativas,
(5) Evaluaciones de desempeño,
(6) Antecedentes penales y policiales, e
(7) Información vinculada a su salud.

Se presentaron tres solicitudes en este marco de la consulta, una en Lima y dos en Chiclayo, el cuarto centro poblado más importante del Perú.

3.4.1 Solicitud presentada en Lima

El 11 de octubre de 2012 se presentó una solicitud a la Municipalidad Distrital de Jesús María, requiriendo la información arriba referida del jefe de la Oficina de Rentas. Los funcionarios de la mesa de partes municipio no sólo no recibieron la solicitud sino que además negaron tajantemente que tuvieran obligación alguna de entregarla.

3.4.2 Solicitudes presentadas en Chiclayo

El 12 de octubre de 2012 se presentó una solicitud a la Municipalidad Provincial de Chiclayo requiriendo la información antes mencionada del Jefe del Órgano de Control Institucional. Los funcionarios de la mesa de partes del municipio tampoco recibieron la solicitud pero alegaron oralmente que era una oficina de la Contraloría General de la República quien debía poseerla.

El 15 de octubre de 2012 se presentó entonces la misma solicitud de información Oficina Regional de la Contraloría General de la República en Chiclayo. Lo insólito de este episodio fue que la mesa de partes tampoco recibió la solicitud indicando que solamente se hacía de manera electrónica vía correo. Al enviarse ese mismo día la solicitud por vía electrónica, nunca hubo un acuse de recibo del requerimiento. A la fecha de cierre de esta consulta, la Contraloría General de la República no ha respondido tampoco a nuestro pedido.

3.5 Relevar la cantidad de casos resueltos por las autoridades de aplicación sobre las tensiones entre el derecho a saber y la protección de los datos personales

En el plano específico del conflicto entre ambos derechos, no existen abundantes sentencias del Poder Judicial o del Tribunal Constitucional que aborden específicamente esta problemática.

Quizás la primera decisión que aborda tangencialmente el tema, de las sentencias que han sido publicadas, es la que recayó el 15 de julio de 2003 sobre el Exp. No. 1480-2003-HD/TC. En dicho caso, el abogado de un acusado en un proceso penal solicitaba a un centro de salud estatal la entrega de una copia certificada de la historia clínica de su representado, la cual contenía la acreditación de una enfermedad de relevancia para efectos de su estrategia de defensa. El Tribunal Constitucional confirmó la denegatoria del pedido bajo el siguiente breve argumento:

> Como se ha hecho referencia en el fundamento anterior, uno de los límites a los cuales se encuentra sujeto el derecho de acceso a la información lo constituyen aquellas informaciones que afectan la intimidad personal. En efecto, el derecho de acceso a la información registrada en cualquier ente estatal no comprende aquella información que forma parte de la vida privada de terceros. Y la información relativa a la salud de una persona, como se establece en el inciso 5) del artículo 17° del Texto Único Ordenado de la Ley N.° 27806, Ley de Transparencia y Acceso a la Información Pública, se encuentra comprendida dentro del derecho a la intimidad personal.
>
> Sin embargo, lo anterior no es óbice y tampoco impide que el recurrente pueda solicitar que esa información le sea proporcionada a través del juez penal, en la medida, desde luego, en que dicha información se considere relevante para la dilucidación de la controversia penal que se le viene siguiendo[253].

Nótese que para este caso, la negativa es "a secas", sin que se ponderen los derechos en juego. Es decir, la regla sería algo así como "si la información afecta el derecho a la intimidad personal (es decir, si es información confidencial), entonces no podrá ser entregada al ciudadano a menos que lo ordene un juez penal".

Encontramos una sentencia posterior del Tribunal Constitucional en la que por vez primera se comienza a soslayar que la tensión entre ambos derechos no puede resolverse *a priori* sino que requiere una ponderación entre los intereses en juego. En la decisión recaída el 14 de septiembre de 2009 sobre el Exp. No. 4407-2007-HD/TC, el Tribunal Constitucional debía resolver en torno a la procedencia de una solicitud que buscaba conocer algunos datos (bienes muebles e inmuebles así como ahorros e inversiones de los funcionarios y sus cónyuges en el sistema financiero) contenidos en las declaraciones juradas de altos funcionarios del Ministerio de Transportes y Comunicaciones. Al respecto, se dijo lo siguiente:

> Lo expuesto, nos conduce entonces a determinar, independientemente de si la norma que clasifica como información reservada la sección primera de las declaraciones juradas tiene rango legal o reglamentario, si es que la información comprendida en la sección primera de la declaración jurada forma parte, en efecto, del contenido constitucionalmente protegido del derecho a la intimidad; y si, de ser el caso, resulta proporcional la difusión de dicha información en procura de la realización de otros fines constitucionalmente legítimos, como lo son la transparencia en la gestión pública y el propio derecho de acceso a la información[254].

En el caso, solamente se declara procedente la entrega respecto a la información que, siendo parte de las declaraciones juradas, podía ser conocida a través de otros mecanismos, y que por tanto, era indudablemente pública. En sus párrafos finales, la sentencia del Tribunal Constitucional precisa que:

> Es necesario agregar que la información solicitada está referida a personas que han ostentado cargos públicos y que existe un alto interés público en conocer la mayor cantidad de información respecto de tales personas, más aún dados los altos índices de corrupción que aún existen en nuestro país y la lucha

[253] Disponible en: http://www.tc.gob.pe/jurisprudencia/2004/01480-2003-HD.html. Este mismo criterio ha sido ratificado en dos decisiones más recientes del Tribunal Constitucional (Exp. No. 04159-2009-PHD/TC y Exp. No. 00147-2011-HD/TC). La última de estas decisiones se encuentra disponible en: http://www.tc.gob.pe/jurisprudencia/2011/00147-2011-HD%20Resolucion.html.

[254] Disponible en: http://www.tc.gob.pe/jurisprudencia/2009/04407-2007-HD.pdf.

frontal contra dicho flagelo que deben realizar el Estado como la sociedad civil. Sin embargo, el otorgar publicidad e información tan detallada de los funcionarios públicos y de sus cónyuges constituye una pretensión que se distanciaría del interés público para pasar al ámbito de la mera curiosidad, la misma que no encuentra en modo alguno respaldo constitucional.

El ejercicio de una función o servicio público no puede implicar, en modo alguno, la eliminación de sus derechos constitucionales a la intimidad y a la vida privada, más aún si la difusión de determinada información puede implicar una eventual amenaza o daño a otros derechos fundamentales como la integridad personal y la propiedad privada de las personas cuya difusión de información se pretende.

4. DOCUMENTO DE BUENAS PRÁCTICAS

En esta sección identificamos las buenas prácticas desarrolladas por las autoridades de implementación para la armonización de la regulación del derecho a saber con la de los datos personales. Como puede colegirse de la primera sección, esta práctica en el Perú es virtualmente inexistente.

Algo que en todo caso vale la pena comentar es lo que se puede deducir a partir de las sentencias del Tribunal Constitucional a las que hicimos referencia párrafos arriba. El Tribunal Constitucional, a partir de lo dicho en su sentencia recaída en el Exp. No. 4477-2007-HD/TC, parece señalar que no basta la mera calificación de la información o dato como reservado a efectos de denegar una solicitud. En efecto, de acuerdo a lo prescrito en la decisión habría además que aplicar un *test* de proporcionalidad para así determinar cuál de los derechos en conflicto debe preferirse. Al respecto, el Tribunal Constitucional sostiene que:

(…) debe concluirse que la información relativa a los ingresos provenientes del sector privado y a los instrumentos financieros de las personas que han ostentado la calidad de funcionarios o servidores públicos se encontraría protegida por el derecho constitucional a la vida privada, por lo que deberá establecerse si su difusión o publicidad (entendida como disposición a cualquier persona interesada) resulta una restricción proporcional a la privacidad en procura de alcanzar fines constitucionalmente legítimos como la transparencia de la gestión pública, la lucha contra la corrupción y el derecho de acceso a la información pública.

Lamentablemente, más allá de esta decisión, no hemos conocido de casos en los que se haya establecido la aplicación de dicho estándar cuando el acceso a la información y la protección de los datos personales entre en conflicto.

Por otro lado, en cuanto a los principios de transparencia activa incluidos en la legislación, el TUO (Ver Anexo 1) ha establecido la obligación de implementar una serie de medidas que pongan a disposición de la ciudadanía la información que requiere el ejercicio de la vigilancia social:

(1) La designación de un funcionario en cada entidad que sea responsable de entregar la información (artículo 3).
(2) La difusión a través de los Portales de Transparencia de cada entidad de sus datos generales, disposiciones y comunicados emitidos, su organización, organigrama y procedimientos, las adquisiciones de bienes y servicios que realicen, información presupuestal, remuneraciones y beneficios del personal, actividades oficiales, e información adicional que la entidad considere pertinente (artículo 5).
(3) La prohibición de destruir la información que posea la entidad (artículo 21).
(4) La obligación de la Presidencia del Consejo de Ministros de remitir un informe anual al Congreso de la República dando cuenta de las solicitudes de información atendidas por las entidades de la Administración Pública (artículo 22).
(5) La publicación trimestral de información sobre finanzas públicas y la obligación de remitirla a la vez al Ministerio de Economía y Finanzas para que sea incluida en su portal de internet (artículo 25).

Lo anterior va bastante de la mano con los principios de transparencia activa planteados en la Ley Modelo. En la práctica sin embargo, si bien los puntos (2) a (5) se verifican casi cabalmente en su cumplimiento, el mayor reto consiste en el cumplimiento del punto (1)[255]. Buena parte de instituciones carecen de un funcionario designado que se haga responsable de la entrega de información. Evidencia de ello son las experiencias narradas en la sección 3.2. Los funcionarios involucrados en las experiencias narradas en muchos casos inclusive desconocían que tenían la obligación de dar respuesta –en algún sentido- a la solicitud que se les presentaba.

En todo caso, la mejor experiencia en este proceso fue la obtenida a partir de la solicitud presentada el 10 de octubre de 2012 ante el Ministerio de la Mujer y Desarrollo Social, cuyos funcionarios nos entregaron la información el mismo día de la solicitud, apenas ésta fue tramitada (Ver sección 3.1.2 y Anexo 11). No obstante, dicha experiencia ha sido en realidad, un oasis en medio de una tendencia evidente a no entregar la información.

Es, en cierta forma, la ironía de esta experiencia: si bien el acceso a la información parece estar mejor implantado en la cultura institucional, es todavía el secretismo la fuerza determinante o más poderosa cuando se presentan eventuales tensiones y conflictos entre ambos extremos.

Normativa y material considerado

Decreto Supremo No. 043-2003-PCM, Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública.
Decreto Supremo No. 072-2003-PCM, Reglamento de la Ley de Transparencia y Acceso a la Información Pública.
Ley No. 29733, Ley de Protección de Datos Personales.
Proyecto de Reglamento de la Ley de Protección de Datos Personales.
Anteproyecto de Ley con la finalidad de crear una Autoridad Nacional para la Transparencia y el Acceso a la Información Pública como ente rector de un Sistema Nacional en la Materia.
Certificado médico sobre la salud de Raúl Cantella Salaverry de 7 de octubre de 2011.
Certificado médico sobre la salud de Raúl Cantella Salaverry de 15 de diciembre de 2011.
Solicitud de información sobre la salud de Raúl Cantella Salaverry presentada a la Clínica San Pablo el 7 de septiembre de 2012.
Solicitud de información sobre la salud de Raúl Cantella Salaverry presentada a la Clínica San Felipe el 13 de septiembre de 2012.
Carta de respuesta de la Clínica San Felipe de 17 de septiembre de 2012.
Solicitud de información sobre los beneficiarios de un programa de complementación alimentaria presentada al Ministerio de la Mujer y Desarrollo Social el 10 de octubre de 2012.

[255] Entrevista con Fernando Castañeda.

Caso de estudio uruguayo

Por Edison Lanza y Tania Rosa Pírez

1. Relevamiento normativo

Uruguay ha regulado en forma paralela el derecho de acceso a la información público (en adelante AIP) y el derecho de protección de datos personales (en adelante PDP), como derechos autónomos e instrumentales a diversos fines (protección de otros derechos fundamentales, transparencia, intimidad, etc.). Lo hizo a través de dos leyes sancionadas en un mismo paquete por parte del Parlamento en el año 2008.

1.1. Acceso a la información pública

En Uruguay el derecho de acceso a la información pública está regulado por la ley 18.381 (en adelante LDAIP), que establece un procedimiento administrativo específico para acceder a este tipo de información, así como obligaciones de transparencia activa, la existencia de un órgano de control y un recurso judicial efectivo para el cumplimiento del derecho. La ley fue reglamentada por el decreto del Poder Ejecutivo 232/2010.

Finalidad

La finalidad explícita de la ley es dotar a la administración pública de un mayor grado de transparencia, establecer obligaciones de rendición de cuentas por parte de los organismos, permitir la efectiva participación de los ciudadanos en asuntos de interés púbico y facilitar el control social de la gestión del Estado.

Sujetos obligados

De acuerdo a la LDAIP los sujetos obligados son "los organismos públicos sean o no estatales". Esta escueta definición no ha sido obstáculo para que se entendiera pacíficamente que la ley abarca a todos los poderes del Estado, los organismos de la administración central, los entes autónomos y servicios descentralizados e incluso los gobiernos departamentales.

No obstante, el organismo de aplicación ha entendido que las sociedades comerciales privadas, con capital accionario propiedad del Estado, no se encuentran comprendidas dentro de los sujetos obligados por la ley. En ese sentido, la norma uruguaya no cumpliría con todos los estándares establecidos a nivel interamericano (en especial la Ley Modelo de Acceso a la Información Administrativa de la OEA), que alcanza a este tipo de sociedades. Cabe anotar que en Uruguay esta definición tiene un alto impacto en la falta de transparencia de un nuevo sector estatal, que maneja una importante cantidad de fondos públicos, dado que han proliferado sociedades creadas por el Estado para manejar diversos negocios y funciones públicas.

Información pública

La definición de información pública que ofrece la ley es amplia (art. 2) e incluye "toda la que emane o esté en posesión" de cualquiera de los sujetos obligados. De acuerdo a esta definición se presume pública toda la información producida, obtenida, en poder o bajo control de los sujetos obligados, con independencia del soporte en que estén contenidas". Se trata de una definición amplia, que si bien tiene una naturaleza indeterminada, hasta el momento no ha generado problemas en cuanto a una interpretación del concepto de información pública.

Principios

A diferencia de lo que ocurre en otras legislaciones, la ley uruguaya no prevé un capítulo destinado a enumerar los principios del derecho al acceso a la información pública. No obstante los estándares y principios del derecho internacional de los derechos humanos se encuentran implícitamente incorporados a la legislación nacional a través del artículos 72 de la Constitución de la República y de los artículos 82 y 332 de la Carta, del cual se derivan todos aquellos aplicables a la forma republicana de gobierno. La propia ley de acceso por las vía de los hechos recoge en sus soluciones los principios de máxima transparencia, gratuidad, derecho a un recurso efectivo, etcétera.

Aunque no es la mejor forma de recepcionarlos, el decreto reglamentario de la LDAIP avanzó respecto a la sistematización de estos principios y en el capítulo II recoge a texto expreso los siguientes: libertad de información; transparencia, máxima publicidad, divisibilidad, ausencia de ritualismo, no discriminación, oportunidad, responsabilidad de los sujetos obligados; y gratuidad (arts. 4 al 12).

Asimismo, el decreto reglamentario en su artículo 24 reguló la denominada "prueba de daño" como requisito de aplicación de la denegatoria de información basada en las excepciones reguladas en la ley.

El procedimiento administrativo se encuentra regido por los artículos 13 a 18 de la ley 18.381. La solicitud puede ser presentada por "cualquier persona física o jurídica" (art 13). La definición amplia y sin discriminar por la nacionalidad o características del solicitante cumple con los estándares internacionales.

Principales características de la ley de acceso a la información pública:

a.- La solicitud de acceso a la información puede ejercer sin necesidad de "justificar las razones por las que se solicita la información" (arts. 3 y 13 de la ley 13.381).
b.- La solicitud, su trámite y el acceso son gratuitos. Únicamente será a costa del interesado la reproducción, pero éste solo pagará el precio del costo del soporte, sin ningún arancel adicional (art. 17). La definición incluye la prohibición a texto expreso de cobrar otro costo que el del soporte en el que se entrega la información. Esto procura impedir que la administración imponga una barrera económica al acceso y a su vez se la protege de conductas irracionales de parte de los solicitantes.
c.- El procedimiento prevé un plazo de 20 días hábiles para franquear el acceso a la información o denegarla por resolución fundada, pero prevé que incluso se permita el acceso en el mismo momento de la solicitud. El organismo requerido también puede hacer uso de una prórroga por otros 20 días hábiles con razones fundadas y por escrito. (Art. 15)
d.- Ni la ley, ni ningún decreto reglamentario, prevén un mecanismo específico y obligatorio de asesoramiento.
e.- El organismo solo podrá negar el acceso a la información mediante resolución motivada del jerarca del organismo que señale la norma legal cuando ésta haya sido declarada reservada o confidencial. Vencido el plazo de 20 días sin resolución fundada la ley de DAIP incluye una disposición muy progresista que entiende el silencio como una respuesta positiva del Estado, y los funcionarios quedan obligados a entregar la información respectiva. La sistemática de la ley no incluye una apelación dentro del proceso administrativo; si establece un recurso judicial específico para el acceso a la información que se puede activar directamente tras una negativa u omisión de entregar la información, lo que se analiza en el capítulo siguiente.

1.2. Protección de Datos Personales.

La ley 18.381 de Protección de Datos Personales y Habeas Data (en adelante LPDP) no es la primera, ni la única destinada a proteger este tipo de información relativa a la intimidad de las personas. Con anterioridad a la aprobación de esta norma, existía legislación que refería únicamente a datos personales para información comercial. La LPDP fue modificada en 2011 por la ley 18.719 que profundizó las competencias y potestades del órgano de control. El marco legal fue reglamentado por el decreto del Poder Ejecutivo 414/2009.
Siguiendo a Ekmekdjian y Pizzolo, la LPDP puede caracterizarse como una "ley ómnibus" cuyo objetivo es brindar una protección general "contra el procesamiento automatizado de datos".[256]

Objeto

La LPDP regula el tratamiento de los repositorios públicos o privados que contengan datos personales, susceptibles de tratamiento y de toda modalidad de uso posterior (art. 3). Conforme a la ley uruguaya, el derecho a la protección de los datos personales se aplica a las personas físicas y "por extensión a las personas jurídicas" (Art. 2). La inclusión de las personas jurídicas dentro del ámbito subjetivo de la norma ha sido cuestionada por parte de la doctrina en función de la consideración del derecho a intimidad como una especie del género de los derechos personalísimos.

Finalidad

Garantizar la protección de los datos personales como un derecho inherente a la persona humana; proveer de recursos efectivos, administrativos y judiciales para acceder a información de carácter personal que se encuentre poder de terceros; ejercer el derecho a suprimir, rectificar, actualizar e incluir datos propios (art. 15); instrumentar la acción judicial de habeas data con similar contenido que la administrativa, pero cuya procedencia refiere al incumplimiento de los sujetos obligados de sus obligaciones de protección (artículos 37 y siguientes).

Sujetos obligados

[256] Durán Martínez, Derecho a la Protección de Datos Personales y al Acceso a la Información Pública, p. 42, AMF, Montevideo, 2009.

De acuerdo a esta norma las personas públicas o privadas (físicas o jurídicas) deberán registrar sus bases de datos, ante el Registro de Bases Personales de la Unidad Reguladora de Control de Datos Personales (URCDP). La regulación exceptúa a una serie de bases por su finalidad: las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito; y las bases de datos creadas y reguladas por leyes especiales. Aunque de acuerdo a la LPDP estas bases quedan por fuera de su regulación, en entrevista con los investigadores el presidente de la URDCP sostuvo que la unidad recibe igualmente consultas de los responsables de las mismas a efectos de procurar armonizarlas a los principios y estándares que rigen el derecho a la protección de los datos personales.

Definiciones

LPDP define las distintas categorías (artículo 18) de datos personales (personales y personales sensibles), su forma de recolección, acceso y transmisión.

A la luz de reciente jurisprudencia comparada hay una serie de datos personales que no tienen especial protección y por ende pueden ser publicitados y abiertos al acceso público por parte de los organismos estatales, aun cuando están asociados a la percepción de recursos públicos.

i) Dato personal: Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.
No constituyen datos especialmente protegidos: Los datos de identificación (nombre, domicilio, estado civil, firma, firma electrónica, RUT, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad).

ii) Datos sensibles. Constituyen datos personales que revelen origen racional o étnico, preferencias políticos, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual (art. 4).Los datos sensibles son "especialmente protegidos" por la LPDP y, en consecuencia, nadie puede ser obligado a proporcionarlo sin su consentimiento, así como se requiere el consentimiento expreso y escrito del titular para su tratamiento.

No obstante este principio general tiene algunas excepciones de acuerdo a la ley Uruguaya. No será necesario el previo consentimiento cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal" (art.9).

Como contrapartida, los datos sensibles solo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general, autorizadas por ley, o cuando el organismo solicitante tenga un mandato legal para hacerlo (art. 18).

Es interesante apuntar, a los fines del derecho de acceso a la información pública, que estos datos podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares.

Sin perjuicio de que la ley uruguaya no determina el contenido de cada categoría de datos personales sensibles, CAinfo realizó la siguiente caracterización en el marco de un trabajo de consultoría para el Ministerio de Desarrollo Social:

a.- Datos Ideológicos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

b.- Datos relacionados con la salud: Estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

c.- Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.

d.- Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

e.- Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.

f.- Origen: Étnico y racial.

iii) Bases de datos. La LPDP designa indistintamente al conjunto de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que sea la modalidad de su formación, almacenamiento, organización o acceso.
Tanto la LPDP como su decreto reglamentario introducen un amplio listado de otras definiciones (tratamiento, transferencia, bloqueo o supresión de datos, etc.).

Principios

La ley define expresamente los principios generales para la protección de datos personales, que deben seguirse como criterios de interpretación y aplicación de las normas vinculadas a la protección de la intimidad y del tratamiento de las bases de datos. De acuerdo al artículo 5 son los siguientes: Legalidad; Veracidad; Finalidad; Previo consentimiento informado; Seguridad de los datos; y Reserva.

1.3 Interacción normativa entre el DAIP y la PDP

Ambas leyes fueron aprobadas como parte de un mismo sistema de regulación del derecho a la información en su doble dimensión: individual y colectiva.
La interacción entre ambas normativas se establece a título de excepción a la información pública. El artículo 9 numeral II de la LDAIP establece que "los datos personales que requieran previo consentimiento informado" se consideran "información confidencial". Esto debe interpretarse armónicamente con el artículo 2º. de la LDAIP que establece la publicidad de toda información que emane o esté en poder de los organismos públicos, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales.
El sistema regulatorio no prevé mecanismos específicos para dirimir conflictos entre ambas leyes. No obstante, las dos regulaciones contienen un amplio capítulo de principios generales que resultan útiles a la hora de procurar armonizar la realización de ambos derechos. Otro factor interesante del sistema uruguayo lo constituye el hecho que ambas unidades se encuentran en la órbita del mismo organismo AGESIC y comparten por ley uno de los integrantes de los respectivos Consejos Ejecutivos. Esto ha llevado a que desde el Estado se refiera a este sistema como "dos caras de la misma moneda".
Las unidades de control de ambas leyes (PDP y AIP) coordinan ante consultas o denuncias sobre la vulneración de un derecho por el otro, o sobre la apertura de determinada información en poder de los organismos públicos que pueda vulnerar datos personales sensibles (Ver: apartado 2.3.3).

2. Diseño institucional

2.1 Diseño institucional para la implementación de la regulación de acceso a la información pública

La ley 18.381 estableció la creación de la Unidad de Acceso a la Información Pública (UAIP) –un organismo desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) "dotado de la más amplia autonomía técnica", que cuenta con la potestad de denunciar ante las autoridades competentes cualquier conducta violatoria a la ley de acceso y aportar las pruebas que consideren pertinentes; es decir que también cumple con un rol de asesor.

La UAIP está compuesta por un Consejo Directivo de tres miembros, el director ejecutivo de AGESIC y dos que se elegirán de entre individuos que, "por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficacia y objetivad e imparcialidad en el desempeño de sus cargos. El mandato de los integrantes de la Unidad es de cuatro en su cargo pudiendo ser reelectos.

Solo podrán ser removidos de sus cargos por "ineptitud, omisión o delito", y de acuerdo con las garantías del debido proceso. La presidencia rotará de forma anual entre los dos miembros designados por el Poder Ejecutivo (Artículo 19). Si bien esta fórmula garantiza la independencia técnica de los directores, el sistema de designación en manos directamente del presidente de la República, sin control parlamentario, no asegura un proceso de designación totalmente autónomo del gobierno nacional.

En cuanto al soporte de personal técnico y no técnico para desarrollar sus funciones, la UAIP cuenta con dos abogadas full time que realizan diversas tareas técnicas (estudian los expedientes por denuncias, asesoran al Consejo, desarrollan guías y capacitaciones). También tiene una gerenta de proyectos y una funcionaria administrativa, que comparte tiempo con tareas concernientes a la agencia en la cual se inserta.

Una de las integrantes del Consejo Ejecutivo de la UAIP renunció a su cargo en mayo de 2012. La ex directora del Consejo Ejecutivo de la Unidad de Acceso a la Información Pública (UAIP), Sonia Sena, denunció al matutino La Diaria,

que renunció por falta de apoyo, recursos y potestades para implementar la Ley de Acceso a la Información Pública, lo que constituye una señal preocupante de que se está debilitando el cumplimiento del derecho a la información.[257]

A la fecha, octubre de 2012, después de haber renunciado una de sus directoras, el Consejo se mantiene desintegrado. No obstante lo cual, la restante directora (actualmente ejerciendo la presidencia de la unidad) manifestó para esta investigación que si bien no ha sido fácil trabajar con la organización que cuenta la UAIP el órgano "recibe mucho apoyo" de la AGESIC para desempeñar sus funciones de manera adecuada. Añadió que en el marco de esta asistencia que proporciona la Agencia se contrató consultorías para monitorear el cumplimiento de la ley, y se realizaron cursos de capacitación dirigidos a funcionarios públicos. Señaló que actualmente se está trabajando para profesionalizar de la UAIP.

Actualmente la UAIP realiza el control de la información clasificada como reservada por parte de todos los organismos, ya que el 31 de julio venció el plazo para culminar con ese proceso.

La UAIP también cuenta con un Consejo Consultivo de cinco miembros, que el Consejo Ejecutivo podrá consultar sobre una gama de asuntos. Los cinco miembros del Consejo Consultivo representarán al Poder Judicial, el Ministerio Público, la academia, la sociedad civil y un experto en derechos humanos nombrado por la legislatura. Será presidido por el presidente del Consejo Ejecutivo (Artículo 20).

Es conveniente aclarar que los miembros del Consejo Ejecutivo y del Consejo Consultivo no perciben remuneración, lo que constituye una debilidad notoria de la autoridad de aplicación, implementación y control de la LDAIP. [258]Asimismo, a pesar de contar con independencia técnica, la UAIP no cuenta con presupuesto propio.

La ley le asigna los siguientes cometidos (art. 21):

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 presente ley en los sujetos obligados.

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.

E) Capacitar a los funcionarios de los sujetos que están obligados a brindar el acceso a la información.

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 presente ley por parte de todos los sujetos obligados.

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 presente ley y aportar las pruebas que consideren pertinentes.

De la amplia competencia que la LDAIP le otorga a la UAIP para vigilar el cumplimiento de la misma, se ha entendido por parte del propio organismo que cuenta con la facultad de resolver denuncias presentadas por parte de los ciudadanos

[257] Entrevista del matutino La Diaria a la ex directora de AGESIC (Sonia Sena).
[258] En la última ley presupuestal, se incluyó una dieta para los dos integrantes del Consejo Ejecutivo designados por el Poder Ejecutivo. Se trata de una partida fija que cubre mensualmente los gastos de participación en el Consejo Ejecutivo pero no reviste el carácter de salario.

contra los sujetos obligados. De acuerdo a lo manifestado por la presidenta de la Unidad, se interpretan las presentaciones de los ciudadanos ante el organismo como peticiones y en función de esa calificación jurídica se emite una resolución administrativa. Esta facultad no ha sido impugnada hasta el momento por ninguno de los sujetos obligados denunciados

La UAIP recibe en promedio unas 60 denuncias anuales de particulares, respecto al incumplimiento de obligaciones de acceso a la información y transparencia por parte de los sujetos obligados.

El órgano de control cuenta con un staff permanente muy reducido (más allá de algunas consultorías puntuales que ha contratado). Su cuerpo técnico está compuesto por dos abogadas especializadas en el área a tiempo completo. Estas dos profesionales, realizan los informes técnicos para el Consejo Ejecutivo ante las denuncias recibidas por los particulares, estudian las solicitudes de asesoramiento y realizan el análisis de la información clasificada como reservada por todos los sujetos obligados, en coordinación con el Consejo Ejecutivo. Las tareas administrativas de la UAIP están a cargo de una persona, la que a su vez cumple funciones en la AGESIC (no es exclusiva de la unidad). El equipo se completa con una gerenta de proyectos.

2.2- Diseño institucional para la implementación de la regulación de datos personales.

La ley 18.331 estableció la creación de la Unidad Reguladora y de Control de los Datos Personales (en adelante URCDP) como un órgano desconcentrado de la AGESIC con autonomía técnica. [259]

La Unidad está compuesta por un Consejo Ejecutivo de tres miembros. La integran el director ejecutivo de AGESIC y otros dos directivos designados por el Poder Ejecutivo. El mandato de los miembros es de cuatro años con posibilidades de reelección. La remoción del cargo sólo está prevista para los casos de "ineptitud, omisión o delito" y debe tramitarse de acuerdo con las garantías del debido proceso.

Si bien, al igual en que el caso anterior, la ley procura asegurar la independencia técnica de los directores, corresponde reiterar la observación realizada en el ítem anterior con respecto al mecanismo para su designación.

El órgano de control cuenta con un Consejo Consultivo de cinco miembros, integrado por un representante del Poder Judicial del Ministerio Público, la academia, un integrante del sector privado y un experto en derechos humanos nombrado por la legislatura.

La infraestructura y el personal son provistos por la AGESIC. La URDCP cuenta con un staff de 10 abogados y escribanos, que selecciona el Consejo de la unidad con la AGESIC. Sus directores son honorarios, aunque uno de ellos es remunerado en régimen de "pase en comisión" de la propia AGESIC.

Desde el punto de vista de los recursos, de acuerdo al art. 33 de la ley 18.331, el órgano "formulará su propuesta de presupuesto al Poder Ejecutivo", el que lo elevará al Parlamento para su aprobación conforme a lo establecido en el art. 214 de la Constitución Nacional.

Aunque esto parece indicar algún grado de autonomía, el presidente de la URDCP declaró para este trabajo, que la aprobación del presupuesto finalmente está sometido a lo que disponga la AGESIC, la agencia en la que se inserta. No obstante, el jerarca explicó que en general se acuerda entre la Unidad y la AGESIC las partidas presupuestales que se le asignan a la protección de datos personales.[260] De hecho, el presupuesto de AGESIC y las unidades de acceso a la información y protección de datos personales no se encuentra discriminado.

En lo que respecta a la competencia funcional, la ley atribuyó a la Unidad Reguladora y de Control de los Datos Personales los siguientes cometidos:

> A) 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.
> B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas en la ley.
> C) Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.

[259] El texto legal prevé que durante su mandato los miembros de la unidad "no recibirán órdenes ni instrucciones en el plano técnico".

[260] Entrevista realizada por los autores a Federico Monteverde, el 6 de setiembre de 2012.

D) 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. 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 aquéllas 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.

Cuando sea necesario para el debido cumplimiento de las diligencias precedentes, requerirá orden judicial de allanamiento.

E) 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.

F) 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.

G) 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.

H) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.

Como se desprende de la enumeración legal el órgano cuenta con amplias potestades de control, inspectivas y sancionatorias, pudiendo disponer: apercibimientos, multas, la suspensión y en casos extremos la clausura de la base de datos respectiva.

Las potestades sancionatorias están reguladas en el art. 35 de la LPDP. Las sanciones van desde la observación, el apercibimiento, la fijación de una multa de hasta 500.000 Unidades Indexadas (el valor de la UI lo fija diariamente el Poder Ejecutivo), la suspensión de la base de datos hasta por cinco días, o la clausura.

Para proceder a la clausura la LPDP dispone que la AGESIC deberá promover ante la justicia ordinaria tal solicitud. En el caso en que no exista pronunciamiento por parte del juez en el plazo de tres días, la URCDP queda habilitada para disponer la clausura. Si con posterioridad la justicia se pronuncia en forma contraria a la misma, la medida debe ser levantada.

En el caso de la multa, la resolución administrativa que haga lugar a su aplicación constituye título ejecutivo a efectos de la promoción de un proceso judicial para el cobro de la misma en caso de ser necesario (art, 35, LPDP).

Cometidos/Diseño institucional	Unidad Acceso a la Información Pública	Unidad Reguladora y de control de Datos Personales
Consultivos	-Asesora al Poder Ejecutivo (Art. 21, A) -Orienta y asesora a particulares respecto al derecho de acceso a la información pública (Art. 21, D). -Órgano de consulta sobre la aplicación de la ley (Art. 21, G)	-Asesora titulares del derecho y sujetos obligados sobre alcance y aplicación de la ley (Art. 34, A). -Asesora al Poder Ejecutivo (Art. 34, G) -Emite opinión a solicitud de autoridades. (Art. 34, F)
Reglamentarios	Ejerce potestades de reglamentación (Art. 20 in fine)	Dicta normas reglamentarias (Art.34,B)
Inspectivos	No tiene	Realiza inspecciones necesarias para el control cumplimiento ley. Pude realizar incautaciones de información y/o exigir exhibición de documentos (Art. 34, D)
Sancionatorios	No tiene	Aplica sanciones en caso de violación de la ley: apercibimiento, multas suspensión o clausura de la base de datos, en éste último caso debe promover procedimiento jurisdiccional (Art. 35).
Control	-Controla implementación de la ley por parte de los sujetos obligados (Art. 21, B). -Realiza informa anual sobre el cumplimiento de la ley (Art. 21, I). -Denuncia ante autoridades competentes cualquier conducta violatoria de la ley (Art. 21, J).	-Realiza censo de bases de datos (Art. 34, C). -Solicita información a entidades públicas y privadas sobre tratamiento de datos personales (Art. 34, E). -Amplias facultades inspectivas (Art.34).
Estructura	-Consejo Ejecutivo de tres miembros (dos designados por el Poder Ejecutivo entre personas que garanticen independencia técnica. Es asistido por un Consejo Consultivo con pluralidad de actores.	-Consejo Ejecutivo de tres miembros (dos designados por el Poder Ejecutivo entre personas que garanticen independencia técnica. Es asistido por un Consejo Consultivo con pluralidad de actores.
Presupuesto	-No tiene presupuesto propio.	-Define su presupuesto en coordinación con AGESIC

2.3 Mecanismos para la resolución de controversias

2.3.1 – Instancias de apelación para que los ciudadanos planteen sus controversias en vía administrativa.

Las leyes uruguayas no contienen previsiones específicas para una apelación interna, ni para tramitar una apelación ante una unidad administrativa independiente de supervisión y vigilancia. Sin embargo, ambas unidades (UCRP y UAIP) cuentan con la potestad de denunciar ante las autoridades competentes cualquier conducta violatoria del derecho y aportar las pruebas que considere pertinentes.

Como se vio en el punto anterior, la UAIP recibe este tipo de denuncias e incluso confeccionó para ello un formulario que se puede bajar desde su página web. De acuerdo a la entrevista mantenida con la presidenta del organismo, María del Carmen Ongay, la UAIP interpreta estas denuncias como peticiones y se pronuncia mediante resoluciones administrativas que son pasibles de ser impugnadas por los sujetos obligados, de acuerdo al marco del derecho administrativo vigente. También pronuncia dictámenes que recogen el criterio técnico de la unidad en determinados

temas. Estos dictámenes se dictan ante solicitudes de asesoramiento, "son informes técnicos y por lo tanto no son recurribles".[261]

En virtud del diseño institucional del órgano de control, en la práctica las resoluciones que éste dicta no son definitivas y están sujetas a revisión del Poder Ejecutivo, vía recursos administrativos.[262] Se han producido casos en los cuales el sujeto obligado impugna la resolución de la UAIP que le ordena entregar determinada información, esta unidad mantiene su decisión pero cuando el asunto es elevado a la Presidencia de la República (órgano jerárquico de la AGESIC-UAIP), ésta lo revoca.[263]

A juicio de la presidenta de la UAIP las debilidades institucionales del órgano de control, no repercuten en la autonomía técnica del organismo:

"La autonomía técnica no se ve debilitada por esta circunstancia. No es letra muerta. La UAIP lleva su autonomía al extremo. No recibe una sola llamada ni una sola solicitud para actuar de tal o cual manera. La UAIP es realmente un desconcentrado técnico".[264]
Sin perjuicio de la autonomía técnica que señala la ley, el hecho de que la unidad esté sometida a jerarquía administrativa de la Presidencia conspira contra el efectivo cumplimiento del derecho, puesto que por la vía de los recursos administrativos es posible revocar una resolución y dilatar varios años el cumplimiento del derecho.[265]

Paralelamente, el diseño institucional habilita la posibilidad de que existan pronunciamientos contradictorios de los órganos jurisdiccionales sobre la publicidad de determinada información. En tanto las resoluciones de la UAIP son recurribles en vía administrativa es posible que, agotada la vía administrativa, se lleve el caso ante el Tribunal de lo Contencioso Administrativo (TCA) para que determine si un organismo público debe o no entregar determinada información. Pero al mismo tiempo, como la ley previó una acción judicial para los casos de denegatoria de la información o silencio de la administración, puede darse la hipótesis de que otro interesado en la misma información presente su caso ante la justicia ordinaria y obtenga una sentencia. Ambas sentencias podrán o no coincidir. Esto determina que una información pude ser reputada pública por la justicia ordinaria y que paralelamente el TCA entienda lo contrario, o viceversa. Esta circunstancia preocupa a las autoridades de la UAIP.

El caso de la Protección de Datos Personales. La LPDP asume facultades para recibir denuncias de particular sobre el incumplimiento de la ley. En efecto el artículo 34 literal a) dispuso como cometido asistir y asesorar a las personas que lo requieran acerca del alcance de la ley y de los medios que disponen para garantizar sus derechos.

De acuerdo a la entrevista mantenida con el presidente del Consejo Ejecutivo de la UDCP, Federico Monteverde, dictamina en función de la interpretación que realiza de la ley, en cuanto ésta le atribuye facultades para asesorar a los particulares.[266]

La URDCP distingue sus resoluciones entre tipos: dictámenes, sanciones y resoluciones. Todas son pasibles de ser impugnadas por los sujetos obligados, de acuerdo al marco del derecho administrativo vigente.

2.3.2 – Instancias de apelación para que los ciudadanos planteen sus controversias en vía judicial.

Tanto para garantizar el AIP como la protección de datos personales, las respectivas leyes establecieron procesos sumarios específicos para proteger los derechos en juego. En ambos casos siguen un idéntico tracto procesal y se sustancian en forma similar a la acción de amparo de los otros derechos constitucionalmente protegidos.

a) Acceso a la información pública

[261] Entrevista de los autores con la presidenta de la UAIP, abogada María del Carmen Ongay y las técnicas de la UAIP, abogadas Mariana Gatti y Mariana Ghione, realizada el 14/9/2012.
[262] Recursos de revocación y jerárquicos establecidos en el artículo 317 de la Constitución para impugnar los actos administrativos, ante la misma autoridad que los haya cumplido. El jerárquico opera cuando se trate de una autoridad sometida a jerarquía.
[263] Resolución del Poder Ejecutivo del 24/8/2012 revoca Resolución 09/2011 de la UAIP.
[264] Ob.cit.6.
[265] Agotada la vía recursiva mediante la presentación de los recursos administrativos correspondientes, los involucrados en la contienda tienen la posibilidad de enviar el caso al Tribunal de lo Contencioso Administrativo (TCA), lo que lleva años para dilucidarse.
[266] Ob. Cit. 5.

El capítulo V de la Ley 18.381 regula la acción de acceso a la información pública[267]. Los supuestos ante los cuales procede la acción son: la denegatoria (dentro de los cuales encontramos la declaración de reserva, confidencialidad o secreto) de la información o el silencio del organismo público obligado al vencimiento del plazo legal para responder a la solicitud de información en vía administrativa (lo que configura el denominado silencio positivo).[268] El agotamiento de la vía administrativa por cualquiera de estos dos supuestos constituye un requisito de admisibilidad de la acción en vía judicial.

Una vez incoada la acción, el juez tiene un plazo de 72 hs para dar traslado de la misma a la parte demandada (el organismo público correspondiente) y fijar audiencia dentro de ese plazo. La sentencia deberá ser dictada al cabo de la misma, pudiendo diferirse la resolución por motivos excepcionales por tres días más. El magistrado tiene la potestad de dictar medidas para mejor proveer.
La sentencia de primera instancia será apelable. La segunda instancia también se procesa sumariamente.

b) Datos Personales

El capítulo VII de la Ley 18.331 regula la acción de protección de datos personales o habeas data. La misma tiene por finalidad garantizar a toda persona física o jurídica el conocimiento de los datos referidos a la misma que obren en una base de datos pública o privada - y en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización - exigir su rectificación, inclusión, supresión o lo que se entienda que corresponda.

En lo que respecta al tracto procesal, como se señaló al comienzo esta acción se sustancia mediante el proceso sumario ya descripto.

Los presupuestos ante los cuales procede la acción son los siguientes:

- Cuando el titular del derecho, su representante legales o sucesores no hayan podido acceder por vía administrativa o extrajudicial al conocimiento de sus datos personales registrados en una base de dato pública o privada, por denegatoria expresa o por falta de respuesta en el plazo previsto legalmente.

- Cuando el titular del derecho, su representantes legales o sucesores no hayan podido lograr la rectificación, actualización, eliminación, inclusión o supresión de un dato personal en vía administrativa o extrajudicial, o no se les haya dado respuesta en el plazo legal.

[267] La doctrina nacional tipifica esta acción como habeas data impropio aunque la ley no recoge esta denominación.
[268] La ley regula un procedimiento administrativo que habilita a cualquier persona a solicitar información a los organismos obligados. Dicha solicitud debe ser tramitada por la Administración en el plazo de 20 días hábiles, pudiendo prorrogarse ese plazo por resolución fundada por 20 días hábiles más.

Acción judicial	Acceso a la Información Pública	Datos Personales
Presupuesto	Denegatoria fundada de la información o falta de respuesta expresa en el plazo legal.	a) Denegatoria fundada de la información o falta de respuesta expresa en el plazo legal. b) Falta de rectificación, actualización, eliminación, inclusión o supresión de un dato personal por denegatoria expresa o por falta de respuesta dentro de los plazos legales.
Legitimación Pasiva	Organismo público obligado al que se le formuló la petición en vía administrativa.	Responsable de la base de datos pública o privada
Legitimación Activa	Persona física: La persona interesada, sus representantes legales. En caso de fallecimiento los sucesores en línea directa o colateral hasta segundo grado. Persona jurídica: el representante legal o apoderado especialmente designado.	Persona física: propio afectado titular de los datos; sus representantes o sucesores en caso de fallecimiento hasta segundo grado en línea directa o colateral.
Objeto de la acción	Garantizar el DAIP	Garantizar el DPDP
Competencia	En Montevideo: Juzgados Letrados en lo Contencioso Administrativo cuando se trata de organismo público estatal o Juzgado Letrado en lo Civil para los restantes casos. En el resto del país: los Juzgados Letrados de primera instancia a los que se les haya atribuido tal competencia.	En Montevideo: Juzgados Letrados en lo Contencioso Administrativo cuando se trata de una base de datos en poder de una persona pública estatal. Juzgado Letrado en lo Civil para los restantes casos. En el resto del país: los Juzgados Letrados de primera instancia a los que se la haya atribuido la competencia.
Contenido Sentencia	Identificación del sujeto obligado, indicación precisa de lo que deba o no hacerse; plazo para el cumplimiento.	Identificación del sujeto obligado, indicación precisa de lo que deba o no hacerse; plazo para el cumplimiento.

2.3.3 Mecanismos establecidos para la resolución de controversias entre el DAIP y el derecho a la protección de datos personales

Si bien ambas normas fueron aprobadas como parte de un sistema jurídico tendiente a desarrollar el derecho a la información de las personas en sus distintas dimensiones, el conjunto normativo no previó un mecanismo o normas específicas que refieran a la armonización entre ambos derechos.
No obstante, ambas regulaciones reconocieron ya sea por la vía legal o reglamentaria la aplicación de una serie de principios generales que sirven de orientación o guía para la interpretación y aplicación de estas normas.
En los hechos, cuando un caso llega a consideración de alguna de las dos unidades encargadas de implementar el derecho en la administración (URCDP y UAIP) e involucra la armonización de los dos derechos, se produce una consulta entre los organismos. Así lo confirmaron los presidentes de ambos organismos en entrevista con los investigadores.
De acuerdo a lo manifestado por la presidenta del Consejo Ejecutivo de la UAIP en entrevista con los investigadores [269] los casos en que se presenta una tensión entre ambos derechos son frecuentes. Refieren principalmente a temas vinculados al salario de los funcionarios públicos e información sobre empresas que contratan con el Estado. Afirmó que el diálogo con la URCDP es fluido y que hasta el presente no se han planteado discrepancias entre los dos organismos de control a la hora de resolver casos en que se plantea la necesidad de armonizar ambas normas.
En igual sentido opinó el titular del Consejo Ejecutivo de la URDCP, [270]quién expresó que ante situaciones de conflicto entre ambos derechos se busca "aplicar el sentido común, no ser dogmáticos en la aplicación de la norma y buscar un equilibrio entre los derechos". Indicó que se realiza una evaluación caso a caso en función de los principios y estándares que rigen ambos derechos.
Esta coordinación se ve facilitada por el hecho de que las unidades se encuentran circunscriptas a una misma agencia y comparten uno de los integrantes del Consejo de Directivos.

2.3.4 Mecanismo de cumplimiento de las resoluciones

En vía administrativa la Unidad de Acceso a la Información Pública emite resoluciones a las que la ley no le confiere poder vinculante a texto expreso. No obstante, las recomendaciones en buena medida son acatadas por los organismos y aquellos que no se encuentran conformes con los fallos optan por impugnar las resoluciones por vía de recursos administrativos y de la acción de nulidad ante el Tribunal de lo Contencioso Administrativo (TCA), como ya se dijo.
Un caso particular refiere a la potestad de ordenar la desclasificación de información. De acuerdo al artículo 26 del Decreto Reglamentario de la LDAIP, decreto del Poder Ejecutivo 232/2010, la UAIP tiene la potestad de ordenar desclasificar la información cuando su ha sido reservada incorrectamente. Hasta la fecha la UAIP había ordenado la desclasificación en un caso. Actualmente las técnicas de la UAIP tienen a estudio decenas de resoluciones por las que se clasificó información como reservada en virtud del mandato legal que ordena efectuar esta tarea a los sujetos obligados por la LAIP anualmente.
En el caso de los datos personales, en vía administrativa el órgano de control cuenta con potestades sancionatorias tanto frente a organismos público como personas físicas o jurídicas privadas titulares de bases de datos, a los efectos de hacer cumplir la ley (Ver apartado 2.2).
En vía judicial, las resoluciones que dicten los tribunales competentes para tramitar la Acción de Acceso a la Información y la Acción de Habeas Data, tiene efecto obligatorio y vinculante para las partes como cualquier otra sentencia judicial. En caso de incumplimiento los magistrados podrán ordenar medidas tales como fijación de conminaciones económicas a los obligados, e incluso denunciar por desacato a los organismos que incumplan la sentencia.

3- Identificación de casos

Los casos en que se plantea la tensión entre el derecho a la protección de los datos personales y el derecho al acceso a la información pública son frecuentes.
Se han seleccionado los siguientes a efectos de ejemplificar cuál ha sido la actuación de los órganos de control.

a) Resolución de la UAIP - Pro acceso a la información pública

En setiembre de 2010 el Centro Integral del Personal de ANTEL (CIPA), una asociación de funcionarios de empresa estatal de telecomunicaciones, solicitó a ANTEL conocer la cantidad de cuotas sociales con destino a CIPA y a SUTEL la otra entidad que nuclean a trabajadores del ente público. Se pidió que la información fuera desglosada por grupos ocupacionales y dentro de éstos, exclusivamente aquellos con cargos profesionales o directivos.

[269] Entrevista de los autores con la presidenta de la UAIP, abogada María del Carmen Ongay y las técnicas de la UAIP, abogadas Mariana Gatti y Mariana Ghione, realizada el 14/9/2012.
[270] Entrevista de los autores con el presidente de la URCDP, Federico Monteverde, realizada el 6/9/2012.

Ante el silencio del organismo ante la solicitud de información formulada, el caso llegó a la UAIP para su resolución. En su resolución[271], la Unidad entendió que los datos solicitados constituyen información pública, y por tanto, "debe ser entregada al denunciante, disociando los titulares y cualquier otro dato que pueda comprometer datos personales (Art. 4 literal G de la ley 18.331)".

b) Resolución de la UAIP- Pro protección de datos personales:

En julio de 2009 la UAIP recibió una consulta de la AGESIC sobre la articulación entre la ley de protección de datos personales y la ley de acceso a la información pública, solicitando además asesoramiento respecto a la información que de acuerdo a dichas normas el organismo estaba habilitado a brindar en relación a los concursos de oposición y méritos para la provisión de puestos de trabajo.

En forma previa a resolver el asunto de fondo, la UAIP estableció que "no es cometido de la UAIP establecer un pronunciamiento con alcance general". Con relación a la divulgación de la información de carácter personal perteneciente a los concursantes, la UAIP dispuso:

a) En relación a los concursantes, la entrega de toda la información discriminada y existente en los expedientes, con excepción de: "aquellos datos que nada hacen a la situación evaluada por ejemplo: estados civiles, documentos de identidad, direcciones postales y electrónicas, números de teléfono; b) datos de carácter sensible como por ejemplo, las evaluaciones sicológicas".

b) En relación a la ciudadanía en general y a la publicación de información en la página web, la UAIP recomendó que "se brinde información de puntajes globales y órdenes de prelación de todos los participantes del concurso; y en caso de solicitarse, se facilite el acceso también a los currículums vitae de los participantes en el concurso, con previsión de segregar u ocultar los datos que no se relacionan con la situación curricular evaluada".[272]

Protección de datos personales y transparencia de los programas sociales

Antecedentes

El Ministerio de Desarrollo Social (Mides), creado en 2005, es uno de los pocos organismos públicos que diseñó una política pública de acceso a la información y protección de datos personales, en cumplimiento de las normas regulatorias de ambos campos citadas en este trabajo.

En el año 2010 el Mides contrató un informe de consultoría para la implementación de ambas leyes, cuyas recomendaciones ha seguido hasta la fecha. En ese sentido, afines del 2011 el organismo puso en marcha cuatro unidades vinculadas al cumplimiento de estos derechos: de Transparencia Pasiva, de Transparencia Activa, de Seguridad de la Información y el Archivo de Políticas Sociales.

Paralelamente, se aprobó un protocolo para tramitar las solicitudes de acceso a la información pública, a los efectos de diligenciarlas de acuerdo a los requisitos y tiempos exigidos por la ley. La cartera también organiza en forma periódica cursos de capacitación en los tres aspectos analizados en este informe: acceso a la información pública, protección de datos personales y seguridad de la información.

En materia de protección de datos personales es significativa la creación por resolución de la Unidad de Seguridad de la Información con la misión de gestionar la información pública, la protección de datos personales y la seguridad de los mismos. De acuerdo a la resolución de creación que se adjunta, esta unidad analiza las solicitudes de acceso a la información para establecer a priori si la información solicitada está alcanzada o no por una excepción; también asesora, implementa y monitorea las políticas de seguridad al interior del ministerio.[273]

Los jerarcas entrevistados para este trabajo señalaron algunos ejemplos de la política de seguridad de la información: "se busca mantener los escritorios de pantalla limpios, un correcto uso del correo institucional del Mides, desarrollamos políticas de seguridad física del ambiente y políticas de destrucción de información que contiene datos personales desactualizados. Los funcionarios del Mides también firman compromisos de confidencialidad en el manejo de la información, así como las empresas privadas que entran en contacto con los locales del Mides".

[271] Resolución 011/2011 UAIP del 28 de marzo de 2011. Posteriormente, ante el incumplimiento de lo resuelto, CIPA llevó el caso a la justicia que en consonancia con lo dispuesto por la UAIP ordenó la entrega de la información.
[272] Resolución: 40/2009 del 14 de julio de 2009.
[273] Resolución 867/2011, firmada por la ministra Ana María Vignoli.

Privacidad y planes sociales

El del Plan Nacional de Emergencia (Panes), fue un vasto programa de transferencia de ayudas económicas a las familias por debajo de la línea de pobreza, desarrollado entre 2005 y 2009 como parte de las políticas de emergencia social implementada por el gobierno del Frente Amplio, una coalición de izquierda que por entonces llegaba por primera vez al gobierno.

Durante una entrevista para este informe, los responsables del área acceso a la información y archivos del Mides, indicaron que se trata de un archivo de consulta frecuente y que está abierto al escrutinio, excepto los datos que hacen referencia a "la situación socioeconómicas de las 170 mil familias beneficiarias".[274] Las fichas socio-económica de cada una de las familias beneficiarias del plan (ingresos de esas familias, estudios de cada integrante, situación de la vivienda, etcétera) es tratada como información confidencial, aseguraron los responsables de ese archivo. Cuando se solicita esa información se procede a disociar los datos socio-económico de los estadísticos.

Los responsables del área información pública aseguran que proveen la mayor cantidad de información relativa a la ejecución de planes sociales vigentes, incluyendo el gasto destinado a cada uno de ellos, las estadísticas referidas a los resultados obtenidos y la cantidad de beneficiarios alcanzados, debido a que la ejecución de los mismos queda plenamente incluida dentro de los objetivos de la LDAIP. La Unidad de Evaluación y Monitoreo de la política social realiza un reporte social con estadísticas de los planes sociales. En cambio, por el momento no se publican los nombres de los beneficiarios de esos planes, punto que se analizará más adelante.

El Mides se encuentra en proceso de registrar todas las bases de datos de beneficiarios de planes sociales ante la Unidad Reguladora de Control de Datos Personales (UCRDP).

Los mecanismos de recolección de datos para procesar las solicitudes de asistencia social tienen varias vías, pero en general para cada programa hay un formulario que el solicitante debe completar. Estos se acercan al ministerio a través de las ventanillas de la propia Secretaría de Estado o a través de llamados públicos.

Los planes sociales actualmente en marcha, que respectivamente generan sus propias bases de datos son las siguientes:

i) Programas Sociales
ii) Uruguay Trabaja
iii) Inmujeres
iv) Tarjeta Uruguay Social
v) Asignaciones Familiares

Sistema de información del área social

Un dato relevante respecto al manejo de los datos personales de los beneficiarios de planes sociales es que el Estado uruguayo construyó un Sistema de Información Integrado del Área Social (SIIAS), con el objetivo de coordinar las bases de datos de los beneficiarios de los principales organismos de asistencia social y seguridad social (Mides, Banco de Previsión Social, Salud Pública, Educación Pública, etcétera).

Se trata de un potente sistema informático que integra los registros de toda la población uruguaya con acceso a prestaciones sociales (se estima en más del 80% de la población). El Mides está a cargo de la gestión de este sistema que maneja una copia espejo de los bancos de datos de más de 40 programas sociales estatales y distintos sistemas de registro (como el registro de usuarios de la salud, de la educación pública, el certificado de nacido vivo, etc.).

En una entrevista realizada con el coordinador de este sistema, declaró que el SIIAS tiene varios objetivos: evaluar el conjunto de políticas sociales que desarrolla el Estado, planificar la política social, detectar vacíos de cobertura entre la población vulnerable, así como duplicaciones en el caso de algunos usuarios.[275] No se prevé, en principio, el cometido de controlar o dotar de más transparencia al gasto en planes sociales.

Esta megabase tiene 16 millones de registros, pertenecientes a 3.4 millones de uruguayos. A los efectos de la presente investigación, es interesante analizar cómo se resolvió la cuestión de la protección y tratamiento de los

[274] Entrevista de los autores con Daniel Distacio y Maríagnel Illarda Estomba, realizada el 31 de agosto de 2012.
[275] Entrevista con Milton Silveira realizada por los autores el 14 de octubre de 2012.

datos personales que forman parte de estas bases de datos estatales que ahora se integran para su análisis interdependiente.

En principio, los datos personales obtenidos por cada organismo que ejecuta políticas sociales no perseguía la finalidad de crear un registro nacional de beneficiarios de los programas sociales, lo cual violentaría el principio de finalidad en la recopilación y tenencia de datos personales. Si bien de la ley orgánica del Mides (17.866) surge que entre las finalidades de la cartera se encuentra la de crear y operar un "sistema de información social con indicadores relevantes", lo que lo habilita a concentrar e integrar todas las bases de datos, no pasa los mismo con las restantes bases sociales integradas al SIIAS.
La solución de este asunto se produjo a través de un decreto firmado por el Consejo de Ministros que ordena a los organismos integrados al SIIAS "aportar" al Mides "sus respectivas bases de datos, necesarias para el cumplimiento de los fines relacionados con el cumplimiento intereses legítimos del emisor y del destinatario en ejercicio de sus respectivas competencias".[276]
El decreto también establece que "la comunicación de los datos personales al sistema de información (SIIAS) no requerirá previo consentimiento informado de sus titulares, aún tratándose de datos sensibles", por encontrarse amparado en una las excepciones que la LPDP (artículo 9 de la ley 18.331). Según esta excepción no se requerirá el previo consentimiento informado para tratar datos sensibles cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado".
Como se ve, no deja de presentar dudas el hecho de que por decreto se integren bases de datos que fueron constituidas por diferentes organismos estatales con la finalidad de desarrollar prestaciones sociales. No obstante, el mismo decreto establece varias obligaciones positivas en cabeza del Mides, a los efectos de proteger la masa de datos personales que gestionará: "formalizar acuerdos de confidencialidad" con privados que quieran acceder a la base con fines de investigación; "adoptar medidas de seguridad para salvaguardar la confidencialidad e integralidad" de la base de datos; "cumplir con todas las normas relativas a la protección de datos personales", etc.

Por otra parte, el Mides está generando otras bases de datos personales sensibles que guardan relación con diversas intervenciones que realiza.

Los siguientes son los archivos identificados como sensibles:

i) Violencia doméstica,
ii) Archivo de imágenes,
iii) Trata de personas,

Se consideran confidenciales por el tipo de datos personales sensibles que maneja de las personas involucradas y se estudia adoptar medidas de seguridad especiales, como el encriptado del acceso a estas bases de datos.

Transparencia y acceso a la información de programas sociales

Finalmente, corresponde analizar la política que sigue el Mides en relación a la transparencia y el acceso a la información de los programas sociales que ejecuta. Al respecto hay que precisar que el organismo aún no definió la política de publicidad de los beneficiarios de los prestaciones sociales. Se trata de una materia pendiente, en consideración que esta cartera tiene un importante presupuesto destinado a ejecutar programas sociales. De acuerdo a los funcionarios entrevistados, se trata de una definición política cuya definición se ha dilatado en el tiempo, debido a los cambios políticos que ha sufrido el organismo.

No obstante, los jerarcas entrevistados reconocen que ha primado la lógica de no estigmatizar a los beneficiarios de prestaciones sociales. En los hechos, hasta el momento se publica el monto de dinero asignado a cada programa, la cantidad de beneficiarios y otras estadísticas, pero no es pública la identidad de quienes reciben el beneficio.

La LDAIP establece que los sujetos obligados (organismos públicos estatales y no estatales) deberán prever la adecuada organización, sistematización y disponibilidad de la información en su poder, asegurando un amplio y fácil acceso a los interesados.[277]

[276] Decreto 109/12 del 12 de abril de 2012.
[277] Artículo 5 y sgtes. de la Ley 18.381.

De esta forma, la divulgación de información relativa a la ejecución de programas sociales, el gasto destinado a cada uno de ellos, las estadísticas referidas a los resultados obtenidos y la cantidad de beneficiarios alcanzados, quedan plenamente incluidos dentro de las obligaciones de transparencia activa de la LDAIP.

Pero que dicen las leyes de acceso y protección de datos sobre los nombres de los beneficiaros de prestaciones sociales. "Los datos personales que requieran previo consentimiento informado", son considerados por la LDAIP como "información confidencial".[278] La LPDP, por su parte, establece respecto a este punto lo siguiente: "No será necesario el previo consentimiento (cuando los datos) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".[279]

Una consulta sobre el tratamiento de los datos personales realizada por el MIDES a la URCDP (Unidad Reguladora y de Control de Datos Personales) se pronuncia sobre este punto: "En cuanto a la aplicación del principio de previo consentimiento informado cabe apuntar que atento a los cometidos asignados al MIDES, por su ley de creación N° 17.866 y normas posteriores, no será exigible recabar el consentimiento informado de los titulares de los datos, en tanto estos sean efectiva o potencialmente beneficiarios de alguno de los programas manejados por el organismo que integran la base de datos macro, por resultar de aplicación el inciso c) del artículo 9 de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, que exime de tal requisito cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".[280]

La misma opinión agrega que el artículo 11 de la LPDP establece un "deber genérico de reserva" para aquellas personas físicas o jurídicas que obtuvieran legítimamente información de una base de datos que les brinde tratamiento, "estando prohibida toda difusión de la misma a terceros".

Hacia diversos niveles de publicidad

A partir de las consideraciones jurídicas reseñadas, cabe concluir que el MIDES debería establecer distintos niveles de publicidad a los efectos de satisfacer las obligaciones de transparencia y rendición de cuentas, sin vulnerar la protección de la intimidad de los beneficiarios de prestaciones sociales.

Según la LPDP y otras experiencias en el derecho comparado[281], hay una serie de datos personales que no tienen especial protección y por ende pueden ser publicitados por los organismos estatales, aun cuando están asociados a la percepción de recursos públicos.

A nuestro juicio no constituyen datos especialmente protegidos la identificación (nombre, domicilio, estado civil, firma, firma electrónica, RUT, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad).
En cambio, constituyen *"especialmente protegidos*", y deberán observarse respecto a ellos medidas de seguridad y de reserva estricta:

> a.- **Datos Ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
> b.- **Datos de Salud:** Estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
> c.- **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.
> d.- **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
> e.- **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.
> f.- **Origen:** Étnico y racial.

Recomendaciones para la toma de decisión

No hay duda de que los datos personales "especialmente protegidos" no pueden ser divulgados por el MIDES a terceros y deberían clasificarse como confidenciales.

---

[278] Artículo 10 de la Ley 18.381.
[279] Artículo 9 de la Ley 18.331.
[280] Ob. Cit. 2.
[281] Instituto Federal de Acceso A la Información Pública Sujeto obligado ante el cual se presentó la solicitud: Mario Gutiérrez Vega c/ Secretaría de Educación Pública. Expediente: 3139/09. Comisionado Ponente: Juan Pablo Guerrero Amparán.

Pero en el caso que nos ocupa, el organismo debe resolver si hace públicos los nombres y otros datos identificatorios de los beneficiarios de programas sociales, vinculados en forma directa a las prestaciones que reciben.

De acuerdo a lo analizado no hay impedimentos legales para que en cumplimiento de las obligaciones de transparencia el MIDES difunda listados conteniendo solo la identificación de los beneficiarios de los distintos programas sociales que estos reciben, vinculados o disociados de las prestaciones que reciben.

No obstante, hay que precisar que el Estado uruguayo mantiene una zona de indefinición importante en cuanto a la publicidad de salarios, beneficios, viáticos y otras retribuciones que perciben funcionarios públicos, de modo de poder identificar el dinero exacto que percibe cada funcionario. Hasta la fecha, los organismos publican en forma disociada el listado de funcionarios y sus cargos por un lado y las escalas de retribución por otro.

Asimismo, las normas anticorrupción no permiten publicar las declaraciones juradas de los funcionarios públicos, salvo las del presidente y vicepresidente de la República.

Con esto queremos explicar que no parece razonable exigir que se publiquen de modo asociado, el nombre de personas vulnerables por su situación socioeconómica y las ayudas sociales que perciben, en tanto el resto de beneficiarios de retribuciones públicas no es identificado de tal forma. Sería una forma de señalar únicamente a los más pobres, cuando para los funcionarios públicos en general se considera –creemos erróneamente como se explicita al analizar la política de datos personales sobre funcionarios públicos- que su retribución exacta es un dato confidencial.

Documento sobre buenas prácticas
Protección de datos personales e historias clínicas en Uruguay

Uruguay avanza hacia la implementación de la historia clínica electrónica (HCE) integrada en todo el país y la creación de un Banco Nacional de HCE. Mediante un acuerdo interinstitucional firmado en octubre de 2012 entre los ministerios de Salud Pública, Economía y la AGESIC[282], el gobierno creó el programa *Salud.uy*. Su cometido es concretar las metas definidas para el Sistema Nacional Integrado de Salud (SNIS) en la Agenda Digital del país para el periodo 2011-2015. [283]
El SNIS se creó a fines de 2007. En él convergen las instituciones del sector público y privado. La puesta en funcionamiento del nuevo modelo supuso la aprobación de un paquete de normas [284]que, entre otros asuntos, reglamentan la relación entre las instituciones prestadoras de servicios de salud y los pacientes.
En el marco de la reforma del sector en el año 2008 el parlamento sancionó la ley 18.335 [285]relativa a los derechos y deberes de los pacientes de la salud. La norma fue reglamentada posteriormente por el decreto del Poder Ejecutivo 274/2010. Estas disposiciones reafirman a texto expreso el carácter reservado de las historias clínicas y reglamentan el derecho de todos los pacientes a revisar y obtener una copia de la misma. Además estipulan obligaciones para los prestadores de salud respecto al: registro y custodia de los datos almacenados en las historias clínicas, deber de garantizar su reserva, y tratamiento con fines estadísticos de la información.

[282] Agencia de Gobierno Electrónico y Sociedad de la Información.
[283] Decreto del Poder Ejecutivo 405/2011.

[284] Hasta entonces existía una gran dispersión normativa. Como se señala más adelante, en lo que respecta al objeto específico de este trabajo, corresponde señalar que el país cuenta con normas que regulan el registro de datos relativos a la salud de los pacientes en las historias clínicas, al menos, desde el año 1954 (MSP, ordenanza 363/54). Varias décadas después atendiendo al proceso de informatización de la sociedad y del Estado, el Decreto 258/92 introducía la historia clínica electrónica (HCE), reafirmaba a texto expreso el derecho del paciente a acceder a su historia y obtener una copia. En el año 2003, el decreto 396/2003 dispuso nuevas normas para las HCE a efectos de asegurar la confidencialidad de la información. Se previó la aplicación de los principios de finalidad, veracidad, confidencialidad, accesibilidad y titularidad particular como criterio interpretativo para resolver las dificultades que pudieran suscitarse en la aplicación práctica de la normativa. En el año 2007 con la creación del Certificado de Nacido Vivo (Decreto 250/07) se introdujeron nuevas normas y se reguló la transferencia electrónica de datos entre las instituciones de salud, la Dirección Nacional de Identificación Civil y el Registro Nacional de Estado Civil. Más recientemente el Decreto 379/08 referente a la regulación de la investigación con seres humanos, dispuso que la recolección de datos personales relacionados con la salud es considerada investigación a los efectos del ordenamiento jurídico nacional, y por ende queda comprendida por las disposiciones de dicha norma.

[285] Ley 18.335, "Pacientes y usuarios de los servicios de salud. Se establecen sus derechos y obligaciones", publicada en el Diario Oficial el 26 de agosto de 2008.

De acuerdo a la legislación los servicios de salud son responsables de la seguridad de los datos contenidos en las HC. Asimismo se encomienda al Poder Ejecutivo "*determinar criterios uniformes mínimos obligatorios de las historias clínicas para todos los servicios de salud".*
Los asesores jurídicos del MSP consultados en el marco de la investigación indicaron que la Secretaría de Estado se encuentra trabajando en el relevamiento normativo sobre historias clínicas a efectos de generar nuevas normas que permitan entre otras cosas, avanzar en la armonización de la normativa específica con los estándares introducidos por la Ley de Protección de Datos Personales (LPDP).[286]
Casualmente ambas normas fueron sancionadas apenas con una semana de diferencia.

Información especialmente protegida

La LPDP establece que la información relativa a la salud de la persona es un dato sensible y se encuentra, en consecuencia, bajo una tutela legal especial. El artículo 19 dispone que esta información puede ser recolectada y tratada por los establecimientos sanitarios públicos o privados y por los profesionales del sector, respetando el secreto profesional, la normativa específica y lo establecido en la propia ley. Complementariamente el decreto reglamentario de la LPDP define el alcance de esta categoría de datos estableciendo que comprende: "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" (Art. 4, Decreto 424/2009).
En forma armónica, la ley de Acceso a la Información Pública (LAIP), prevé que los datos personales sensibles son confidenciales y quedan fuera del alcance del principio de máxima divulgación que rige en relación a la información en poder del Estado.
Conforme a la legislación el tratamiento de los datos personales sólo puede realizarse con el previo consentimiento informado, salvo algunas excepciones, como el caso en que éstos "*se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal"* (Art. 9, LPDP). En el caso de los datos sensibles, además, se establece que estos *"sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga un mandato legal para hacerlo"* (Art. 18, LPDP).
La coexistencia de estas disposiciones de la LPDP con, la normativa sobre derechos y obligaciones de los usuarios de la salud en lo que respecta a la política de acceso a las HC, y la regulación general del secreto profesional, plantea actualmente en Uruguay controversias jurídicas.
Según informaron los funcionarios consultados, en los casos en que, en el marco de sus potestades, el Ministerio de Salud Pública o el Poder Judicial, requieren la copia de una historia clínica, se plantea frecuentemente la discusión respecto a si las instituciones deben o no recabar previamente el consentimiento del paciente antes de remitir un facsímil de la misma al organismo requirente. Así comentó este punto uno de los entrevistados:
"Una posición señala que la reserva estaría 'levantada' cuando quien solicite el acceso a la historia clínica sea el Poder Judicial o el propio Ministerio de Salud Pública. Paralelamente hay otra corriente doctrinaria que armonizan ambas normas entendiendo que para ello se requiere recabar el consentimiento del paciente. Esta es una práctica que adoptan muchas instituciones hoy. Lo cierto es que hoy muchas sedes judiciales solicitan la historia a través del Ministerio. El Ministerio solicita copia de la historia clínica completa a las instituciones y sanciona si no se cumple con ello".[287]

Regulación e implementación

Uruguay cuenta con normas legales y reglamentarias relativas al registro, tratamiento, custodia y acceso a las historias clínicas desde hace décadas, las que han venido experimentado sucesivas modificaciones en el marco de las distintas políticas públicas que los sucesivos gobiernos han implementado para mejorar el sistema sanitario. No obstante, persisten algunos desafíos en la implementación de la normativa (ver recuadro).
Conforme la legislación vigente, el paciente tiene derecho a conocer todo lo relativo a su salud y a que se lleve una historia clínica completa, escrita o electrónica (Art. 18, ley 18.335). El correcto llenado de la historia clínica forma parte de la atención a la salud. El trabajador actuante tiene la responsabilidad de realizar el *"registro correspondiente de manera completa, ordenada, veraz e inteligible"* (Art. 29, Decreto 274/2010).
El contenido mínimo de las historias clínicas se encuentra definido al menos desde el año 1954. [288] Estos requisitos son actualizados por el MSP periódicamente de acuerdo a las metas asistenciales que va trazando la

[286] Entrevista de los autores con el Asesor de la Dirección de Habilitaciones Sanitarias y Economía de la Salud del MSP, abogado Aldo Prisco, y la Asesora Letrada de la Dirección General del Sistema Nacional Integrado de Salud (DGSNI) del MSP, abogada Claudia Damiano, realizada el 5/9/ 2012.
[287] Ob. Cit. 4, Dr. Prisco.
[288] Ordenanza 363/54.

política sanitaria nacional y a los avances de la medicina. La secretaría de Estado controla y aplica sanciones en los casos en que se detectan errores u omisiones en el llenado de las historias clínicas.[289]
La legislación uruguaya admite que las historias clínicas se lleven en formato papel o electrónico. Muchas instituciones se encuentran hoy en plena etapa de transición, algunas gestionan la historia clínica sólo en formato papel y otras en ambos.[290]
La ley de derechos y deberes de los pacientes de la salud atribuye a los servicios de salud la responsabilidad de dotar de seguridad a las historias clínicas.
Si bien desde el Ministerio no se han definido protocolos que establezcan disposiciones y medidas específicas en relación a la seguridad de los datos, *"si hay normas que establecen que las instituciones son responsables de una adecuada conservación de la historia clínica, partiendo de la base que el prestador es el depositario de un bien del usuario".*[291]
En efecto, el art. 34 del decreto 272/2010 establece que *"los servicios de salud deberán conservar y custodiar las historias clínicas de sus pacientes, sin alterarlas ni destruirlas, de acuerdo a los requisitos y procedimientos establecidos por las disposiciones vigentes".*
El plazo durante el cual instituciones médicas deben conservar la historia clínica de sus pacientes también está regulado. Mientras dure la relación contractual con el prestador de salud, éste tiene la obligación de custodiar dicha información. Una vez que el paciente se desafilia o fallece, se debe mantener la historia clínica en forma completa durante un periodo de dos años. Para el caso de la llamada "historia clínica pasiva" – es decir la perteneciente a aquellos usuarios que no asisten a ningún control o consulta por un plazo de tres años. [292]En estas hipótesis, la normativa vigente establece que la institución deberá confeccionar una ficha en la que se resuman los datos más importantes de la salud del paciente. Dicha información la debe custodiar por plazo indefinido.[293]

Cesada la obligación de custodia, la destrucción y/o microfilmación de las historias clínicas son admitidas por la legislación vigente, si bien no se establece expresamente los mecanismos idóneos para la destrucción de este tipo de documentos. [294]

El control de los registros médicos también está regulado. Desde el año 1984 las instituciones de salud deben contar con una Unidad de Registros Médicos, la que tiene entre otros cometidos, la revisión periódica de la forma en que se llevan los mismos.[295] En el año 2008 el MSP también dispuso la creación de las *Comisiones Institucionales de Seguridad de los Pacientes y Prevención del Error en Medicina*. Las comisiones cuentan con potestades para el control de la regularidad del registro de los datos en las historias clínicas.[296]

Política de acceso a las HC

Como se estableció precedentemente, la legislación reconoce el derecho de los pacientes a que se resguarde su intimidad. De acuerdo con el art. 20 de la ley sobre derechos y obligaciones de los usuarios de la salud la historia clínica es de propiedad del paciente y será reservada.
De la lectura complementaria entre la ley 18.335, su Decreto Reglamentario y el art. 51 literal D de la ley 18.211 [297]que dispuso la creación del Sistema Nacional Integrado de Salud, surge que sólo podrán acceder a la historia clínica:

a) El paciente o las personas que por él sean autorizadas;

b) El representante legal del paciente declarado jurídicamente incapaz.

c) En el caso de incapacidad o de manifiesta imposibilidad del paciente, su cónyuge, concubino o pariente más próximo.

---

[289] Ob. Cit. 4, Dr. Prisco
[290] Ob. Cit. 4, Dr. Prisco.
[291] Ob. Cit. 4. Dr. Prisco.
[292] Decreto 37/2005.
[293] Ob. Cita 4. Dr. Prisco.
[294]Decreto 274/2010, art. 34. Remite al Decreto 355/82 con las modificaciones introducidas por el Decreto 37/2005.
[295] Ordenanza 33/84 y modificativas.
[296] Ordenanza 482/2008.
[297] Artículo 51.- Los usuarios del Sistema Nacional Integrado de Salud tienen los siguientes derechos respecto de los prestadores integrados al mismo: D) A la confidencialidad de toda la información relacionada con su proceso y con su estancia en las entidades que presten servicio de salud, sin perjuicio del requerimiento fundado de la Junta Nacional de Salud, del Ministerio de Salud Pública y del Fondo Nacional de Recursos cuando se trate de actos médicos financiados por el mismo, siempre conservándose la condición de confidencialidad respecto a terceras personas.

d) Los responsables de la atención de la salud de los pacientes y el personal administrativo vinculado a dicha atención, incluyendo al personal del Fondo Nacional de Recursos cuando se trate de actos médicos financiados por el mismo;

e) El Ministerio de Salud Pública incluyendo la Junta Nacional de Salud cuando lo consideren pertinente.

La ley sobre derechos y deberes de los pacientes prevé la penalización de la violación del deber de reserva que recae sobre las historias clínicas, por remisión expresa a las normas sobre revelación de secreto profesional (art. 302 del Código Penal).
De acuerdo a la letra de la ley, la revelación se configurara cuando se da a conocer el contenido de la historia clínica sin que, fuere necesario para el tratamiento o mediare orden judicial, o en violación de las normas sobre firma y seguridad electrónica de las mismas.
Como hemos señalado en este trabajo, la redacción dada por estas normas genera algunos conflictos interpretativos por parte de los operadores de la salud, en cuanto algunos entienden que en virtud de la ley de protección de datos personales y de las normas sobre secreto profesional, resulta necesario recabar el consentimiento del paciente cuando el MSP o el Poder Judicial requieren una copia de la historia clínica en el ejercicio de sus funciones. Otros en cambio, entienden que la obligación de reserva quedaría levantada en estos casos por tratarse de excepciones a la regla.[298]
La ley 18.335 regula el derecho del paciente a obtener una copia de su historia clínica a sus expensas o en forma gratuita en caso de imposibilidad probada de pago.

Comunicación de datos

En consonancia con la excepción dispuesta por la ley de Protección de Datos Personales (LPDP) 18.331, el Decreto Reglamentario dispone que los datos relativos a la salud contenidos en las historias clínicas pueden ser comunicados a terceros sin previo consentimiento informado *"cuando sea necesario por razones de salud e higiene pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación".*[299]
Otra situación especialmente protegida refiera al derecho a la confidencialidad que se les reconoce a los adolescentes, respecto la información sobre su salud contenida en las historias clínicas. En consonancia con lo dispuesto por la ley 18.246 sobre salud sexual y reproductiva, el decreto reglamentario de la ley sobre derechos y deberes de los usuarios y pacientes de la salud prevé que el deber de confidencialidad del personal, en relación con el estado de salud de los adolescentes, incluye a los familiares de los jóvenes, a sus padres, tutores u otros responsables, salvo que a juicio del profesional actuante o de la Dirección Técnica del Servicio exista riesgo grave para la salud del usuario o paciente, o terceros (art. 31, Decreto 247/2010).

[298] En un reciente artículo de opinión publicado en la Revista Médica del Uruguay del Sindicado Médico del Uruguay (SMU) se afirma que la historia clínica integra el secreto profesional y que el médico o las instituciones se encuentra impedidos de brindar datos relativos a la salud de sus pacientes, al menos que sean relevados del secreto por mismo. Según esta posición, que estudia la situación para el caso de las investigaciones a cargo de la justicia penal sobre abortos, existe "una aparente colisión de intereses: por un lado, el interés público en la investigación y en la persecución de los delitos, y por otro, el interés de preservar la confianza del paciente en su médico, en no colocarlo en la encrucijada de que si se asiste se expone a una acusación penal (…) También la oposición aparece entre el interés público de perseguir el delito y la preservación del principio que proscribe la autoinculpación. Se trata en realidad de falsas oposiciones. En un Estado democrático de derecho, la persecución del delito debe respetar determinados principios y la proscripción de la autoinculpación – aún por vía indirecta mediante la violación de secretos- es uno de los principios esenciales del derecho al debido proceso". Se afirma en consecuencia que las instituciones médicas no pueden ser objeto de allanamiento para obtener historias clínicas o datos sensibles, salvo que exista consentimiento o pedido del paciente o se trate de una situación de defensa del médico demandado (Adriasola, Gabriel, La inviolabilidad de la clínica médica: custodia de la intimidad del paciente y de su historia, Rev. Med. Urug 2012; 28 (2): p128-141).
[299] Art. 32 del Decreto 274/2010.

Desafíos para la implementación del marco legal

La circunstancia de que todo nuevo paradigma requiere además de la adopción de un marco legal habilitante un cambio cultural por parte de todos los actores involucrados es, a esta altura, un hecho incontrovertible.
Hemos visto como el marco legal con el que cuenta el país busca garantizar el correcto registro, almacenamiento, tratamiento y custodia de las historias clínicas. Esto se ve reforzado por el hecho que para obtener la habilitación, todas las instituciones deben contar con una dirección de registros médicos y un archivo a cargo de profesionales de la salud debidamente formados y especializados. No obstante, más allá del marco legal general reseñado y de algunas ordenanzas existentes, a efectos de mejorar la seguridad en el manejo de la información, las autoridades sanitarias no han adoptado un protocolo que estandarice y defina con alcance nacional y específico cuáles son las medidas concretas que deberían adoptar las instituciones en este campo.
En el caso del MSP si bien todos los funcionarios están al tanto del carácter reservado de las historias clínicas, no existe un protocolo que defina normas para la seguridad de la información.
Veamos la práctica seguida en algunos ejemplos concretos: la forma en que las instituciones de salud deben entregar al MSP la copia completa de las historias clínicas de sus pacientes no está protocolizada (algunas instituciones la envían en sobre cerrado, otras no); no se ha pre-establecido a nivel de la Secretaría una política de escritorios limpios en las oficinas que manejan este tipo de información; tampoco existe un protocolo para la destrucción de información con datos sensibles.
Del mismo modo, no existe regulación especial que tutele la seguridad de la información una vez que la historia clínica ingresa al Ministerio, dando lugar a la formación de un expediente administrativo. En algunos casos, por ejemplo, sobre presunta mala praxis que han llegado a la justicia y que han tenido un alto interés público, durante la investigación administrativa se ha optado por guardar la historia clínica en una caja fuerte del MSP y prohibir que se realicen copias del expediente a efectos de resguardar la privacidad de los pacientes y la reserva de la información contenida en sus historias clínicas, pero estas medidas no se encuentran protocolizadas sino que fueron adoptadas por decisión de quienes estaban a cargo de cada caso. [300]
En otra situación, ante la forma en que se realizó la comunicación al MSP de un caso de aborto por parte de una Institución de Asistencia Médica Colectiva (IAMC), se inició una investigación administrativa para determinar si se había violado el derecho de la paciente al mantenimiento de la reserva sobre su estado de salud. En ese caso, si bien el mecanismo seguido impidió preservar la identidad de la paciente, el MSP entendió que se había actuado conforme la normativa vigente en la materia y de acuerdo a la práctica habitual y descartó que haya existido transgresión a la normativa vigente sobre protección de datos personales. [301]

Cambio cultural

En los últimos años, la adopción del nuevo marco legal relativo a los derechos y deberes de los pacientes y usuarios de la salud ha sido complementada con algunas campañas y acciones para su difusión. Con ese propósito se ha dispuesto la entrega de cartillas de derecho en las instituciones médicas y su envío postal al domicilio de los pacientes, un servicio telefónico gratuito de atención al usuario, y la difusión proactiva de dicha información a través del sitio web del Ministerio y de la Administración de Servicios de Salud del Estado.[302]
A efectos de mejorar los niveles de cumplimiento de la normativa, actualmente la distribución de la cartilla entre los afiliados forma parte del contrato de gestión entre el MSP y las instituciones públicas y privadas que conforman el SNIS. [303]
No obstante estas acciones *"han existido muchas situaciones de conflicto respecto al cumplimiento del derecho de acceso que se estipula para el usuario a su historia clínica, fundamentalmente en el interior del país".* [304]

El MSP no contaba a la fecha con información sistematizada respecto a la cantidad de procedimientos, denuncias u otro tipo de quejas iniciadas o recibidas por incumplimiento de la normativa relativa a las historias clínicas. Se preveía comenzar a sistematizar dicha información en breve.

[300] Ob. Cit. 4
[301] Todos los trámites que se inician ante el MSP se ingresan por un mismo mostrador denominado "Administración Documental". Esta oficina forma con cada asunto entrado un expediente y luego la deriva a la repartición correspondiente. Este mismo trámite es el que se sigue en la práctica por las instituciones médicas para comunicar las solicitudes de autorización para la realización de abortos. Estas peticiones son luego analizadas por una comisión especial del MSP que puede autorizar a practicar el aborto en ciertos casos legalmente establecidos. De acuerdo a lo manifestado por los entrevistados, si bien en el caso concreto se entendió que se había actuado conforme a la normativa vigente y a la práctica de la Administración, resulta necesario estudiar, o bien la revisión de la normativa sobre la comunicación de solicitud de autorizaciones para la interrupción de los embarazos para su armonización con la ley de protección de datos personales, o la adopción de protocolos que definan la circulación restringida y la seguridad de la información de este tipo de expedientes.
[302] Ver por ejemplo: http://www.msp.gub.uy/ucsnis_6062_1.html o http://www.msp.gub.uy/ucsnis_6072_1.html
[303] Ob. Cita 4. Dra. Damiano
[304] Ob. Cita 4. Dr. Prisco

Anexo I: Metodología

Este documento presenta la metodológica consensuada para el desarrollo de los casos de estudio en México, Perú, Uruguay, Chile y Argentina. El estudio desarrollará un caso de estudio por país y un documento transversal sobre buenas prácticas en la gestión de información pública con datos personales.

Propuesta metodológica

1. Relevamiento normativo: en este primer nivel la revisión deberá determinar cuál ha sido el reconocimiento normativo del derecho a saber y la protección de datos personales. Sobre este punto el caso deberá responder las siguientes preguntas:
    a. Existe en el país una ley que regula el derecho de acceso a la información pública?
    b. Existe en el país una ley destinada a proteger los datos personales?
    c. Cuál es la relación entre las dos normativas: es un mismo texto o son dos textos separados, cuál de los textos antecede al otro, alguno de los dos emerge como una reforma al marco normativo del otro?
    d. La ley de acceso a la información pública, considera la gestión de los datos personales en las excepciones?
    e. La ley que protege los datos personales, brinda lineamientos acerca de la divulgación de los datos personales? Hace alguna distinción en relación al interés general que algunos datos pudieran tener?

2. Diseño institucional para la implementación de la regulación de acceso a la información

El estudio de cada uno de los casos deberá describir y analizar los organismos encargados de implementar la ley de acceso a la información y en especial, la autonomía del organismo para resolver controversias. Para describir el organismo se propone utilizar el concepto de autonomía desarrollado en Torres (2009) en base a los estudios de Carpenter (2001) y Wilson (1989). Estos estudios apuntan a aprehender no sólo las condiciones objetivas en las que opera una agencia sino también la dinámica que distingue a una organización de otra organización. Para describir la autonomía de un organismo se contemplan las siguientes dimensiones:

- Dimensión Externa: esta dimensión apunta a evaluar si una agencia posee una definición clara de dominio-jurisdicción y sus atribuciones y si enfrenta conflictos jurisdiccionales con agencias potencialmente rivales (Wilson, 1989). En esta dimensión también se considera la posición de la agencia dentro del organigrama en tanto la ubicación en la jerarquía administrativa ha sido señalada como clave por algunos analistas del concepto de autonomía (Demarigny, in Majone, 1996; Diaz and Valdivia, 2006; Majone, 1996),

- Dimensión Interna: la autonomía de una agencia requiere de capacidades organizacionales que le permitan analizar y crear programas, y planificar y administrarlos con eficiencia (Carpenter, 200). Para desarrollar estas tareas resulta fundamental que las agencias cuenten con recursos suficientes, personal calificado y emprendedores que puedan desarrollar programas innovadores para ganar apoyo político (Carpenter, 2001; Evans and Rauch, 1999; Wilson, 1989). Apoyados en este marco teórico, la investigación analizó de qué modo se encuentran equipados los organismos encargados de proteger periodistas e investigar los ataques a la prensa.

- Identidad y diferenciación política: otro aspecto fundamental para la construcción de autonomía organizacional es la diferenciación de la agencia de aquellos que la crearon y controlan (Carpenter, 2001). Esta dimensión fue evaluada en términos de las reglas de designación de los funcionarios y en función de las acciones desarrolladas para constituir una identidad organizacional (Wilson, 1989).

Para utilizar este marco conceptual se ha operacionalizado el concepto de autonomía en una matriz que se encuentra incluida en el Anexo I.

3. Diseño institucional para la implementación de la regulación de acceso a la información

El estudio de cada uno de los casos deberá describir y analizar los organismos encargados de implementar la normativa destinada a proteger los datos personales. El estudio deberá dar cuenta de las instancias creadas para resolver controversias vinculadas con la gestión y divulgación de datos personales considerando el mismo marco conceptual descripto en el ítem anterior. En el caso de identificar un solo organismo encargado de implementar ambas normativas, deberá darse cuenta de la especial distribución de las atribuciones y del modo en que el organismo resuelve las tensiones que puedan emerger en casos donde aparezcan ambos derechos en pugna.

4. Organizaciones en acción

a. Relevar mecanismos y bases de datos mediante los cuales los organismos recolectan datos personales de manera masiva (historias clínicas, guía telefónica, información patrimonial, etc.).
b. En los casos en los que conviven las dos normativas: identificar el mecanismo mediante el cual se solicita información personal al estado: ¿se utiliza la figura del habeas data o se recurre a un pedido de información?
c. Identificar los casos en que la administración ha denegado información por poseer datos personales.
d. Relevar situaciones en las que se dan conflictos o tensiones paradigmáticas entre el derecho a saber y la protección de los datos personales como la gestión de las DDJJ, la divulgación de datos personales de los funcionaros políticos de alto rango, la publicidad del listado de beneficiarios de los programas sociales, etc.

5. Buenas prácticas

Identificar buenas prácticas que hayan sido desarrolladas por las autoridades de implementación para la armonización de la regulación del derecho a saber con la de los datos personales

- Identificar lineamientos interpretativos emitidos por las autoridades de aplicación que permitan uniformizar el modo de gestionar la información pública con datos personales
- Identificar principios de transparencia activa incluidos en la legislación o en la práctica administrativa que permitan publicar proactivamente aspectos como: nómina de funcionarios, listados de beneficiarios, etc.
- Identificar casos en los que la autoridad de aplicación o la justicia haya decidido sobre la publicación de información pública con datos personales.
-

Caso de Estudio

1. Relevamiento normativo: en este primer nivel la revisión deberá determinar cuál ha sido el reconocimiento normativo del derecho a saber y la protección de datos personales. Sobre este punto el caso deberá responder las siguientes preguntas:

a. ¿Existe en el país una ley que regula el derecho de acceso a la información pública?
   i. Objeto, finalidad, sujetos y definiciones conceptuales. Principios.

b. ¿Existe en el país una ley destinada a proteger los datos personales?
   i. Objeto, finalidad, sujetos y definiciones conceptuales. Principios.

c. ¿Cuál es la relación entre las dos normativas: es un mismo texto o son dos textos separados, cuál de los textos antecede al otro, alguno de los dos emerge como una reforma al marco normativo del otro?

d. La ley de acceso a la información pública, ¿considera la gestión de los datos personales en las excepciones o en alguna otra sección del documento?

e. La ley que protege los datos personales, ¿brinda lineamientos acerca de la divulgación de los datos personales? ¿Hace alguna distinción en relación al interés general que algunos datos pudieran tener?

2. Diseño institucional

2.1 Diseño institucional para la implementación de la regulación de acceso a la información

El estudio de cada uno de los casos deberá describir y analizar los organismos encargados de implementar la ley de acceso a la información y en especial, la autonomía del organismo para resolver controversias. Para esto se utilizará la matriz analítica que se presenta al final de este documento.

2.2 Diseño institucional para la implementación de la regulación de datos personales

El estudio de cada uno de los casos deberá describir y analizar los organismos encargados de implementar la legislación de datos personales y en especial, la autonomía del organismo para resolver controversias. Para esto se utilizará la matriz analítica que se presenta en el Anexo I.

2.3 Mecanismos para resolución de controversias

Para la descripción de los mecanismos de resolución de controversias se deberá detallar los siguientes aspectos:

a. Instancias de apelación para que los ciudadanos planteen controversias

b. Mecanismos establecidos para la resolución de controversias entre AI y DP

c. Mecanismos de cumplimiento de las resoluciones

3. Organizaciones en acción

Una vez analizadas las organizaciones en términos de su diseño, cada uno de los casos analizará el modo en que estas organizaciones resuelven las controversias y definen qué se entiende por información pública, datos personales y deciden su publicación o resguardo. Para esto, cada uno de los casos deberá:

3.1 Relevar mecanismos y bases de datos mediante los cuales los organismos recolectan datos personales de manera masiva. Para realizar esta tarea se sugiere identificar: mecanismos para recolectar informar, preservar y clasificar información y formatos para el almacenamiento de información; información a los usuarios sobre el uso de la información proporcionada.

i. historias clínicas
ii. listados de beneficiarios de un plan social

3.6 Relevar el modo en que se gestiona la información personal de funcionarios públicos

iii. Curriculum vitae
iv. Salario
v. Declaraciones juradas
vi. Sanciones administrativas
vii. Evaluaciones de desempeño
viii. Antecedentes penales y policiales
ix. Información vinculada a la salud

3.7 Relevar la cantidad de casos resueltos por las autoridades de aplicación sobre las tensiones entre el derecho a saber y la protección de los datos personales. Describir y relatar dos casos emblemáticos: uno pro-acceso y otro pro-datos personales.

Documento de buenas prácticas

Identificar buenas prácticas que hayan sido desarrolladas por las autoridades de implementación para la armonización de la regulación del derecho a saber con la de los datos personales

- Identificar lineamientos interpretativos emitidos por las autoridades de aplicación que permitan uniformizar el modo de gestionar la información pública con datos personales
- Verificar el cumplimiento y aplicación de los lineamientos interpretativos, si los hubiera.
- Identificar principios de transparencia activa incluidos en la legislación o en la práctica administrativa que permitan publicar proactivamente aspectos como: nómina de funcionarios, listados de beneficiarios, etc. Para esto se desarrollará una matriz en donde se comparará la realidad local con lo establecido en la Ley Modelo[305].
- Narrar una buena práctica identificada en la gestión de la información pública con datos personales.

[305] Los temas identificados de referencia para el relevamiento en las normativas locales son los siguientes:

a) la descripción de su estructura orgánica, de sus funciones y deberes, de la ubicación de sus departamentos y organismos, de sus horas de atención al público y de los nombres de sus funcionarios;

b) las calificaciones y salarios de los altos funcionarios;

e) sus procedimientos, lineamientos, políticas en materia de adquisiciones, contratos otorgados y datos para la ejecución y seguimiento del desempeño de contratos;

n) una lista completa de los subsidios otorgados por la autoridad pública;

Matriz para la descripción del diseño institucional de organismos

Variable independiente: diseño institucional	
Dimensión	**Indicador**
Aspectos externos	Contexto en el que surge la agencia
	Tipo de legislación que crea la agencia
	Posición de la agencia en el organigrama/cobertura territorial
	Atribuciones (especial foco en la capacidad de resolver controversias y el poder sancionatorio)
	Existencia de organizaciones rivales
Aspectos internos	Presupuesto (anual 2011, considerar la autonomía presupuestaria del organismo, considerar las ratio presupuesto/staff, presupuesto/cantidad de resoluciones o apelaciones y presupuesto/cantidad de habitantes)
	Staff (considerando la ratio cantidad de empleados/cantidad de resoluciones o apelaciones)
	Expertise de RRHH
Diferenciación política	Reglas para designación y remoción
	Duración de mandatos