SABER MÁS III

INFORME REGIONAL SOBRE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES

28 DE SEPTIEMBRE
DÍA MUNDIAL DEL SABER

alianzaregional
Por la Libre Expresión e Información

ÍNDICE

i. PRESENTACIÓN

Karina Banfi, Secretaria Ejecutiva.
Alianza Regional por la Libre Expresión e Información

El **SABER MAS** es un informe regional que publica y difunde, desde hace 3 años, la Alianza Regional por la Libre Expresión e Información. Estos informes contienen la diversidad de opiniones de los miembros que integran la red en base a su experiencia y conocimiento en el ejercicio de la promoción, implementación y defensa del acceso a la información pública.

En esta oportunidad, presentamos la tercera publicación cuyo contenido es la relación y convivencia de dos derechos, el acceso a la información pública y la garantía de la protección de datos personales. Esta relación experimenta tensiones permanentes cuando se invoca el principio de máxima publicidad de los actos públicos frente al derecho a la privacidad de los actos privados. Dicha tensión no debería existir, siempre que se establezca una clara línea entre lo público y lo privado. Sin embargo, esto no sucede a menudo, ya que se desdibujan los límites tanto en la promoción como en la implementación y con mayor énfasis en la defensa del derecho del acceso a la información pública. Este informe detalla casos en varios países que ejemplifican estos conceptos.

Hemos invitado a participar de **SABER MAS** a la organización *Article XIX* – BRASIL para transmitir la experiencia en la promoción del proyecto de ley de acceso a la información pública y su relación con la protección de datos personales. Este reporte integra, junto con los trabajos elaborados por las organizaciones miembros, el primer capítulo, que detalla la situación diversa y particular que experimentan los activistas y defensores del acceso a la información en cada uno de sus países con respecto a esta garantía. Se suma para enriquecer el contenido de este informe facilitado por el *Cyrus Vance Center for International Justice of the New York City Bar Association*, de los Estados Unidos. Presentan un capítulo técnico-jurídico sobre el tratamiento que se aplica en materia de protección de datos personales y acceso a la información pública en los Estados Unidos.

Cubriendo casi todo el continente de las Américas con la situación por país y las reflexiones del sistema estadounidense, consideramos importante incorporar a este informe los criterios que se aplican en Europa. El foco en España es puesto por la organización *Access- Info,* que nos ayuda a comprender acabadamente la necesidad de revisar del tratamiento contrapuesto que se otorga a la protección de datos personales con relación a los estándares que debería tener una necesaria ley de acceso a la información pública.

Los avances y retrocesos en materia de transparencia y acceso a la información en Latinoamérica de la última década nos permiten valorar el acceso a la información como herramienta democrática para conocer la actividad pública del Estado. Asimismo, nos obliga a profundizar el análisis para mantener el equilibrio en el ejercicio de los derechos. De esta manera, los individuos nos vemos fortalecidos por la protección y garantías provistas por el Estado y el pleno uso de los derechos fundamentales.

La Alianza Regional es una red regional constituida por organizaciones de la sociedad civil de Centroamérica, Sudamérica, México, Estados Unidos y República Dominicana dedicadas a defender y promover libertad de expresión y el acceso a la información pública en la región. Es un punto de encuentro para analizar e intercambiar experiencias entre organizaciones, a fin de proponer acciones de intervención multiplicadoras que sirvan para investigar, capacitar y promover la libertad de la expresión e información en la región. También está entre nuestros objetivos generar una interrelación entre la sociedad civil, los organismos multilaterales y los gobiernos latinoamericanos.

El "*Día Mundial del Saber*" nos permite tomar conciencia de la necesidad colectiva de hacer una práctica el pedirle al Estado información de sus actos públicos. Conocer y elaborar nuestras opiniones es fundamental para fortalecer y consolidar la vida en democracia.

Queremos agradecer la colaboración del *Cyrus Vance Center*, *Article XIX – Brasil* y *Access – Info*. Agradecemos de modo muy especial a las organizaciones miembros de la *Alianza Regional por la Libre Expresión e Información* que, una vez más, se han destacado transmitiendo sus experiencias en la defensa de los derechos. En este caso, buscaron la armonía entre la máxima publicidad de la información pública y el respeto por el derecho a la privacidad de los actos privados.

El agradecimiento también es para la consultora Silvana Fumega por su excelente trabajo de compilación y edición de este informe con la colaboración y seguimiento de Julia Fernández Cruz, integrante de la Secretaría Ejecutiva y a Moisés Sánchez, director ejecutivo de Pro Acceso – Chile por la cooperación en la metodología de trabajo para este informe.

Queda demostrado, una vez más, el carácter estratégico que tiene el trabajo colectivo que posee la Alianza Regional. A cada organización que ha participado con su conocimiento y análisis acerca de la realidad local y específica, muchas gracias.

Las organizaciones de la Alianza Regional son:

1. Acción Ciudadana (AC), Guatemala

2. Asociación de Periodistas de El Salvador (APES), El Salvador

3. Asociación Nacional de la Prensa (ANP), Bolivia

4. Asociación por los Derechos Civiles (ADC), Argentina

5. Centro de Archivos y Acceso a la Información (CAInfo), Uruguay

6. Comité por la Libre Expresión (C-Libre), Honduras

7. Consejo Nacional de Periodismo (CNP), Panamá

8. Fundación Democracia sin Fronteras (FDsF), Honduras

9. Fundación Institucionalidad y Justicia (FINJUS), República Dominicana

10. Fundación para el Debido Proceso Legal (DPLF), Estados Unidos

11. Fundación para la Libertad de Prensa (FLIP), Colombia

12. Fundación Pro Acceso, Chile

13.Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES), El Salvador

14. Fundación Violeta Barrios de Chamorro (FVBCH), Nicaragua

15. Fundamedios, Ecuador

16. Fundar- Centro de Análisis e Investigación, México

17. Instituto de Derecho y Economía Ambiental (IDEA), Paraguay

18. Instituto de Prensa y Libertad de Expresión (IPLEX), Costa Rica

19. Instituto Nicaragüense de Estudios Humanísticos (INEH), Nicaragua

20. Instituto Prensa y Sociedad (IPYS), Perú

21. Participación Ciudadana (PC), República Dominicana

22. Transparencia por Colombia, Colombia

23. Transparencia Venezuela, Venezuela

24. Trust for the Americas (OEA), Estados Unidos

ii. INTRODUCCIÓN Y METODOLOGÍA DEL TRABAJO

Silvana Fumega. Especialista en Acceso a la Información Pública y Gobierno Abierto

Desde finales de la década del 80' hasta nuestros días se han producido importantes transformaciones en el campo tecnológico[1]. Dicho progreso en la tecnología de información y comunicación convierten en tarea sencilla el tratamiento e intercambio de datos y de información[2]. Si bien esto presenta nuevos desafíos a la hora de resguardar libertades fundamentales, tales como el derecho a la privacidad, también surgen nuevas oportunidades para profundizar el ejercicio del derecho de acceso a la información pública (AIP), y por ende la transparencia de la gestión pública.

Actualmente, el derecho de Acceso a la Información Pública se encuentra regulado por leyes nacionales en 11 países de América Latina[3] – y por más de 80 en todo el mundo[4] -. Uno de los principios fundamentales- que debe estar presente en todas las leyes que regulen el mencionado derecho- es el de máxima publicidad. En ese sentido, toda información producida y/o en manos de organismos públicos debe estar a disposición de toda persona que quiera acceder a ella.

Esa misma publicidad se encuentra delimitada por una serie de excepciones, en concordancia con los estándares internacionales en la materia. El listado de excepciones- que debe estar sujeto a una ley previa- sólo incluye los motivos considerados legítimos para que los organismos públicos puedan negarse a divulgar determinada información. De todos modos, cabe señalar que no es suficiente que la información esté comprendida dentro de las excepciones de la ley para no divulgarla, sino que el organismo público debería también demostrar que la publicidad de la información podría causar un daño sustancial a ese interés legítimo[5].

Una de las excepciones a la obligación de publicar información se encuentra relacionada con la protección del derecho a la privacidad[6] y, por ende, el derecho de protección de los datos personales[7]. Este último entendido como el derecho de las personas a controlar la recolección, el acceso y uso de su información personal, que se lleva a cabo por los gobiernos y los organismos privados. Es por ello que en determinadas circunstancias pueden surgir disputas o tensiones en el ejercicio de

[1] Uno de los principales adelantos fue la creación de la Web alrededor de 1989 por el inglés Tim Berners-Lee y el belga Robert Cailliau mientras trabajaban en el CERN en Ginebra, Suiza.
[2] Datos e información no son sinónimos. Sin embargo, en este documento han sido utilizados como intercambiables. El termino "dato" hace referencia a una representación simbólica o un atributo de una entidad. Es importa destacar que el dato no tiene sentido en sí mismo, sino que se utiliza en la toma de decisiones o en la realización de cálculos a partir de un procesamiento adecuado y teniendo en cuenta su contexto. En ese mismo sentido, el concepto de "información" hace referencia a un conjunto organizado de datos.
[3] Chile, República Dominicana, Ecuador, Guatemala, Honduras, México, Nicaragua, Panamá, Perú, Uruguay y El Salvador. Dichas leyes se pueden encontrar en: http://alianzaregional.net/site/index.php?option=com_content&task=view&id=26&Itemid=19
[4] Para un listado completo, ver: http://right2info.org/resources/publications/Fringe%20Special%20-%20Overview%20FOIA%20-%20sep%2020%202010.pdf/at_download/file
[5] Ver http://www.article19.org/data/files/pdfs/standards/righttoknow.pdf
[6] Para mas información en la materia ver: http://wbi.worldbank.org/wbi/news/2011/03/10/available-now-new-working-paper-right-information-and-privacy
[7] Toda aquella información relativa al individuo que lo identifica o lo hace identificable

ambos derechos: entre el objetivo de hacer pública determinada información gubernamental y la necesidad de proteger los datos personales que puedan estar contenidos en ella.

De los ejemplos más citados que pueden llegar a generar algún tipo de conflicto entre el ejercicio de ambos derechos pueden mencionarse los pedidos de publicación de los salarios de los funcionarios públicos[8] y de los beneficiarios de planes sociales.

En relación al planes sociales, un claro y reconocido ejemplo de la relación en el ejercicio de ambos derechos es el conflicto que se suscitó en 2006 en México con la petición de apertura del padrón de beneficiarios por el programa de "Desarrollo Humano Oportunidades" en el estado de Sinaloa con el objetivo de identificar a las personas por localidad. En esa situación, el pleno del Instituto Federal de Acceso a la Información Pública (IFAI) consideró que el valor superior correspondía a las disposiciones legales que obligan a la rendición de cuentas, y resolvió ordenar al programa "Oportunidades" a cumplir con la petición del solicitante.

Un caso similar se presentó en Argentina, tal como lo señala la organización miembro, Asociación por los Derechos Civiles (ADC) en su informe, cuando patrocinaron el reclamo del Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento (Cippec),que había solicitado al Ministerio de Desarrollo Social el acceder a información sobre los beneficiarios de los planes sociales que administra ese organismo. Dicho pedido fue denegado alegando que implicaba acceder a "datos sensibles". Luego de que la justicia en lo contencioso administrativo fallara a favor de Cippec, el Ministerio presentó un recurso extraordinario[9], por lo que el caso todavía no cuenta con una resolución de la Suprema Corte.

Por todo lo expuesto, el objetivo del informe Saber Mas III en 2011, es el de conocer el estado de la relación entre el ejercicio del derecho al acceso la información y el derecho a la protección de los datos personales, tal como se ha mencionado en la presentación de este informe. Para poder cumplir con ese objetivo- así como para poder contar con información comparable- cada una de las organizaciones que conforman la Alianza Regional por la Libre Expresión e Información ha guiado su relato por un cuestionario común (expuesto más abajo), el cual ha sido diseñado con el propósito de reflejar las convergencias y tensiones entre las disposiciones legales que obligan a la rendición de cuentas y transparencia, y las que protegen los datos personales.

El trabajo de compilación y edición se realizó en base a las respuestas y relato de las organizaciones miembros sobre sus experiencias locales. Sumado al análisis sustantivo de dos informes: la situación del tratamiento de estos derechos en el continente europeo y la relación de convivencia que desarrolla el sistema legal estadounidense conforman el SABER MAS del 2011.

[8] Para un ejemplo ver de este tipo de conflictos ver: http://www.lanacion.com.ar/1214805-el-recibo-de-sueldo-de-la-presidenta-es-secreto

[9] La Alianza Regional por la Libertad de Expresión e Información se presentó en calidad de Amicus Curae (Amigo del Tribunal) con la finalidad de expresar la opinión fundada sobre el objeto del litigio. Para mas información: http://www.idea.org.py/gfx/espanol/descargas/noticias/2010/amicus-cippec-ii.pdf

iii. FORMATO DE ENCUESTA
Esta encuesta fue la herramienta utilizada para recolectar la información.

"DÍA MUNDIAL DEL ACCESO A LA INFORMACIÓN PÚBLICA"
EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES

Instrucciones para completar el cuestionario:

El objetivo de esta propuesta es contar con un informe, desarrollado por cada una de las organizaciones que conforman la Alianza Regional por la Libre Expresión e Información, acerca de la relación entre el derecho al acceso la información y el derecho a la protección de los datos personales. Este último entendido como el derecho de las personas a controlar la recolección, el acceso y uso de su información personal, que se lleva a cabo por los gobiernos y los organismos privados.

Para poder contar con relatos comparables, es necesario que cada organización se **ajuste a las preguntas del cuestionario**, a continuación. Cada una de las preguntas deberán ser respondidas con un **breve relato**.

Es importante clarificar que el relato debe tener como foco el derecho de protección de datos personales **en relación** al derecho de acceso a la información pública.

El reporte debe ir acompañado de anexos (o notas al pie) que refieran a los datos y fuentes utilizadas que dan fundamento a lo expresado en el documento.

País: **Organización:**

Cuestionario:

1. **Acceso a la Información Pública**:
    a. ¿Existe una normativa (ley o decreto) que regule el ejercicio del derecho de acceso a la información pública (AIP) en su país?

    b. ¿Cuáles son las principales características y alcance de la mencionada normativa?

    c. Explique brevemente las características del órgano de control.

2. **Protección de Datos Personales:**
    a. ¿Existe una normativa (ley o decreto) que regule la Protección de Datos Personales (DP) en su país?

    b. ¿Cuáles son las principales características y alcance de la mencionada normativa?

    c. Explique brevemente las características del órgano de control.

3. **Relación entre ambos derechos**: Tomando en cuenta lo expuesto en las primeras dos preguntas:

a. ¿Cuál es la relación entre ambas normativas?/ Según la legislación ¿alguno de los dos derechos tiene preponderación sobre el otro?

b. ¿Cómo se controla el ejercicio de ambos derechos?

c. ¿Cuáles son los mecanismos para dirimir conflictos entre ambos derechos?

4. **Casos prácticos:**
   a. ¿Podría mencionar 2 casos que puedan dar testimonio de lo expuesto en la pregunta anterior sobre la relación (conflictiva o no) entre AIP y Datos Personales en su país?

5. **Jurisprudencia**:
   a. ¿Existe jurisprudencia (incluyendo dictámenes o resoluciones del órgano de aplicación del AIP y del de Datos Personales) que haya obligado al Estado a entregar información que se **consideraba** un dato personal? *Transcribir párrafo más sustancioso de esa jurisprudencia y referenciar el caso en nota al pie.*

   b. ¿Existe jurisprudencia (incluyendo dictámenes o resoluciones del órgano de aplicación del AIP y del de Datos Personales) que haya obligado al Estado a entregar información que **fuere** un dato personal? *Transcribir párrafo más sustancioso de esa jurisprudencia y referenciar el caso en nota al pie.*

6. **Rol de la Sociedad Civil:**
   a. ¿Existe en su país iniciativas en la sociedad civil para promover la protección de datos? Redacte brevemente en qué consiste.

Parte I

1.1. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA

Asociación por los Derechos Civiles (ADC)
Director Ejecutivo: Álvaro Herrero
Director del Área de AIP: Ramiro Álvarez Ugarte

Acceso a la Información Pública

En la República Argentina existen diversas normativas que regulan el acceso a la información pública, dependiendo de si se trata del ámbito nacional o federal, provincial, o municipal. Este análisis se centra en la normativa de orden federal, es decir, el decreto 1172/03[10].

El decreto sólo se aplica en el ámbito federal y al Poder Ejecutivo. El mismo regula, en términos amplios, el derecho de acceso a la información. Establece procedimientos para acceder a la información y habilita distintos recursos judiciales para cuestionar aquellos casos en los que se deniega el acceso a la misma. Asimismo, en su artículo 16 establece diversas excepciones al principio general de "máxima divulgación" (garantizado en el artículo 8), en algunos casos remitiendo a otras normas (como, por ejemplo, la Ley de Protección de Datos Personales número 25.326).

La autoridad de aplicación del mencionado decreto reside, conforme al artículo 18 del reglamento, en una subsecretaría del Poder Ejecutivo de la Nación- la Subsecretaría para la Reforma Institucional y Fortalecimiento de la Democracia-. Dicho organismo se encuentro a cargo de un funcionario político designado por el Poder Ejecutivo y no cuenta con una estructura muy desarrollada. Sin embargo, el decreto 1172/03 creó un sistema de "enlaces"- funcionarios en cada dependencia estatal quienes están a cargo de recibir y tramitar los pedidos de acceso a la información que reciben de la población-. El sistema de "enlaces" constituye el mecanismo mas directo a través del cual se efectiviza el derecho de acceso a la información. Cabe destacar que, según el artículo 19 del reglamento, el órgano administrativo encargado de recibir denuncias e informar a las autoridades responsables sobre el incumplimiento del régimen de acceso a la información pública es la Oficina Anticorrupción, dependiente del Ministerio de Justicia y Derechos del Poder Ejecutivo Nacional.

Protección de Datos Personales

En relación al ejercicio del derecho de Protección de Datos Personales (PDP), Argentina cuanta con la ley de Protección de Datos Personales número 25.326[11].

La mencionada ley define a los datos personales en forma amplia, como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables" (artículo 2). La ley regula el manejo de "datos personales" en toda clase de archivos, tanto públicos como privados. Establece que esos datos sólo pueden ser recopilados con el consentimiento del titular y se debe garantizar su "confidencialidad". Asimismo, la regulación impone a quienes manejan

[10] http://www.infoleg.gov.ar/infolegInternet/anexos/90000-94999/90763/norma.htm
[11] http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

archivos que contienen datos personales el deber de "confidencialidad" y establece el principio de "finalidad", según el cual los datos no pueden utilizarse para fines distintos a los que fueron recolectados. En cuanto a la "cesión", el artículo 11 de la ley dispone:

> *"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."*

Es conveniente destacar que este artículo es el que mayores problemas de armonización genera con el régimen de acceso a la información pública.

El órgano de control del ejercicio del Protección de Datos Personales es la Dirección Nacional de Protección de Datos Personales (DNPDP). Su titular es un profesional de reconocida trayectoria. La DNPDP suele intervenir cuando se pone en juego la transferencia de información en manos del Estado que contiene "datos personales". De acuerdo a un estudio realizado por la ADC sobre los dictámenes de la DNPDP de los últimos tres años, la mayor parte de las intervenciones de esta dependencia está motivada en pedidos de acceso a la información pública[12].

Relación entre ambos derechos:

No existe una relación formal entre la normativa que regula el acceso a la información publica y la ley de Protección de Datos Personales. Asimismo, ningún derecho tiene preponderancia sobre el otro. Sin embargo, la relación entre las normativas existentes genera diversos conflictos de interpretación que no se resuelven en el ámbito del Poder Ejecutivo, y que –en el marco jurídico vigente— sólo pueden encontrar solución si esos conflictos se llevan al ámbito del Poder Judicial.

De todos modos, debido a que la ley de Protección de Datos Personales tiene más jerarquía que el decreto 1172/03, así como un órgano de control específico con facultades de control e interpretación en todo lo que hace a la ley, podría sostenerse que, en el ámbito del Poder Ejecutivo, los conflictos interpretativos entre la protección de datos personales y el acceso a la información se resuelven –de hecho— a favor de la primera. En efecto, según el análisis de ADC ya mencionado y sobre 45 dictámenes analizados, en un 89 por ciento de los casos la DNPDP negó el acceso a los datos solicitados o –más comúnmente— estableció condiciones para ese acceso no previstas en el decreto de acceso a la información, como la existencia de un interés legítimo[13]. Por otra parte, la interpretación de la DNPDP del concepto de datos personales es muy amplia, y ello conlleva que no pueda compatibilizarse

[12] Análisis realizado por la ADC sobre la base de un relevamiento de los dictámenes de la Dirección Nacional de Protección de Datos Personales correspondientes a los años 2008, 2009 y 2010. Según ese relevamiento, la intervención de la DNPDP se divide del siguiente modo: (a) pedidos de acceso a la información pública, 43 por ciento; (b) Interpretación de la ley, 33 por ciento; (c) Cesión de Registros 9 por ciento; (d) Contratos de Transferencia Internacional, 9 por ciento; (e) Creación de registros, 4 por ciento; (f) otros, 2 por ciento. El análisis se encuentra actualmente en desarrollo.

[13] Cabe destacar que, dentro de ese 89 por ciento, el 80 por ciento de los casos la DNPDP recomendó la entrega de la información con condiciones no previstas en el decreto 1172/03 y sí establecidas en la Ley de Protección de Datos Personales.

adecuadamente la Protección de los Datos Personales con el Acceso a la Información.

SI bien la autoridad de aplicación del decreto 1172/03 y la Dirección Nacional de Protección de Datos Personales deben velar por el adecuado ejercicio de ambos derechos por parte de la ciudadanía, se trata de dos dependencias separadas que funcionan en el ámbito del poder ejecutivo y –hasta donde se pudo averiguar— no cuentan con ningún mecanismo de coordinación de sus tareas.

Casos prácticos:

Dos casos que puedan dar testimonio de lo expuesto en la pregunta anterior sobre la relación (conflictiva o no) entre Acceso a la Información Pública y Datos Personales son:

Ejemplo 1. *Caso CIPPEC c. Estado Nacional.* En este caso, la Asociación por los Derechos Civiles (ADC) patrocinó el reclamo del CIPPEC que había solicitado información sobre distribución de planes sociales y la misma había sido denegada alegando que conocer quiénes eran los beneficiarios de esos planes implicaba acceder a "datos sensibles", que según la ley 25.326 son 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*". Según la DNPDP, "*si bien el hecho de integrar una lista de beneficiarios de un plan 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 [decreto 1172/03]".* La Subsecretaría para la Reforma Institucional y el Fortalecimiento de la Democracia se sumó a esa interpretación de la DNPDP, aunque reconoció que el acceso podría favorecer el control de la implementación de los planes sociales en cuestión[14].

Ejemplo 2. La Dirección Nacional de Protección de Datos Personales ha considerado en numerosas oportunidades que el acceso a información sobre nómina de empleados del Estado requiere la demostración de un "interés legítimo" por parte de quien lo solicita, requisito que el decreto 1172/03 no establece pero sí la ley 25.326. Ello es así por la definición amplia de "datos personales" que establece la ley, que en la práctica restringe fuertemente el alcance del derecho de acceso a la información. Así, por ejemplo, la DNPDP condicionó a la existencia de un "interés legítimo" la entrega de información relativa al salario del vocero presidencial (1/10); sobre personas detenidas durante una ola represiva en la década del sesenta (4/09); información sobre personas condecoradas con motivo de los servicios prestados durante la Guerra de Malvinas (30/09); información sobre transferencias presupuestarias a organizaciones sin fines de lucro (38/09); nómina de autoridades de la Policía Federal Argentina (3/08); información sobre personas detenidas durante un conflicto que involucró a productores agropecuarios (5/08); sueldo de la Presidenta de la Nación (37/08); entre otros[15].

Jurisprudencia:

[14] Cfr. Nota 495/08 del Ministerio de Desarrollo Social, Secretaría de Coordinación y Monitoreo Institucional, del 9 de abril de 2008.
[15] Todos los números entre paréntesis corresponden a dictámenes de la Dirección Nacional de Protección de Datos Personales, disponibles en: http://www.jus.gob.ar/datos-personales.aspx

En relación a jurisprudencia que haya obligado al Estado a entregar información que éste consideraba un dato personal, se puede citar lo resuelto por la Sala II de la Cámara en lo Contencioso Administrativo Federal en el caso *Cippec c. Estado Nacional*[16].

En dicho caso se encontraba en discusión la negativa del Estado a brindar información sobre destinatarios de planes sociales (ver Ejemplo 1, *ut supra*). Los magistrados intervinientes consideraron que no correspondía aplicar la excepción del artículo 16.i del Reglamento de Acceso a la Información Pública (decreto 1172/03), ya que "*no se advierte que existan razones válidas para dicha negativa ya que no se trata de aspectos que involucren la seguridad así como tampoco –en principio— sean susceptibles de afectar la intimidad y el honor de las personas o que pudiera importar una forma de intrusión arbitraria de la recurrente*"[17].

> *"[L]a Oficina Anticorrupción señaló claramente que los padrones de beneficiarios no son datos personales de carácter sensible (…) por lo que la información requerida con arreglo al objeto de la fundación actora que surge del artículo 2 del acta de constitución de la entidad (…) puede ser razonablemente considerada como incluida dentro de las pautas del control comunitario de la inversión social"*[18].

Rol de la Sociedad Civil:

En cuento al rol de la sociedad civil en la promoción del derecho de protección de datos personales, cabe destacar la labor de la Fundación Vía Libre que trabaja sobre cuestiones vinculadas con privacidad y nuevas tecnologías -en particular vinculadas con la vigilancia del Estado a través del uso de cámaras de seguridad y mecanismos de ciber-vigilancia-. De todos modos, la cuestión de la "privacidad" parece ser una cuestión secundaria a su agenda principal, vinculada a la tecnología.

En líneas generales, la protección de datos personales ha estado promovida, principalmente, por órganos estatales, como la mencionada DNPDP o el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires.

16 https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=1G4ljEi5gq23c55hD5loL1r0BomSUezHs15TMwEoeM5NP-Q80PhndtTXuhrSU&hl=en_US

17 Cámara Federal en lo Contencioso Administrativo Federal, Sala II. Caso CIPPEC c. Estado Nacional. Sentencia del 8 de abril de 2010. Considerando 7.

18 Cámara Federal en lo Contencioso Administrativo Federal, Sala II. Caso CIPPEC c. Estado Nacional. Sentencia del 8 de abril de 2010. Considerando 7.

1.2. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN BOLIVIA

Asociación Nacional de la Prensa (ANP)
Director Ejecutivo: Juan Javier Zeballos

Acceso a la Información Pública:

La norma que reconoce el derecho de acceso a la información pública en Bolivia es la Constitución Política del Estado (CPE) vigente desde el 7 de febrero de 2009, que en su acápite de derechos civiles, artículo 21, numeral seis dispone que los bolivianos y bolivianas tienen derecho a *"(…) acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva."*[19] La Constitución Política del Estado es la norma suprema del ordenamiento jurídico. Su aplicación es preferente a cualquier ley o decreto, y alcanza a todas las instituciones del Estado y personas individuales.

Asimismo, Bolivia cuenta actualmente con dos decretos que tratan tangencialmente el derecho de Acceso a la Información Publica; ellos son el Decreto Supremo 28168, de 17 de mayo de 2005, y el Decreto Supremo 0214, de 22 de julio de 2009. El Decreto Supremo 28168 regula el acceso a la información pública con relación a las dependencias del Poder Ejecutivo (ahora llamado Órgano Ejecutivo), en tanto que el Decreto Supremo 0214 tiene por objeto aprobar la Política Nacional de Transparencia y Lucha contra la Corrupción, con la finalidad de contar con instrumentos orientados a la prevención, investigación, transparencia, de acceso a la información y sanción de actos de corrupción.

Asimismo, la Ley Nro. 2341 de Procedimiento Administrativo- - regula esencialmente procedimientos seguidos ante entidades ejecutivas de todos los niveles de gobierno (central, departamental, municipal)- vigente desde abril de 2004 establece en su artículo 18 lo siguiente:
"Articulo 18º.- (Acceso a archivos y registros y obtención de copias).
***I.** Las personas tienen derecho a acceder a los archivos, registros públicos y a los documentos que obren en poder de la Administración Pública, así como a obtener certificados o copias legalizadas de tales documentos cualquiera que sea la forma de expresión, gráfica, sonora, en imagen u otras, o el tipo de soporte material en que figuren.*
***II.** Toda limitación o reserva de la información debe ser específica y estar regulada por disposición legal expresa o determinación de autoridad administrativa con atribución legal establecida al efecto, identificando el nivel de limitación. Se salvan las disposiciones legales que establecen privilegios de confidencialidad o secreto profesional y aquellas de orden judicial que conforme a la ley, determinen medidas sobre el acceso a la información.*
***III.** A los efectos previstos en el numeral anterior del derecho de acceso y obtención de certificados*
y copias no podrá ser ejercido sobre los siguientes expedientes: a) Los que contengan información relativa a la defensa nacional, a la seguridad del Estado o al ejercicio de facultades constitucionales por parte de los poderes del Estado. b) Los sujetos a reserva o los protegidos por los secretos comercial, bancario, industrial, tecnológico y financiero, establecidos en disposiciones legales."[20]

[19] http://www.oas.org/Juridico/mla/sp/bol/sp_bol-int-text-const.html

[20] http://bolivia.infoleyes.com/shownorm.php?id=153

Por otra parte, esa misma ley establece, en cuanto al interés legitimo, lo siguiente:

El Artículo 11º de esta ley señala que *"Toda persona individual o colectiva, pública o privada, cuyo derecho subjetivo o interés legitimo se vea afectado por una actuación administrativa, podrá apersonarse ante la autoridad competente para hacer valer sus derechos o intereses, conforme corresponda*".

En cuanto al órgano que tiene a su cargo el control del ejercicio del derecho de acceso a la información publica, exceptuando al Ministerio de Transparencia y Lucha contra la corrupción, no existe un organismo que ejerza un control preventivo especializado en materia de acceso a la información pública. El Ministerio de Transparencia y Lucha contra la corrupción no goza de autonomía ya que forma parte del Gabinete, por tanto, su ámbito práctico de acción es limitado. Asimismo, es conveniente destacar que el control preventivo que realiza el Ministerio no es significativo, ya que sus operaciones se concentran principalmente en promover procesos administrativos y judiciales después de que el acto de corrupción o falta de transparencia ocurre.

En cuanto a las denuncias relacionadas con el ejercicio del mencionado derecho pueden dirigirse a la Defensoría del Pueblo (decisiones no vinculantes), o a la justicia ordinaria.

Protección de Datos Personales:

El derecho de Protección de Datos Personales es reconocido en Bolivia por la Constitución Política del Estado, en su artículo 21, numeral 2. Dicho articulo establece que los bolivianos y bolivianas tienen derecho a "*la privacidad, intimidad, honra, honor, propia imagen y dignidad*." La misma norma en su artículo 130 reconoce la acción constitucional de privacidad bajo el siguiente régimen:

"*Artículo 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad*."

Asimismo, el Código Civil en su artículo 18 estipula que *"Nadie puede pertutar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley."*

Por otra parte, la recientemente promulgada Ley de Telecomunicaciones establece en su artículo 55 lo siguiente:
"Artículo 55. (inviolabilidad y secreto de las comunicaciones). En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias y usuarios salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma."[21]

[21] http://www.itu.int/ITU-D/treg/Legislation/Bolivia/ley_tlc.pdf

La misma ley en su artículo 83, respecto a los proveedores, establece la obligación de "*brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley."*

En cuanto a las acciones para dirimir conflictos en torno a la protección de la privacidad y los datos personales, al existir una acción constitucional específica se da por vía de la justicia de las acciones extraordinarias constitucionales. Esta es la versión actualizada de lo que en la anterior Constitución se entendía por el recurso de "habeas data". En esencia, el derecho que protege esta acción no varía. Las acciones constitucionales se interponen ante las cortes superiores distritales, con una instancia de revisión obligatoria ante el Tribunal Constitucional Plurinacional.

Al ser las instancias de control los tribunales judiciales de la justicia constitucional, la única característica que vale la pena destacar en cuanto al control del ejercicio del derecho de protección de los datos personales es la jurisdicción de estos tribunales. Las Cortes Superiores de Distrito son cortes de apelación, en la justicia ordinaria. En la justicia extraordinaria constitucional operan como tribunales de primera instancia para conocer y resolver acciones constitucionales. Resuelta la acción constitucional, ésta pasa en revisión al Tribunal Constitucional, que es el órgano llamado por ley para revisar las acciones constitucionales interpuestas ante todas las Cortes Superiores de todo el país. Cabe mencionar que el fallo de revisión genera jurisprudencia vinculante.

Relación entre ambos derechos:

No existe un criterio expreso de jerarquización de derechos. Conceptualmente se entiende que el derecho de acceso a la información y el derecho de protección de datos personales regulan materias distintas. El acceso a la información pública, se refiere a información fuera del ámbito de la privacidad o la intimidad. Sin embargo, tanto el acceso a la información como la protección de datos privados se puede realizar a través de la acción constitucional de privacidad.

El control de la vigencia de dichos derechos, por el momento, se realiza en la medida de la solicitud de la persona individual o colectiva afectada. No existe un órgano estatal encargado de prevenir posibles lesiones a estos derechos. Sin embargo, la Defensoría del Pueblo se erige como órgano promotor de los Derechos Humanos en general, y promotor de la defensa de los mismos.

Si bien la Defensoría no tiene facultad de emitir decisiones coercibles, si puede emitir pronunciamientos que generen presión sobre autoridades que, en un caso o queja específico hubieren generado riesgo o afectación efectiva de cualquier de los derechos previstos en la Constitución Política del Estado.

La autoridades competentes para dirimir conflictos y emitir jurisprudencia vinculante con criterios más específicos que los legalmente establecidos son el Tribunal Supremo (antes Corte Suprema) y el Tribunal Constitucional Plurinacionales. El mecanismo para la dirimición serían los procedimientos ordinarios y constitucionales que generen jurisprudencia vinculante.

Casos prácticos:

En cuanto a los casos que dan testimonio de la relación entre el acceso a la información pública y la protección de los Datos personales, se puede mencionar la negativa de la Fuerzas Armadas a acatar un fallo de la Corte Suprema que les obligaba a revelar la documentación que permite establecer el destino de los restos de las personas muertas durante el golpe de estado de 1981.

Jurisprudencia

Considerando que el control del acceso a la información y de los datos personales está a cargo de la justicia ordinaria y de la justicia constitucional, y en atención que solo la justicia constitucional tiene jurisprudencia disponible y sistematizada, en base a la información disponible, no se ha podido identificar un caso en el cual al Estado se le haya obligado a entregar datos personales por efecto de un reclamo de acceso a la información pública. Es por ello que cabe aclarar que, a continuación, se incluye una afirmación general extraída de la Sentencia Constitucional 0030/2006-R del 11 de enero de 2006 del Tribunal Constitucional, ya que se hizo una extensa búsqueda pero no se pudo ubicar un caso emblemático donde las cortes se hubieran pronunciado sobre la colisión de derecho de acceso a la información con el derecho de protección de datos personales.

"III.1.La naturaleza jurídica y alcances del hábeas data

Al efecto, con carácter previo a examinar y dilucidar la problemática planteada, resulta necesario referirse a la naturaleza jurídica y alcances del recurso de hábeas data, así como a los derechos que tutela este recurso instituido por el art. 23 de la CPE.
Según la doctrina del Derecho Procesal Constitucional el hábeas data es un proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informativa"; es una garantía constitucional que brinda a la persona una protección efectiva e idónea frente al manejo o uso ilegal e indebido de información sobre los datos personales generados, registrados, almacenados en bancos de datos públicos y privados y distribuidos a través de los medios informáticos.
Del concepto referido se infiere que el hábeas data es una garantía constitucional de carácter procesal para la protección de los datos personales, aquellos que forman parte del núcleo esencial del derecho a la privacidad o a la intimidad de una persona, frente a la obtención, almacenamiento y distribución ilegal, indebida o inadecuada por entidades u organizaciones públicas o privadas. Esta garantía constitucional otorga a toda persona, sea natural o jurídica, la potestad, facultad o derecho de acudir a la jurisdicción constitucional para demandar a los bancos de datos y archivos de entidades públicas y privadas con el fin de que le permitan el conocimiento, la actualización, la rectificación o supresión de las informaciones o datos referidos a ella, que hubiesen obtenido, almacenado y distribuido.

En consecuencia, siguiendo la doctrina constitucional se concluye que la protección que brinda el hábeas data abarca los siguientes ámbitos:

a) Derecho de acceso a la información o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo se que dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son

correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal.
b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos, o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podrían ocasionar graves daños y perjuicios a la persona; así, por ejemplo, si una persona aparece como procesada cuando ya fue sobreseída.
c) Derecho de corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos públicos o privados; tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona; así, por ejemplo, registren una condena penal en los datos personales cuando esa persona jamás fue sometida a proceso penal alguno, por lo mismo jamás fue condenado a sufrir pena alguna.
d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona; así, por ejemplo, balances presentados ante una entidad fiscal, pero que no tendrían que suministrarse a empresas rivales o competidoras.
e) Derecho a la exclusión de la llamada "información sensible" relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado.

En definitiva, según la doctrina el hábeas data, como garantía constitucional, reivindica el derecho que tiene toda persona a verificar qué información o dato se difunde acerca de ella y cuál es el fundamento de los datos correspondientes; asimismo el derecho a corregir o aclarar lo inexacto y solicitar la eliminación de las informaciones falsas o erróneas que, por tanto, lesionan su buen nombre, y las de aquellas que invaden la órbita reservada de su intimidad personal o familiar.

III.2 El hábeas data en el sistema constitucional boliviano

El hábeas data como una vía procesal instrumental de protección al derecho a la autodeterminación informativa, referido a los derechos fundamentales a la intimidad y la privacidad de la persona, fue incorporado al sistema constitucional boliviano mediante la Ley 2631 de Reforma de la Constitución de 20 de febrero de 2004.
Según dispone el art. 23.I de la Constitución "Toda persona que creyere estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos, de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de hábeas data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya". De la disposición constitucional glosada se infiere que, en el sistema constitucional boliviano, el hábeas data es una vía procesal instrumental para protección del derecho a la autodeterminación informativa, precautelando que la persona pueda acceder al conocimiento de los datos o informaciones, referidos a su vida privada o íntima así como la de su familia, obtenidos y almacenados en los bancos de datos públicos o privados, con la finalidad de conocer qué datos se han

obtenido y almacenado; es decir, cuánta información, con qué finalidad y a quienes se distribuyó, se distribuye o distribuirá la misma.

En consecuencia, del contenido de la norma prevista por el art. 23.I de la CPE, se infiere que el hábeas data, en el sistema constitucional boliviano, tiene por finalidad proteger el derecho a la privacidad o vida íntima contra el manejo de información sobre datos personales por medios informáticos, que según la doctrina se conoce como derecho de "autodeterminación informativa" de la persona, garantizando el ejercicio de los siguientes derechos:

1º De acceso a los datos o información referidos a su persona, que hubiesen obtenido y almacenado los bancos de datos públicos o privados, para conocer qué informaciones se consignan sobre su persona, con qué fundamentos, asimismo conocer los fines y objetivos de la obtención y almacenamiento; es decir, qué uso le darán a esa información.
2º De rectificación o corrección de la información obtenida y almacenada, si la misma contiene datos personales falsos o errados, cuya difusión podría causar graves daños y perjuicios a la persona registrada en el banco de datos.
3º De obtener la eliminación o exclusión de la llamada "información sensible" relacionada al ámbito de su intimidad o la de su familia; es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado."[22]

Rol de la Sociedad Civil:

No se conocen organizaciones de la sociedad civil que se encuentren trabajando para la promoción del derecho de protección de datos personales.

[22] Extraído de la SENTENCIA CONSTITUCIONAL 0030/2006-R de 11 de enero de 2006 del Tribunal Constitucional. http://www.tribunalconstitucional.gob.bo/resolucion13415.html

1.3. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN BRASIL

Article XIX
Coordinadora Article XIX-Brasil: Paula Martins
Organización observadora

Acceso a la Información Pública:

El derecho de acceso a la información pública es garantizado en Brasil por el artículo 5º, XXXIII de la Constitución Federal de 1988[23]. El artículo 5º es el que trata de los derechos fundamentales y es considerado *clausula petrea*. El artículo establece que sus dispositivos deberán ser reglamentados por ley, pero hasta este momento no existe una ley de acceso a la información de ámbito nacional en Brasil. De todos modos, existen dispositivos de acceso a la información presentes en legislaciones temáticas diversas, como por ejemplo en la ley de licenciamiento ambiental, la ley de combate a la violencia contra la mujer y la ley de urbanismo (también conocida como el Estatuto de la Ciudad).

A pesar de que Brasil no cuenta aún hoy con una regulación del derecho de acceso a información pública, existen dos leyes en vigencia que sí tienen un impacto sobre el derecho de acceso y hacen referencia a las excepciones al principio de transparencia contenido en el artículo 5º - las leyes 11.111/2005[24] y 8.159/1991[25]. Esas leyes disponen sobre la clasificación de documentos públicos y sobre archivos públicos (ambas son restrictivas, especialmente la primera). Asimismo, es conveniente destacar que es problemático que el país cuente con leyes que tratan del sigilo de los documentos públicos cuando no hay ley que detalle el ejercicio del derecho a la información. Las dos normativas son hoy objeto de acciones judiciales que cuestionan su constitucionalidad.

En 2003 el Diputado Reginaldo Lopes presentó un proyecto de ley (PL) de acceso a la información pública a la Cámara de los Diputados. El PL nunca fue a votación por el pleno de la Cámara y quedó parado por muchos años. En 2007 el Ejecutivo presentó un nuevo PL de su iniciativa a la Cámara. El mismo fue debatido internamente y con la sociedad, incluso con la realización de audiencias públicas. El texto revisado con algunas importantes modificaciones fue aprobado por el pleno de la Cámara en 2010 y fue enviado al Senado. En el Senado el texto de la Cámara fue aprobado sin modificaciones de contenido por 3 comisiones internas y actualmente se encuentra en la Comisión de Asuntos Exteriores. En esa misma Comisión, el Senador Collor ha sugerido diversas alteraciones que, de ser aceptadas, harían que el PL no solo tuviera que retornar a Cámara de los Diputados sino que además propone modificaciones inadecuadas al texto, poniendo en riesgo importantes principios consagrados hasta el momento y distanciando el texto del PL de los principios internacionales y mejores practicas legislativas sobre Acceso a la Información Pública.

- Jurisdicción:
El PL se aplica a todos los órganos federales, estatales y municipales. Ejecutivo, legislativo y judiciario. Administración directa e indirecta (autarquías, fundaciones

[23] http://www.constitution.org/cons/brazil.htm
[24] http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2011.111-2005?OpenDocument
[25] http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%208.159-1991?OpenDocument

públicas, empresas públicas, sociedades de economía mixta); así como entidades privadas sin fines de lucro que reciban recursos públicos.

- Es considerada información pública:
  - información producida o acumulada por órganos y entidades publicas;
  - información producida o mantenida por persona física o privada en razón de un vinculo con órganos o entidades privadas
  - información sobre las actividades de órganos y entidades, incluso sobre su política, organización y servicios;
  - informaciones sobre el patrimonio publico, utilización de recursos públicos, licitación y contratos administrativos;
  - informaciones sobre políticas publicas, inspecciones, auditorias y prestación de cuentas

- Como el proyecto facilita el acceso a la información:
  - Todos los órganos públicos estarán obligados a facilitar la divulgación de informaciones a través de: (i) la creación de un servicio de informaciones al ciudadano en ubicación y condiciones adecuadas para atender y orientar el publico, informar sobre el procesamiento de documentos, y sobre el deposito de documentos y de demandas / solicitudes de acceso a informaciones; e (ii) incentivo a la participación popular, en especial con la realización de audiencias y consultas publicas.
  - Internet pasa a ser considerada un medio privilegiado para divulgación de informaciones. Las páginas web de los órganos deben contener lenguaje y herramientas fáciles y claras para legos, pero también brindar facilidades para aquellos que manipulan datos de forma más compleja (open data). La información debe ser actualizada y estar en formatos electrónicos diversos, posibilitando acceso por maquinas. Sólo los municipios con menos de 10mil habitantes están exceptuados de la obligación de la divulgación de información por páginas web.

- Como deben ser publicadas las informaciones:
  - Existen 2 formas principales de publicación según la nueva ley: la publicación proactiva, independiente de las solicitudes, y la publicación que responde a demandas específicas. Toda información de relevante interés publico y colectivo producida o mantenida por entidades publicas debe ser publicada independientemente de demanda. Pero toda información que no tenga sido publicada previamente, puede ser objeto de pedidos de información. Los órganos públicos deben ofertar orientaciones al usuario sobre como acceder a una información y deben ofertar datos primarios, integrales, auténticos y actualizados. Cuando una información es confidencial, el acceso es liberado a todas las otras partes del documento que contiene la información, con ocultación tan solamente de la parte sigilosa.
  - Publicación de rutina: La divulgación de informaciones de manera proactiva / voluntaria está establecida en el PL a partir de criterios mínimos. Es decir, todo órgano debe ofertar automáticamente, por todos los medios disponibles, como mínimo, información sobre sus competencias, organigrama y contractos, movimientos financieros y gastos, información sobre procedimientos licitatorios, datos generales sobre acompañamiento de políticas y obras públicas y respuestas a las preguntas más frecuentes de la sociedad. Todo órgano publico debe mantener una pagina web donde, anualmente, brindara la lista de documentos que dejaran de ser considerados confidenciales, la lista de documentos confidenciales y un

informe estadístico sobre pedidos de información recibidos, respondidos y negados.

- Pedidos de Información: los pedidos de información pueden ser enviados a los órganos públicos responsables incluso vía Internet. Ellos deben identificar el demandante, pero la exigencia de identificación no puede impedir el procesamiento de la solicitud. Además, no se puede demandar justificativas cuanto a los motivos que levan el demandante a presentar el pedido de información. Una vez recibido el pedido, el órgano debe autorizar o conceder acceso inmediato a la información. Si eso no es posible, debe responder el demandante dentro de un máximo de 20 días con la siguiente información: (i) fecha, local y modo para efectuar el acceso; (ii) motivos por los cuales el acceso demandado es negado, informando igualmente los procedimientos para recurso; (iii) comunicado de que no tiene la información o que envió el pedido recibido a otro órgano que sí tiene la información; (iv) justificativa para extender el plazo de respuesta en 10 días adicionales.

- Recursos:
Siempre cabe recurso en caso de demanda de información negada o no respondida. El sistema de recursos, todavía, es confuso y descentralizado y no existe un órgano independiente responsable por las decisiones finales.

- Obligación de promoción del derecho de acceso:
La ley también establece algunas obligaciones mínimas de promoción del derecho de acceso por las autoridades públicas, incluso la capacitación de servidores públicos, la producción de material informativo, etc.

La ley no crea un nuevo órgano de control. Las actividades de promoción deben ser asignadas a un órgano ya existente y la responsabilidad por la evaluación y análisis de los recursos cabe a variados órganos, ninguno completamente independiente del Estado. El rol principal en la implementación de la ley será de la *Controloladoria Geral da União* – CGU, órgano que tiene un importante histórico de combate a la corrupción, pero que es un órgano de control interno del Ejecutivo federal.

Protección de Datos Personales:

No existe ley específica para la protección de datos personales en Brasil. El tema es regulado en términos generales por la Constitución y por el Código Civil. A su vez, se pueden encontrar dispositivos sobre el tema en otras normas variadas como el Código de Defensa del Consumidor - en especial los artículos que dicen respecto al tratamiento de datos personales por entidades comerciales-. Asimismo, en Brasil se cuenta con una ley que reglamenta el uso del Habeas Data- herramienta judicial para conocer, retirar o corregir informaciones personales constantes de banco de datos gubernamentales o de carácter público-.

Actualmente, una propuesta de proyecto de ley de protección de datos personales se encuentra en discusión- aunque aún en análisis por el Ministerio de Justicia-. Dicho Ministerio organizó una consulta pública sobre un borrador inicial y aún no divulgó si ese borrador será alterado con base a los resultados de la consulta. Información sobre el mismo pueden ser encontrada en el sitio web de la consulta on-line organizada por el Ministerio: http://culturadigital.br/dadospessoais.

La Constitución, en su articulo 5, protege la intimidad (X) y la inviolabilidad del sigilo de los datos personales (XII). La propuesta de proyecto de ley de protección de

datos regulará estos artículos constitucionales. El borrador no se aplica solamente al tratamiento de datos para finalidades exclusivamente personales y domesticas, y a los bancos de datos utilizados para el ejercicio del periodismo. Además, el borrador establece que los bancos de datos relacionados a la seguridad pública y del Estado serán regulados por una ley especifica.

La propuesta exige el consentimiento libre, expreso e informado del titular para el tratamiento de datos personales por entidades publicas o privadas, con excepción de los datos necesarios al ejercicio de las funciones propias del Estado. Los datos solamente podrán ser mantenidos por la entidad mientras sea necesario para alcanzar los fines originalmente indicados y para los cuales el titular dio su consentimiento. La propuesta contiene capítulos específicos sobre el tratamiento de datos sensibles (datos que pueden generar discriminación en contra del titular) y la seguridad de los datos. El borrador también exige el consentimiento del titular para la comunicación o interconexión de datos, así como establece reglas específicas para la transferencia internacional de datos.

Para la protección administrativa de los derechos relacionados al uso y tratamientos de datos personales, será creada una instancia administrativa llamada Consejo Nacional de Datos Personales. La propuesta de ley promueve la adopción de Códigos de Buenas Practicas por los responsables por el tratamiento de datos personales.

De todos modos, cabe destacar que la propuesta no incluye, como seria necesario, disposiciones especificas sobre datos personales de personas que se encuentren en el ejercicio de funciones públicas.

Actualmente no se encuentra institucionalizado un órgano de control, pero la propuesta de proyecto de protección de datos dispone la creación del Consejo Nacional de Protección de Datos Personales, con autonomía administrativa, presupuestaria y financiera. La propuesta dispone que el Consejo debe actuar como autoridad garante en cuanto a la protección de datos personales, con poderes para planear y proponer, coordinar y ejecutar la política nacional de protección de datos, así como poderes para editar normas, recibir denuncias, aplicar sanciones, entre otras atribuciones.

Las sanciones administrativas previstas van desde multas hasta la prohibición del funcionamiento de un banco de datos.

Relación entre ambos derechos.

Es difícil, en la actualidad, poder establecer la relación entre el derecho de acceso a la información pública y el de protección de datos personales en Brasil, especialmente considerando que la propuesta de proyecto de ley de protección de datos no ha ingresado al Poder Legislativo y el proyecto de ley de acceso a la información se encuentra en el Senado. De todos modos, cabe señalar que el sistema legal brasileño es por tradición muy civilista y privatista, y por lo tanto puede existir una tendencia a la protección mas contundente de la privacidad sobre la protección del derecho de acceso a la información. Además, el borrador de ley de protección de datos contiene la previsión de creación de un órgano de control especializado e independiente, mientras el proyecto de ley de acceso se limita a atribuir nuevas responsabilidades a órganos no independientes ya existentes y que están atascados con las atribuciones que ya hoy poseen.

Actualmente, el ejercicio de ambos derechos se controla por vía judicial. Para dirimir las disputas relacionados con ambos derechos, se puede aludir al procedimiento de "mandado de segurança", que es un procedimiento para impugnar cualquier tipo de ilegalidad cometida por una autoridad pública. También se encuentra el procedimiento de habeas data, aunque sólo para poder tener acceso a información personal).

Asimismo, en el caso que el Estado divulgue datos considerados privados, la parte interesada también puede demandar judicialmente una indemnización a través de una acción por daños morales o materiales.

Casos prácticos:

- **Divulgación de salarios de los servidores públicos.** Se produjo un intenso debate cuando la Municipalidad de Sao Paulo decidió publicar en su sitio web "De Olho nas Contas" la lista de los servidores públicos, con puestos y salarios efectivamente recibidos (o sea, salarios nominales y otros beneficios)[26].

- **Ampliación de las informaciones sobre procesos judiciales disponibles on-line.** El tema de los límites entre la privacidad y la protección de datos personales fue también muy discutido cuando el Consejo Nacional de Justicia decidió empezar una iniciativa para ampliar el acceso a la información judicial en Brasil.

Jurisprudencia:

En referencia al caso, anteriormente citado, contra la Municipalidad de Sao Paulo por la publicación de los nombres de los funcionarios de la municipalidad, seguidos de sus puestos y valor de sus salarios en una página web destinada a ampliar la transparencia municipal, se puede añadir que la municipalidad fue condenada en primer y segundo grado, pero el caso sigue en ámbito de apelación.

"La situación de estancamiento, por el contrario, apareció con la publicación de los nombres de los empleados públicos junto con sus honorarios, cuando lo cierto es que la información sobre la remuneración del cargo de la posición se hace anualmente, pero no necesariamente en correlación con el nombre del titular oficina o empleado de la Administración Pública, so pena de invasión de la privacidad del empleado público. En otras palabras, se publica en el sitio web el nombre del servidor junto con la posición y la cantidad, en cumplimiento con las normas locales, y cada año, se publica, por otra parte, el valor del subsidio y la remuneración del cargo o función, de conformidad con la regla del artículo 39, § 6 de la Constitución Federal. (...) Esta es la razón por la cual la publicación que apareció en el sitio web de la Municipalidad, en lugar de la tan mentada "transparencia" fue más allá de lo que ordena el legislador constitucional y atacó a la intimidad del servidor, sin tener en cuenta a la establecida en el artículo 37, § 3, II de la Constitución, que hace referencia expresa a la regla del artículo 5, X, de la Constitución. No es necesario mencionar que el empleado público ("persona física" antes que anda, y sujeto de derecho por excelencia), ve vulnerada su seguridad cuando el Estado, con el argumento de que cumplan un supuesto "deber de transparencia" divulga, en el

[26] Mas informacion sobre el caso:
http://jus.com.br/revista/texto/13163/divulgacao-da-remuneracao-dos-servidores-publicos
http://www.correioforense.com.br/noticia/idnoticia/46610/titulo/stf_permite_divulgacao_de_salarios_de_servidores_municipais_de_sp_na_i.html

mismo portal electrónico y, al mismo tiempo, uno al lado del otro, la información que debe limitarse a una simple referencia a la remuneración del cargo o función por una parte, y otra información que, para cumplir con las leyes locales, deben contar con mera publicación del nombre del empleado, la posición y capacidad. (...) Declarar la inconstitucionalidad e ilegalidad de la publicación conjunta, en el mismo documento o registro electrónico, de la información sobre los "remuneración bruta " de los empleados municipales y la información sobre el nombre de los mismos empleados públicos, tal como se encuentra en el sitio web de la Ciudad de São Paulo. Por lo tanto, determino la remoción de la información que se hizo en esa forma, impedir su divulgación en esos términos, por cualquier otro medio."[27]

Rol de la Sociedad Civil:

Las iniciativas por parte de la sociedad civil en relación a la protección de datos personales que han podido ser relevadas se encuentran destinadas únicamente a ampliar el debate sobre las propuestas normativas que tienen impacto sobre la privacidad y la protección de datos personales[28]; incluso dispositivos sobre protección de datos personales contenidos en la propuesta normativa para regular los derechos civiles en Internet.

En ese sentido, si bien no hay un movimiento organizado y articulado de la sociedad civil, cabe señalar algunas entidades que están trabajando individualmente en el área:

Organización de derechos del consumidor que trata del tema de protección de datos personales:

- **Instituto de Defensa do Consumidor - IDEC**
  www.idec.org.br

Centro de investigación que está trabajando en el proyecto de ley de protección de

[27] Proceso 0020793-83.2009.8.26.0053, 8a Vara da Fazenda Publica, Foro Central, São Paulo. http://www.apmsp.org.br/documento.pdf Parrafo original en portugues: *"A situação de impasse, de outra forma, surgiu com a publicação do nome dos servidores acompanhado das respectivas remunerações, quando é certo que a informação relativa à retribuição do cargo há de ser feita anualmente, mas sem necessária correlação com o nome do titular do cargo ou do empregado da Administração Pública, pena de invasão da esfera da privacidade do servidor. Em outras palavras, trata-se de publicar, no sítio da Internet, o nome do servidor, juntamente com o cargo e a lotação, em cumprimento à norma local, e todo ano, vale dizer, a cada ano, o valor do subsídio e da remuneração do cargo ou da função, em cumprimento à norma do artigo 39, § 6º, da Constituição Federal. (...)Daí porque a publicação feita no sítio eletrônico da Prefeitura, no lugar da tão propalada "transparência", acabou mesmo por despir o cidadão, pois, ao ir além do que manda o legislador constitucional, investiu contra a intimidade do servidor, sem atender à ressalva feita no artigo 37, § 3º, II, da Constituição, que remete expressamente à norma do artigo 5º, X, da Constituição Federal. Não é preciso dizer que o servidor público ("pessoa natural", antes de mais nada, sujeito de direito por excelência), vê a sua segurança vulnerada quando o Estado, sob o argumento de cumprir um suposto "dever de transparência", divulga, no mesmo portal eletrônico e ao mesmo tempo, lado a lado, informações que deveriam se resumir a simples referência à remuneração do cargo ou da função, de uma parte, e informações outras que, para dar cumprimento à lei local, deveriam ser prestadas com a só publicação do nome do servidor, cargo e lotação. (...) declar[o] a inconstitucionalidade e a ilegalidade da publicação conjunta, em um mesmo documento ou registro eletrônico, de informação relativa à "remuneração bruta" dos servidores municipais e de informação referente ao nome daqueles mesmos servidores, tal qual se encontra na listagem existente no site da Cidade de São Paulo. Por conseguinte, determino a remoção das informações que naquela forma se fez, impedida a divulgação, naqueles termos, por qualquer outro meio."*

[28] Para leer los comentarios de la sociedad civil brasileña (tercero sector/ONGs y sector privado) sobre el proyecto de ley de protección de datos (ver columna lateral izquierda): http://culturadigital.br/dadospessoais/

datos personales:

- **Centro de Tecnologia e Sociedade - CTS, Fundação Getúlio Vargas**
  http://direitorio.fgv.br/cts/

- **Habeas Data**
  www.habeasdata.org

1.4. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN CHILE

Fundación ProAcceso
Director Ejecutivo: Moisés Sánchez

Acceso a la Información Pública:

El ejercicio del Derecho de Acceso a la Información Pública en Chile se encuentra regulado a través de la ley N° 20.285[29], que fue publicada en el Diario Oficial el 20 de Agosto de 2008, que entro vigencia el 20 de Abril de 2009. La ley, cuenta a su vez, con un reglamento, contenido en el Decreto Supremo N°13/2009, del Ministerio Secretaría General de la Presidencia de Chile.

La ley 20.285 establece un procedimiento para el ejercicio del Derecho de Acceso a la información y establece la creación de un órgano público autónomo, denominado Consejo para la Transparencia, con facultades fiscalizadoras para velar por el efectivo cumplimiento de las normas de transparencia. A su vez, dicho organismo es el encargado de la promoción, publicidad y de garantizar, en definitiva, el derecho de Acceso a la Información Pública. En tercer lugar, desarrolla a nivel legal, las causales de reserva contempladas en el artículo octavo de la Constitución Política de la República de Chile, por medio de las cuales la administración pública puede negarse a entregar cierta información que obre en su poder. Por último, establece la obligación de mantener a disposición permanente por parte de los órganos del Estado, cierta información pública a través de los portales de Internet que mantienen, conocida como transparencia activa.

El mencionado Consejo para la Transparencia es un organismo público autónomo, con patrimonio propio que conoce del procedimiento de amparo a través del cual los ciudadanos a los que les hubiese sido denegada una solicitud de acceso pueden recurrir para ser analizada tal circunstancia en los términos legales que exige la ley. Asimismo, conoce de las reclamaciones que pueden formular las personas, por infracción a las normas de Transparencia Activa, esto es, información que debe estar disponible en forma permanente y actualizada en los sitios web de los organismo públicos. El Consejo para la Transparencia también puede actuar mediante el control interno que realice cada una de las entidades obligadas, ya que las unidades internas de control tendrán la obligación de velar por la observancia de la ley. Finalmente, el Consejo tiene atribuciones para "velar" por la protección de datos personales, pero para el ejercicio de esas funciones no hay un aún pautas legales. Para cambiar esta situación, actualmente se encuentra en tramitación en el Congreso Nacional, proyectos que avanzan en este punto.

Protección de Datos Personales:

La protección de datos personales en Chile se encuentra regulada a través de la ley N° 19.628, conocida también como "Ley sobre protección de la vida privada", publicada en el Diario Oficial el 28 de Agosto de 1999.

La ley 19.628 incorpora una serie de definiciones básicas en el tema de protección de datos pero no establece una entidad pública que fiscalice el cumplimiento de la normativa de protección de datos personales. Asimismo, tampoco existe un

[29] http://www.leychile.cl/Navegar?idNorma=276363

organismo estatal que promueva y aplique la ley. A su vez, no establece un catalogo preciso de infracciones y sanciones para los casos de incumplimiento de la ley.
La ley se aplica tanto a las bases de datos como a su procesamiento que se encuentran en manos del Estado como de los particulares.

En relación al control del ejercicio del derecho de protección de datos personales, actualmente Chile no cuenta con una entidad pública que ejerza esa función.

Como se ha mencionado, el Consejo para la Transparencia -por mandato de la propia ley de Transparencia y no de la ley de protección a la vida privada- solamente tiene el rol de *"velar por el adecuado cumplimiento de la ley N°19.628, por parte de los órganos de la administración del Estado"*[30]. Por tanto, corresponde al Consejo, ponderar en cada caso cuando prevalece entregar la información pública solicitada y en qué casos denegarla por afectar la vida privada de las personas. Así, el Consejo puede asumir tres posiciones en materia de protección de datos:

1.- Respecto de las bases de datos que se encuentren en poder de entidades públicas, corresponde una función de protección. Sin embargo, el Consejo, en esta hipótesis, no se ha pronunciado respecto de protección de datos cuando no son objeto de un reclamo. Se estudian recomendaciones para tratar justamente este tema.
2.- Respecto de información que se encuentre en poder de la administración del Estado, que pueda afectar derechos de terceros ante una solicitud de acceso (requisito previo), debe ponderar; y
3.- Respecto de las bases de datos que mantienen los privados, no existe un control. Por tanto, quienes se vean afectados solamente pueden ejercer acciones judiciales o administrativas – en algunos casos-, transformándose en vías bastante gravosas para el ciudadano en la protección de sus datos personales.

Relación entre ambos derechos:

La relación de ambas normativas, es que regulan "dos caras de la misma moneda"[31]. Por una parte, la ley de Transparencia viene a desarrollar el ejercicio del derecho de acceso a la información que obra en poder del Estado, que contiene información sobre la mayoría de los ciudadanos del país y, por otra parte, la ley de protección a la vida privada, pone énfasis en el tratamiento de dichos datos cuando son contenidos en bases de datos, procurando que estos no afecten los datos personales de las personas. Según la legislación vigente, no se supone entonces la preponderancia de un derecho por sobre el otro.

Al no existir una entidad de control pública que vele por la debida protección de datos, han sido los Tribunales de Justicia u órganos administrativos (como Superintendencias), que a través de multas han sancionado a empresas que no cumplen con la debida confidencialidad y privacidad de ciertos datos.

Con la creación del Consejo para la Transparencia, como ente llamado a dar publicidad, promoción y fiscalización del derecho de acceso a la información, la legislación ha implantado una facilitación para el ejercicio del derecho, por lo que a

[30] Art. 33, letra "m", Ley 20.285 (LAIP)
[31] 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

priori, pareciese haber una preocupación del legislador en orden a consagrar el ejercicio de este derecho, sin el debido desarrollo de la protección de datos[32].

En los casos en que el Consejo para la Transparencia (CPLT) tiene incumbencia en la protección de los datos personales, se trabaja en base a una solicitud que pudiese o genera una contienda con la administración por un tema de protección de datos, en la que el Consejo resolviendo de un amparo se pronuncia al respecto. Empero, también existen casos en que no hay una contienda con la administración o en que no hay una solicitud, siendo por ejemplo, casos en que se filtra información desde bases de datos que maneja la administración o también de que puede hacer una persona que siente que sus datos han sido traficados. En esos casos, se hace referencia a otro procedimiento distinto para cancelar el registro de sus datos en las bases de acuerdo a la ley 19.628. En estos casos, si hay ponderación, esta no la hace el CPLT, sino que los tribunales u otras entidades administrativas.

En el caso del derecho de acceso a la información, el control se ejerce a través de dos vías: activamente por la presentación de una solicitud de acceso (mal llamada "Transparencia pasiva") o por Transparencia Activa. En forma activa, cualquier persona puede realizar una solicitud de acceso a la información a cualquier entidad pública, con restricción de aquellos que la propia ley se encarga de dejar fuera de este tipo de forma de control. Así, en el caso que la administración no responda una solicitud, se ejerza el derecho de oposición a la entrega de información por parte de un tercero eventualmente afectado por la entrega de la información o el organismo no responda la solicitud, puede ejercer el derecho de amparo ante el Consejo para la Transparencia, que es un organismo público autónomo, que resuelve obligando o negando a hacer entrega de la información. Por otra parte, a través del ejercicio de Transparencia activa, se habilita a cualquier persona para acudir vía reclamo directamente ante el Consejo para la Transparencia, en el caso que cualquiera de los organismos llamados por ley a mantener un registro permanente y actualizado en sus sitios web respecto de ciertas materias, no lo hagan[33].

Al ser derechos de naturaleza antagónica, toda vez que la administración se ve enfrentada a una solicitud que requiere información pública, pero que a la vez contiene información de carácter personal, debe dar cuenta al tercero eventualmente afectado por la entrega de la información, para que ejerza su derecho a oponerse a su entrega, por escrito y fundamentada, pudiendo invocar la causal de reserva del numeral 2 del art. 21 de la ley de Transparencia[34]. En este caso, la administración queda impedida de hacer entrega de la información, sin perjuicio que el solicitante ejerza amparo ante el Consejo para la Transparencia para que resuelva. En este caso, el CPLT deberá ponderar entre sí prima el interés público de dar a conocer la información o prima el interés personal, que impide entregarla. Eventualmente, podría darse el caso que proceda respecto la decisión del Consejo que deniega la entrega de la información, el recurso de ilegalidad que es de competencia de la

[32] Cabe destacar, que actualmente se tramitan en el Congreso Nacional, proyectos que pretenden precisamente ajustar la normativa a parámetros internacionales en materia de protección de datos. Así, por ejemplo, el boletín 6120-07. Disponible en <http://www.camara.cl/pley/pley_detalle.aspx?prmID=6505&prmBL=6120-07>

[33] La información que debe estar publicada en los sitios web, está contenida en el artículo 7 de la 20.285 (LAIP), así como en la Instrucción General N° 4 "Sobre Transparencia Activa" y la N° 5, "Sobre Transparencia Activa para empresas públicas, empresas del Estado y sociedades del Estado".

[34] 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". Numeral 2, del artículo 21 de la ley N° 20.285, de Acceso a la información pública"

Corte de Apelaciones del domicilio del reclamante, por tanto, también existe una eventual ponderación.

Casos prácticos:

A continuación se presentaran casos prácticos en los que el Consejo para la Transparencia ha debido ponderar, frente a una solicitud de acceso a la información, sobre el interés público en revelar la información o la protección de algunos datos de la esfera de la vida privada de las personas respecto de las cuales dice relación la solicitud.

El primer caso tiene que ver con dos solicitudes hechas a una misma entidad[35] (Dirección Nacional del Servicio Civil), sobre la misma materia: postulaciones a cargos de Alta Dirección pública[36]. En una de ellas, él solicitante requiere información sobre su evaluación, como asimismo la de cuya persona fue finalmente fue elegida para el cargo; el otro requirente, solicita la nómina de candidatos seleccionados para proveer el cargo al que postulo. En ambos casos, la reclamada niega la entrega de la información aduciendo principalmente a) Que la tanto la nómina de postulantes, como las evaluaciones que la contienen, tienen el carácter de reservado y confidencial por mandato de la ley N° 19.882; b) Que la entrega de dicha información implicaría un detrimento al sistema de elección de cargos de alta dirección pública; c) Que se afectaría el derecho a la vida privada e intimidad de los postulantes, en la medida que podría afectar su empleabilidad presente y futura. En el mismo sentido, la ley de protección de datos, no permitiría su tratamiento por contener datos sensibles (exámenes psicológicos). El CPLT, conociendo del caso, obligo a la entidad pública a entregar en forma íntegra los datos de uno de los solicitantes (resultados de su postulación, conjuntamente con los de la persona elegida para el cargo, con exclusión de los datos sensibles) y en el otro caso, lo acoge íntegramente, esto es, obliga la entrega de la nómina de candidatos seleccionados para el cargo; En lo que respecta a protección de datos, los fundamentos del CPLT fueron principalmente que aun cuando existen informes que contienen información de carácter personal, el hecho de que se postule a cargos de Alta Dirección Pública es de interés público, por tanto, existe un escrutinio en que la privacidad debe ceder en pos del control social (considera el Consejo, que incluso se beneficiaría el sistema de alta dirección pública); Excluye la entrega de datos de carácter sensible contenidos en los informes.

Sin embargo, lo interesante de este caso es que la Corte de Apelaciones, conociendo del recurso de ilegalidad interpuesto por la reclamada[37], dejo sin efecto ambas resoluciones. Lo anterior, principalmente fundado en que a) el proceso que establece la ley para el nombramiento es confidencial, siendo exigencias ineludibles; b) Que el hecho de tratarse de un procedimiento confidencial, garantiza que no existan consecuencias negativas presentes o futuras, evitando de este modo presiones que afecten el proceso y que afecten la dignidad de los postulantes; c) en el caso de la oposición de terceros, razona en base a la descontextualización que el

[35] Decisiones de amparo A35-09, disponible en: http://www.cplt.cl/data_casos/ftp_casos/A35-09/A35-09_decision_web.pdf y decisión A29-09, disponible en: http://www.cplt.cl/data_casos/ftp_casos/A29-09/A29-09_decision_web.pdf.
[36] Proceso regulado por la Ley N° 19.882
[37] SC de A. 943-2010, con fecha 3 de Septiembre de 2010. Disponible en: http://www.cplt.cl/consejo/site/artic/20100906/asocfile/20100906163335/sentencia_ri_rol943_2010_dnsc.pdf

revelar la información podría traer como consecuencias tanto al postulante (afectando su dignidad) como al examinador (objetividad).

Otro caso, es la decisión del amparo **N°A53-09**[38]**.** Acá, el solicitante presentó amparo al derecho de acceso a la información por haberle sido denegado el acceso a la copia de los expedientes relativos a las multas cursadas en su contra, por la Dirección del Trabajo. No obstante estimar el Consejo que la confidencialidad en este procedimiento de fiscalización sólo rige durante su tramitación, se señaló que se reconoce que cierta parte de la información contenida en los expedientes solicitados por el reclamante podrían contener datos personales de terceros —e incluso sensibles—, que deberían ser protegidos; Hace hincapié en el hecho que no se puede desconocer la naturaleza especial de las denuncias realizadas por los trabajadores ante la Dirección del Trabajo y el riesgo de que su divulgación, así como la de la identidad de los denunciantes o la de los trabajadores que han declarado en un proceso de fiscalización en contra del empleador, afecte su estabilidad en el empleo o los haga víctimas de represalias; Por consiguiente, dispuso que, respecto de aquellos datos personales señalados, cabe entender que la publicidad, comunicación o conocimiento de dicha información puede afectar derechos de terceros —en el caso en análisis de los trabajadores denunciantes o de los que han prestado declaración—, en particular tratándose de la esfera de su vida privada y sus derechos de carácter económico emanados de la relación laboral, configurándose de esta forma y respecto de aquellos datos la causal del artículo 21, numeral 2 de la Ley de Transparencia,

Interesa reflexionar sobre lo que sucede con las bases de datos que son manejadas por privados. La importancia radica – como se apreciará en los siguientes casos- en que no existe una entidad pública dotada de facultades sancionatorias, por lo tanto, los particulares afectados, solamente pueden recurrir por vía judicial o administrativa, lo que hace gravoso la protección de sus datos.

El primer caso se encuentra en relación con el traspaso de datos desde la Institución de Salud Previsional (Isapres) hacia las farmacias, sin el consentimiento de los beneficiarios del sistema. En este caso, la dependiente del recinto, por medio del rut (numero de identificación nacional) de la titular, tuvo conocimiento del padecimiento de una enfermedad que tuvo el cliente, ofreciéndole un producto de menor valor para su tratamiento. El caso termino siendo conocido tanto por la Superintendencia de Isapres, que aplicó una sanción millonaria por la vulneración de confidencialidad y el conocimiento por los Tribunales de justicia.

El otro caso se encuentra en relación con el almacenamiento de datos biométricos para la venta de bonos de atención de salud. La empresa I-med S.A., es la que mantiene la base de datos de los beneficiarios, los que al colocar la huella – según indicaba una pequeña leyenda al costado del lector – autorizan su eventual transmisión a título gratuito a otras instituciones. El tema que hay detrás del caso es que si la persona que se va a atender no compra el bono “en línea” a través de este sistema, debe ir directamente a la Isapre, con lo cual el trámite se hace mucho más engorroso. Tras una denuncia, esta leyenda fue modificada, garantizándose que la información no será dada a conocer a terceros

[38] Este es solo un resumen del caso, expuesto en el documento de trabajo “Estrategias emergentes para el desarrollo de la protección de datos en Chile”. Elaborado por: Jessica Matus, abogada Unidad de Normativa y Regulación; y Alfredo Steinmeyer, abogado Unidad de Promoción y Clientes, ambos del Consejo para la Transparencia. Decisión Disponible en: http://www.cplt.cl/data_casos/ftp_casos/A53-09/A53-09_decision_web.pdf

Jurisprudencia:

A continuación se exponen dos casos en que se ha sopesado el interés público v/s la entrega de datos personales; Detrás de estas resoluciones del CPLT, esta no la ponderación de derechos, sino las razones de interés público que hay detrás. Estas razones, son las que están en evolución en la jurisprudencia, que ha pasado desde una etapa de menor comprensión del ámbito de protección hacía una fase que ha entendido el alcance de estos derechos.

Decisión amparo rol A315-09[39] El 27 de julio de 2009 don Eduardo Hevia Charad requirió al Servicio de Impuestos Internos se le informe el valor, a la fecha de respuesta del órgano, de la totalidad de las variables consideradas en el cálculo de los avalúos de los siguientes bienes: Roles N° 528-003; 528-497; 528-607; 528-617; 528-747; 528-748; 528-837; y 591-1. Asimismo, solicitó se le informe de dichos valores a diciembre de 2005, enero de 2006 y diciembre de 2008.

El organismo contesta invocando causales de datos personales:

d) "Procedencia de la causal de secreto o reserva contemplada en los artículos 21 N° 2 de la Ley de Transparencia, en relación al artículo 19 N° 22, de la Constitución, toda vez que esta última norma dispone que es deber de todos los órganos del Estado abstenerse de realizar actuaciones que alteren el natural equilibrio que debe existir entre los distintos agentes económicos, en la especie, entre los locatarios de un centro comercial. Señala que la pretensión del peticionario apunta a conocer el real costo que tendrían los valores cobrados a los locatarios y dicho dato le permitirá obtener una posición ventajosa respecto de los demás propietarios de locales comerciales. Agrega que conforme al artículo 19 N° 26, el Servicio de Impuestos Internos y este Consejo se encuentra en el imperativo constitucional y legal de evaluar si su actuación puede afectar en su esencia del derecho garantizado"

e) "Que la entrega del detalle de las características catastrales de los bienes raíces de personas naturales y personas jurídicas (en el presente caso los propietarios son personas jurídicas), podrían afectar derechos tales como la seguridad y la vida privada de las primeras y de los representantes de las segundas"

A lo que el Consejo para la Transparencia señalo en los considerando:

"12) Que, sobre el particular, no se advierte una afectación al bien jurídico que se pretende proteger con la reserva de la información solicitada, toda vez que, por una parte, en la actualidad ninguno de los supuestos competidores comerciales posee una posición ventajosa respecto de los demás dado el desconocimiento general de la información sobre las variables y valores para el cálculo de los avalúos y, por otra, si se reconociese el carácter público de la misma, atendida su propia naturaleza, todo competidor podrá acceder a dicha información sin distinción alguna, razón por la cual no cabría sostener la existencia, en ninguno de los dos casos, de dicho tipo de ventajas en el mercado inmobiliario de que se trata. Por lo demás, teniendo presente que la información relativa a los avalúos de las propiedades en consulta es pública, no se reconoce en las variables y valores que permiten su determinación un

[39]Decisión disponible en: http://www.consejotransparencia.cl/data_casos/ftp_casos/A315-09/A315-09_decision_web.pdf

antecedente económico diferenciador en el mercado, que permita al solicitante un posición ventajosa respecto de los demás participes en el comercio."

13) "Que acerca de la afectación del derecho a la vida privada o a la seguridad de las personas, más allá de su invocación general, el servicio reclamado no ha argumentado la forma en que la divulgación de la información solicitada afectaría dichos bienes jurídicos. Al respecto, teniendo presente las variables consideradas para la determinación del avalúo (ubicación, las obras de urbanización, equipamiento del que dispone, clase, calidad, antigüedad, destino, etc.), no se advierte en su divulgación una expectativa probable de afectación a la vida privada o seguridad de las personas"

Por estas y otras razones, el Consejo para la Transparencia acoge el amparo y obliga al servicio a entregar los datos como los solicitó el requirente.

Caso Servicio electoral (Decisión amparo C407-84)[40]: Se solicita la entrega de copia digital del padrón electoral alfabético vigente. El organismo responde señalando que en conformidad a las Leyes N°18.556 y N°18768, dicha entrega procede previo pago asociado que además constituye costo de reproducción a la luz de la Ley N°20.285 y que asciende a $ 21.698.799. Frente a esta respuesta requirente formula solicitud de amparo ante el Consejo para la Transparencia indicando que el costo de reproducción es inferior y comprende solo el almacenamiento de la información en un CD virgen. El padrón electoral contiene todos los datos de las personas que se han inscrito para sufragar en cargos de elección popular. Contiene el nombre, rut, domicilio, fecha de nacimiento, profesión y oficio, situación de analfabetismo o discapacidad. El pago de los costos de reproducción, que alega el servicio, es porque históricamente se vendía a empresas privadas o particulares. El solicitante, estima que como es información que obra en poder del Estado y se encuentra en una fuente de datos digital (aparte de los libros en los que queda registro materialmente), es pública y, por tanto, solamente correspondería pagar los costos de reproducción, que equivale al precio de un CD. En este caso, finalmente el Servicio electoral debió hacer entrega del padrón electoral con un costo no superior a los $200.- pesos. El entonces Presidente del Consejo, Don Juan Pablo Olmedo, emitió voto de disidencia en el sentido de:

"…y está por acoger sólo parcialmente el presente amparo, eliminando de la copia del padrón a entregar al solicitante la profesión, fecha de nacimiento, domicilio, número de cédula de identidad e indicación de discapacidad (no vidente, analfabeto) de las personas inscritas en los Registros…"

Continúa en el número 6 y 7 del Voto disidente:

6) "Que, en cambio, los demás datos personales contenidos no tienen mayor interés en materia electoral. Ni la profesión, ni la fecha de nacimiento, ni el domicilio, ni el número de la cédula de identidad resultan indispensables para controlar estos procesos. En cambio, su tráfico indiscriminado —atendido el bajo costo que tiene la reproducción de esta información en soporte electrónico, según el criterio adoptado por esta decisión y que el suscrito comparte— arriesga severamente el derecho a la intimidad de las personas, pues implica que cualquiera podría tener acceso a esos

[40] Disponible en: <http://www.consejotransparencia.cl/data_casos/ftp_casos/C407-09/C407-09_decision_web.pdf>

datos, en circunstancias que el SERVEL no está autorizado a tratarlos informáticamente"

7) "Que resultaría más grave aún entregar la indicación de discapacidad (no vidente, analfabeto) pues esta información, según la Ley Nº 19.628, es de carácter sensible, lo que impide tratarla salvo en los precisos casos que señala su art. 10 y que, en este caso, no concurren."

Rol de la Sociedad Civil:

En relación a las iniciativas de la sociedad civil para promover la protección de datos es conveniente destacar la labor que la Fundación Proacceso ha desarrollado. En ese sentido, se pueden encontrar dos importantes estudios en materia protección de datos:

- **"Nivel de cumplimiento de la Ley 19.628 Sobre la Protección de la Vida Privada o Protección de Datos de Carácter Personal"** (28 de Diciembre de 2009)[41]; Fue un estudio aplicado a los ministerios de Vivienda y Urbanismo, Trabajo, Planificación Salud, Educación y el Servicio Nacional de la Mujer dio a conocer que la protección los derechos personales de los ciudadanos aún es altamente vulnerada. Las materias consultadas a los servicios, programas o y/o beneficios decían relación con materias específicos ligados a la ley de protección a la vida privada, a saber: existencia de bases de datos personales y su registro obligatorio en las bases del Registro Civil e Identificación, el nivel de seguridad con que éstas son manejadas por los jefes de los servicios y por ultimo justificación de la existencia de tales bases de datos. Como primer distinción, se diferenció entre aquellas que respuestas que fueron satisfactorias (30%) de las que no lo fueron (70%). De éstas últimas, 49% responde formalmente la solicitud de acceso, pero no las preguntas de fondo que les fueron consultadas. De los requeridos y que respondieron satisfactoriamente, se permitió identificar que la mayoría de estos cuentan con una base de datos personales (78%), pero tan solo un 13% cumple con la obligación de registro en el Registro Civil y de Identificación; A la vez, las medidas de seguridad que deben tomar los jefes de los servicios, son dispersas, por cuanto queda a criterio de cada división, por lo tanto, no existe un estándar mínimo de protección legal. Para terminar, solo un13% informa poseer una división encargada de la protección de las bases de datos, por tanto, no existe un despliegue especial en estructura orgánica del servicio para el tratamiento de datos personales (Ley N° 19.628).

- **"Protección de datos personales en el sector público"[42] (**11 de Julio de 2011). El estudio busca medir el tratamiento que el servicio público le entrega a las bases de datos personales y si sus instituciones cumplen con la Ley Nº 19.628, sobre la protección de aquella información. Se hicieron 166 solicitudes de información a Servicios y Programas dependientes de los distintos Ministerios, el Consejo Nacional de la Cultura y las Artes y el

[41] Disponible en: http://www.proacceso.cl/contenido_general/nivel_de_cumplimiento_de_la_ley_19_628_0#attachments
[42] Disponible en: http://www.proacceso.cl/noticia/estudio_de_pro_acceso_revela_deficiencias_en_la_administraci_n_de_bases_de_datos_personales . Versión en Inglés: http://www.proacceso.cl/contenido_general/study_pro_acceso_reveals_deficiencies_management_public_service_databases.

Servicio Nacional de la Mujer. Los principales temas a identificar fueron si las instituciones cuentan con base de datos personales, como lo establece la Ley Nº 19.628**,** y de contar con una o más bases, constatar si disponen de sistemas de seguridad que aseguren la privacidad de los datos. A la vez, se pidió que las instituciones consultadas justifiquen la posesión de dichas bases declarando el fin de éstas. Junto a esto, se revela si las entidades han hecho transferencia de los datos personales, tanto a entes públicos como privados, durante el último año. Comparativamente con el estudio del año 2009, Mientras en 2009 sólo el 30%de las164 instituciones consultadas respondió a la solicitud, en 2010, lo hizo el 70% de las 83 entidades requeridas. Esto, sin duda, representa un avance en materia de transparencia y acceso a la información pública. De las 50 instituciones que respondieron en 2009, solo un 78% declaro tener una o más bases de datos personales. En tanto, las 58 entidades que respondieron la solicitud en 2010 aseguraron tener bases de datos personales. Por otro lado, solo un 13% de las instituciones que dijeron tener base de datos en 2009, cumplió con su deber de registro en el Registro Civil, tal como lo establece la ley 19.628. En 2010, la cantidad de entidades que cumplieron con esta obligación aumento a un 52%. Un cifra que, sin embargo, sigue siendo baja. Finalmente, en 2009, solo un 13% de las entidades afirmo contar con un departamento o división encargado de velar por el tratamiento de sus bases de datos. El estudio del año 2010, establece que para ese año la cifra aumento a un 81%.

1.5. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

A) Fundación para la Libertad de Prensa (FLIP)
Director Ejecutivo: Andrés Morales

Acceso a la Información Pública:

En Colombia, actualmente, no existe ninguna norma que regule el derecho de acceso a la información pública. El desarrollo del derecho se ha hecho principalmente a partir de sentencias de la Corte Constitucional. Sin embargo, se encuentra normas dispersas que lo reglamentan parcialmente como la Ley 594 de 2000, según la cual, las entidades están obligadas a administrar y custodiar su documentación en archivos públicos, la Ley 80 de 1993, en la cual se incluye la transparencia como principio de contratación estatal, o la Ley 1266 de 2008, de *habeas data*, entre otras.

Actualmente existen dos normas que regulan procedimientos para solicitar información, la ley 57 de 1985 y el Código Contencioso Administrativo, que será remplazado por uno nuevo a partir del 2 de julio de 2012.

La Ley 57 de 1985, que se refiere al deber de divulgación de los actos y decisiones de las autoridades públicas y contiene las siguientes disposiciones:

- Se establece un tiempo límite de reserva de 30 años y se interpone que el término para responder solicitudes de información es de diez días hábiles.
- En temas de transparencia activa, las autoridades están obligadas a tener en sitios de fácil acceso al público información relacionada con su labor: las normas que dan origen a la institución, su estructura, organigrama y trámites de su competencia.
- Se establece un recurso de insistencia para controvertir las decisiones de las autoridades de negar información cuando se alega una reserva. En aquellos casos que se niegue la información sin aducir que existe una reserva legal, aplicará la acción de tutela, mecanismo constitucional de protección de derechos fundamentales.

El Código Contencioso Administrativo reglamenta el derecho de petición, que consiste en la facultad que tiene todo ciudadano de presentar peticiones respetuosas a las autoridades públicas y que es uno de los principales mecanismos de acceso a la información que existen actualmente. Según esta norma, las solicitudes de información se deben de resolver en el plazo de 10 días hábiles.

La ley 1437 de 2011 crea un nuevo Código Contencioso Administrativo que regirá desde el 2 de julio de 2012. En relación al derecho de acceso a la información, el alcance de esta norma es el siguiente:

- las peticiones de documentos se deberán responder dentro de diez días hábiles después de ser recibidas. En caso de no darse respuesta, la entidad deberá entregar la información en el plazo de 3 días.
- Se establece como causales de reserva en protección de secretos industriales y comerciales, de la defensa y seguridad nacional, del secreto profesional, la privacidad e intimidad de las personas, y los relacionados con condiciones financieras y operaciones de crédito público de la nación.
- Se establecen obligaciones de publicación proactiva de información sobre procedimientos administrativos, regulaciones, y actos administrativos de

carácter general en el sitio de atención al público y en la página electrónica de las entidades.
- Se permite la presentación de solicitudes a organizaciones privadas. Esto también se podrá realizar ante a personas naturales cuando el solicitante se encuentre en una situación de vulnerabilidad frente al requerido.

Actualmente no existe un órgano de control dedicado exclusivamente al derecho de acceso a la información. Tanto el recurso de insistencia como la acción de tutela deben ser resueltos por jueces o magistrados (la competencia varía dependiendo de cada caso).

Protección de Datos Personales:

En Colombia existe una ley que regula el derecho al *habeas data*, es la ley 1266 de 2008, que aplica en el ámbito comercial y financiero. Actualmente hay una norma que sería complementaria de la que actualmente se encuentra en proceso de control previo en la Corte Constitucional, es el Proyecto de ley estatutaria No.184 de 2010 Senado, 046 de 2010 de Cámara.

Los alcances y características de la ley 1266 de 2008

Objeto: se contempla lo relacionado a la recolección, tratamiento y circulación de datos personales y el derecho a la información relacionada con el ámbito financiero, crediticio, comercial, de servicios y la proveniente de otros países.
Ámbito de aplicación: La ley aplica a datos de información privada que estén en bancos de datos públicos y privados; se excluyen, entre otros, los datos relacionados con la inteligencia del Estado y aquellos que se recolectan dentro de ámbitos personales y domésticos.
Sobre este punto es importante mencionar que puede llegar a considerarse que existe un traslado de cargas públicas a entidades privadas, especialmente si se tiene en cuenta que puede haber personas naturales y jurídicas que no están en capacidad de cumplir todas las obligaciones que se establecen en la ley y que utilizan la información en ámbitos distintos de los personales y los domésticos, como por ejemplo las bases de datos que son realizadas con fines académicos.
Definición de dato personal: Con respecto a la definición de dato personal, se tiene que es información que se relaciona con una o más personas, ya sean determinadas o determinables, naturales o jurídicas. Los datos de los que trata la ley se presumen como personales. La clasificación es de públicos, privados y semiprivados. Los datos públicos son aquellos calificados específicamente como tales según los mandatos de la Constitución y la ley(se da como ejemplo los documentos públicos, sentencias ejecutoriadas y lo relativo al estado civil de las personas) y aquellos que no sean ni privados ni semiprivados; los primeros son aquellos sin naturaleza íntima, reservada, ni pública y que pueden interesar al titular y a algunos grupos de personas o a la sociedad en general, como por ejemplo los datos crediticios y financieros; los segundos son aquellos que tienen una naturaleza íntima o reservada que sólo es relevante para el titular.
Principios rectores: Para la administración de datos se consideran como principios los de veracidad o calidad de los registros de datos, de finalidad, de circulación restringida, de temporalidad de la información, de interpretación integral de derechos constitucionales, de seguridad, y de confidencialidad.
Ámbito procedimental: Se establecen procedimientos para hacer consultas y reclamos sobre la información de la cual uno es titular; dichos reclamos podrán

referirse a la defensa de otros derechos distintos del *habeas data* y podrán hacerse a cualquier banco de datos, sea público a privado,.

Sanciones: Se imponen sanciones desde multa hasta el cierre definitivo (dependiendo de cada caso) para aquellas fuentes, operadores y usuarios de información que incumplimiento de las obligaciones y procedimientos que se establecen en la ley, sus normas reglamentarias y las órdenes e instrucciones impartidas por las Superintendencias con respecto al tratamiento de datos personales.

Las personas que tienen relación con los datos personales son los titulares, las fuentes, los operadores y los titulares de información. Los titulares, son aquellas personas naturales o jurídicas a las que se refiere la información. Las fuentes son personas, entidades u organizaciones que reciben o conocen datos personales de los titulares para enviarlos a los operadores, que son las personas que recibe al recibir la información, la administran y ponen en conocimiento de los usuarios. Estos últimos son aquellas personas que están autorizados a recibir la información.

Deberes de los operadores de información: Los deberes de operadores de información son, entre otros, los de garantizar que el titular pueda ejercer su derecho de habeas data y de petición para poder conocer y solicitar la actualización o corrección de su información. Velar por una recolección, tratamiento y circulación de datos que respete los derechos de los titulares, para estos es importante tener en cuenta que se debe adoptar un manual de políticas y procedimientos para tramitar de manera efectiva las consultas y reclamos que hagan los titulares.

Asimismo, está la obligación de suministrar la información a las personas autorizadas. Para esto es importante tener en cuenta que en algunos casos la información que se administra requiere que el operador solicite certificación a la fuente de la existencia de autorización del titular.

Con respecto a la administración de los registros, los operadores deben conservarlos de manera que no se alteren, deterioren o tengan un uso que es fraudulento o sin autorización. Además, deberá hacerse una actualización y rectificación periódica de las novedades reportadas por las fuentes. Cuando haya una solicitud de actualización o rectificación, deberá indicarse en el registro.

Las obligaciones de las fuentes de información: entre otras, son las de Garantizar que la información suministrada a los operadores y usuarios sea veraz, completa, exacta, actualizada y comprobable.

La fuente deberá reportar al operador las novedades de los datos suministrados. En la misma medida, se deberá rectificar e informar aquella información que sea incorrecta. Para esto, se deben diseñar e implementar mecanismos eficaces.

Dado que hay información que requiere autorización de los titulares, esta se deberá solicitar cuando sea necesario. Dicha autorización deberá ser certificada al operador de manera semestral, para lo cual es obligatorio conservar copia o evidencia de la misma. Cuando se presenten solicitudes de información y actualización, se deberá informar al operador.

Las Obligaciones de los usuarios: aparte de lo que establezca la Constitución y la ley, los usuarios deben guardar reserva sobre la información que se les suministra, la cual también deberá ser conservada de manera que no se deteriore, pierda, altere o use fraudulentamente. Frente a los titulares, es importante destacar que se les debe comunicar, cuando lo soliciten, sobre el uso que se da a la información.

La información de datos personales se puede suministrar, sin perjuicio de otros casos que establezca la ley, a:

a. A los titulares, a las personas autorizadas por ellos, y a los causahabientes.
b. A los usuarios de la información.
c. A cualquier autoridad judicial mediante orden judicial.

d. A las entidades del poder ejecutivo en el cumplimiento de sus funciones, caso en el cual se someten a las obligaciones de los demás usuarios.
e. A los órganos de control que requieran la información para el desarrollo de una investigación.
f. A otros operadores de datos, con autorización del titular o cuando el destinatario tengan la misma finalidad o una relacionada a la del que la suministra.

El control del derecho de habeas data en la actualidad jurídica colombiana

Actualmente no existe una entidad de control que se dedique de manera exclusiva e integral a la defensa del derecho de habeas data. En lo que se refiere a temas crediticios, financieros y comerciales, la competencia recae sobre la Superintendencia de Industria y Comercio en su área de protección al consumidor y en algunos casos, recae a la Superintendencia Financiera. Para los demás aspectos del derecho de habeas data, el mecanismo de defensa es el de la acción de tutela, por lo que la entidad de control sería la misma rama judicial. Estas entidades son organismos técnicos adscritos al Ministerio de Comercio, Industria y Turismo y al de Hacienda y Crédito Público, respectivamente, con personería jurídica, autonomía administrativa y financiera y patrimonio propio.
Las dos superintendencias cumplen funciones de vigilancia y sancionatorias dentro de las cuales se identifican las siguientes como las más importantes.

Funciones de vigilancia[43]
Dentro de las funciones de vigilancia tenemos que las superintendencias pueden impartir instrucciones y órdenes sobre cómo deben cumplirse los lineamientos de la ley; Velar porque los operadores y fuentes tengan un sistema de seguridad y cumplan con condiciones técnicas para que haya una correcta salvaguarda y actualización de los registros.
Las superintendencias podrán ordenar que se realicen auditorías externas para verificar que haya un efectivo cumplimiento de la ley. Asimismo, podrán ordenar de oficio o a petición de parte la corrección actualización de datos que se necesiten.

Funciones sancionatorias[44]**:**
Las Superintendencias con funciones de ente de control tendrán la función de Iniciar de oficio o a petición de parte investigaciones administrativas contra operadores, fuentes y usuarios de información para interponer sanciones en caso de ser necesario.
Con respecto a las sanciones que pueden interponer las superintendencias a los operadores, fuentes y usuarios, están las de imponer multas, suspensión de actividades y cierre o clausura tanto temporal como definitiva.

Proyecto de ley estatutaria No.184 de 2010:

El Proyecto de ley estatutaria No.184 de 2010 Senado, 046 de 2010, que se encuentra actualmente en control previo por parte de la corte constitucional tiene las siguientes características:

[43] Ley 1266 de 2008
[44] Idem

Ámbito de aplicación: Su ámbito de aplicación es en relación con la información que esté en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, excluyendo las bases de datos o archivos que se mantienen en el ámbito personal o doméstico; a aquellas que tengan como finalidad la seguridad y defensa nacional, y la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; las que tengan como fin y contengan información de inteligencia y contrainteligencia; las bases de datos y archivos periodísticos y editoriales; las reguladas por la Ley 1266 de 2008; las reguladas por la Ley 79 de 1993, de censos de población y vivienda. A pesar de esto, los principios de protección de datos aplicarán para las bases de datos excluidas.
Categorías de información: Se establece la categoría de datos sensibles, los cuales son aquellos que afecten la intimidad de su titular o que si son usados de manera indebida pueden causar discriminación, tales como el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición; y los relativos a salud, vida sexual y datos biométricos. El tratamiento de estos datos es prohibido salvo en casos que haya autorización de su titular o se actúe en defensa de sus intereses, entre otros, o que sean datos de naturaleza pública como por ejemplo los relacionados con el registro civil de las personas.
Reglas sobre el suministro de información: Se establece como regla para el suministro de información que esta sea "de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos."
Creación de autoridad encargada: Se crea una autoridad de protección de datos que estará a cargo de la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de datos Personales, sus funciones son las mismas que se establecen en la ley 1266 de 2008.

La relación entre ambos derechos.

La garantía del derecho a la información y el habeas data en Colombia:
De acuerdo con lo anterior, pese a que ambos derechos cuentan con protección constitucional por ser considerados derechos fundamentales, podría considerarse que en la práctica actual, el derecho de habeas data tiene preponderancia sobre el derecho de acceso a la información en la legislación colombiana. Esto bajo el entendido que no hay una norma que desarrolle integralmente el derecho de acceso a la información, salvo las mencionadas anteriormente, que son normas previas a la Constitución Colombiana de 1991, que están pensadas bajo estándares constitucionales distintos, y que junto a otras normas posteriores, abarcan el tema de manera tangencial.

En contraposición está el derecho de habeas data, que actualmente cuenta con una regulación parcial en los temas crediticios, financieros y comerciales y con una regulación complementaria que actualmente está en proceso de control previo por parte de la Corte Constitucional; cabe resaltar que estas normativas fueron tramitadas como leyes estatutarias, las de mayor jerarquía dentro del ordenamiento jurídico colombiano.

Colisión de derechos:
Los mecanismos que se usan para dirimir los conflictos entre el derecho de habeas data y el derecho al acceso a la información son dos: el primero es el recurso de insistencia, que se encuentra consagrado en el artículo 21 de la Ley 57 de 1985; su aplicación solo se puede dar cuando el funcionario que niega la información alega que esta es reservada, en este caso, por ser información reservada en razones del habeas data, caso en el cual si el ciudadano que solicita información no comparte la decisión, puede insistir en su solicitud para que el Tribunal de lo Contencioso Administrativo defina si se puede entregar la información. A pesar de esto, existe el procedimiento de la acción de tutela, que es una acción constitucional mediante la cual se protegen derechos fundamentales, aplica en casos como que no haya respuesta a la solicitud o esta sea incompleta o evasiva o no sea de fondo, se soliciten trámites adicionales injustificados o se soliciten cobros excesivos por la información. [45]

Es importante resaltar que la corte constitucional ha establecido que cuando existan conflictos entre derechos fundamentales, se debe hacer un test de proporcionalidad, de acuerdo al cual "el operador jurídico no sólo debe valorar que una norma de rango legal autorice la reserva del documento, sino cuáles derechos, principios y valores constitucionales están afectados con la restricción, ya que en algunas ocasiones deberán prevalecer los derechos, valores y principios que inspiran la confidencialidad de la información, y en otros, los que se le oponen." [46]

Casos Prácticos

A continuación se mencionan litigios estratégicos promovidos por la FLIP en el tema.

a. Consejo de Redacción logra acceder a base de datos personales

El 8 de noviembre de 2010, Consejo de Redacción, una organización colombiana de periodistas que tiene como misión promover el periodismo de investigación hizo una solicitud de información a la Junta Central de Contadores con el fin de obtener la "lista de todas las personas que han obtenido el título profesional de contador público en Colombia indicando de cada una su nombre completo, cédula, número y estado de la tarjeta profesional, universidad y año en que se graduó".

Dicha solicitud fue negada por la entidad, argumentando que en lo pedido "existe información amparada por el derecho fundamental de la intimidad previsto en el artículo 15 de la Constitución Política, que requiere de autorización de su titular para suministrarla a terceros."

De acuerdo a la respuesta dada por la Junta Central de Contadores, se procedió a realizar el recurso de insistencia, alegando que los datos personales son objeto de reserva cuando se refieren a aspectos exclusivos y propios de una persona natural y constituyen "datos sensibles", es decir, aspectos como la dignidad, intimidad y libertad, que incluye datos referidos a la inclinación sexual, ideología y hábitos. En esta situación no se estaba solicitando datos sensibles y por lo tanto, la información pedida no se encuentra cobijada por el derecho a la intimidad.

[45] Corte Constitucional, sentencias T-473 de 1992, T-12 de 1992, T-464 de 1991, T-424 de 1998; Consejo de Estado, sentencia del 29 de enero de 2010, Rad: 25000-23-31-000-2009-01566-01.
[46] Corte Constitucional, Sentencia T-928 de 2004.

El recurso de Insistencia fue remitido al Tribunal Administrativo de Cundinamarca, el cual resolvió que la información debería ser entregada al solicitante.

Este caso es importante porque sirve para delimitar casos en que los datos personales en manos de un operador pueden ser accedidos por personas distintas a los usuarios y su titular cuando estos son información pública y no implican 'datos sensibles'.

b. Periodista amenazada usa mecanismos judiciales para acceder a información sobre ella

Una periodista Colombiana había sido objeto de amenazas y de un atentado, por lo que se vio obligada a salir de la zona en la cual vivía y trabajaba. Su caso fue remitido al Ministerio del Interior y de Justicia, donde se estudian estos casos a través del Comité de Reglamentación y Evaluación del Riesgo (CRER) para periodistas, encargado de determinar las medidas de protección para los periodistas en peligro.

En estos casos, la Policía Nacional debe hacer un estudio que determine el nivel de riesgo de la persona amenazada. Al final, la entidad da una calificación de 'ordinario' o 'extraordinario'. Pero no da a conocer las razones que motivan la decisión.

En este caso, se determinó que la periodista se encontraba en un nivel de riesgo 'ordinario', el cual, según la Policía Nacional es igual "al que están sometidas todas las personas, en igualdad de condiciones, por el hecho de pertenecer a una determinada sociedad". Esta decisión conllevó que se asignaran unas medidas de protección que no eran satisfactorias para la periodista, quien consideraba encontrarse en una situación de riesgo 'extraordinario', es decir "aquél que las personas no están jurídicamente obligadas a soportar y conlleva el derecho de recibir del Estado la protección especial por parte de sus autoridades".

La periodista solicitó a la Policía una copia del estudio de riesgo para poder controvertirlo. La información fue negada. Los argumentos se limitaban a mencionar el artículo 20 de la Ley 57 de 1985 y el artículo 27 de la Ley 594 de 2000, los cuales solo se refieren a que el acceso a la información pública no es un derecho absoluto y a que los funcionarios de los archivos públicos deben respetar los derechos a la intimidad, la honra y el buen nombre de las personas. Por otra parte, se citaron dos sentencias de la Corte Constitucional: la T-525 de 1992 y la T-444 de 1992, las cuales no determinan ningún tipo de reserva para estos casos; la última de estas, establece que el habeas data "implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos […] Lo importante es que las personas no pierdan el control sobre la propia información, así como sobre su uso".

Dado que ninguna de las leyes o sentencias mencionadas por La Policía Nacional establece algún tipo de reserva, y que además se está negando a una persona a acceder a información sobre sí misma, se considera que hay una vulneración tanto de los derechos de habeas data, como de acceso a la información. Por esta razón, se interpuso un recurso de insistencia contra la decisión, el cual fue resuelto por el Tribunal Contencioso Administrativo del Valle del Cauca el 30 de julio de 2010. La decisión del Tribunal fue que la información debía ser entregada a la periodista por ser información relacionada con ella y con su situación de riesgo.

Este caso es importante porque demuestra que los derechos de acceso a la información y de habeas data pueden estar en armonía. Especialmente si se tiene en cuenta que el mecanismo judicial que fue utilizado es aquel que se usa normalmente para controvertir las negativas al acceso a la información. Además, el resultado fue significativo para la FLIP en la medida que antes de estos hechos, no se había podido conocer las motivaciones contenidas en los análisis de estudio de riesgo de periodistas.

Jurisprudencia

En cuanto a la jurisprudencia actual que interpreta la implementación del derecho a habeas data en Colombia, se puede mencionar la Sentencia T-559/07[47] de la Corte Constitucional sobre el derecho de acceso a la información relacionada con datos personales propios.

Marlenis Cárdenas, junto a otros ciudadanos, realizó una solicitud de información a la oficina territorial en Cesar, Agencia Presidencial para la Acción Social y la Cooperación Internacional-Acción Social. Simultáneamente, el señor Luis Aníbal Pacheco Sanguino también radicó una petición en la misma oficina. La intención de los solicitantes era que se les certificara su condición de desplazados por la violencia. Esto para poder aportar dicho documento como requisito para vincularse a una asociación de desplazados.
Acción Social contestó la solicitud de información negando la entrega de lo solicitado argumentando que la información es confidencial y no puede ser entregada por razones de seguridad del desplazado. Por esta razón, los solicitantes decidieron interponer una acción de tutela por vulneración de sus derechos fundamentales de petición y de asociación.

La acción de tutela fue denegada en primera instancia por el Juzgado de Menores de Valledupar. Su argumento se basaba en que el derecho de petición fue contestado por la entidad de manera oportuna. El Tribunal Superior del Distrito Judicial de Valledupar, en segunda instancia se confirmó la decisión. Esta sentencia fue seleccionada para ser revisada por la Corte Constitucional, la cual decidió revocar los fallos de primera y segunda instancia por considerar que hubo una vulneración del derecho de petición, habeas data y asociación.

"En efecto, si bien para la Corte, es claro que la confidencialidad de la información contenida en el Registro Único de Población Desplazada estipulada en el artículo 9° del Decreto 2132 de 2003 que modificó el inciso 2° del artículo 15 del Decreto 2569 de 2000, ha sido prevista con el fin de proteger el derecho a la vida, a la intimidad, a la honra y los bienes de los inscritos, esta confidencialidad, de conformidad con las consideraciones expuestas en el punto 4 de esta providencia, no puede en manera alguna desconocer la facultad que tienen las personas de conocer la información que se relacione con ella misma y que se encuentre recopilada en una base de datos, máxime si de tal información depende el goce efectivo de otros derechos de orden constitucional como lo es el de la libre asociación contemplado en el artículo 38 de la C.P."

[47] http://www.flip.org.co/alert_display/3/2319.html

Rol de la Sociedad Civil

Incidencia en la política pública frente al derecho de habeas data.

En Colombia, existe el observatorio de la protección de datos Personales Habeasdata.org.co, el cual forma parte de la organización internacional HABEASDATA.ORG. Es un espacio vinculado directamente con el Grupo de Estudios en internet Comercio electrónico, Telecomunicaciones e Informática-GECTI y el Observatorio Constitucional de la Facultad de Derecho de la Universidad de los Andes. Es un espacio académico en el cual se hace observación y reflexión sobre la protección de datos personales en el país. Su postura es la de que "cada colombiano (a) debe ser consciente de los riesgos y efectos que implica el tratamiento indebido de su información." Dentro de las acciones que llevan a cabo hacen documentación de normas, jurisprudencia, artículos, columnas de opinión y noticias referentes al protección de datos personales en Colombia.

En abril de 2010 presentaron una intervención ciudadana para el control previo que la Corte Constitucional está haciendo al proyecto de ley estatutaria No.184 de 2010 Senado, 046 de 2010 En esta intervención, el organismo considera que la normatividad es acorde a la Constitución Colombiana, pero adolece de una omisión legislativa con respecto a las obligaciones y responsabilidades de los usuarios de los datos personales.

B) Transparencia por Colombia
Directora Ejecutiva: Elisabeth Ungar Bleier
Directora del Área de Sector Público: Marcela Restrepo Hung

Acceso a la Información Pública

En Colombia no existe una ley que reconozca y garantice el derecho de acceso a información pública de forma autónoma. Existe un reconocimiento constitucional de manera directa del acceso a la información pública en los siguientes artículos:

- Artículo 74: *Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley,*
- *Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.*
- *Artículo 23. Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales*
- *Artículo 78: La ley regulará el control de calidad de bienes y servicios ofrecidos y prestados a la comunidad, así como la información que debe suministrarse al público en su comercialización…*
- *Artículo 93: contempla que los tratados internacionales que suscriba Colombia sobre la materia, pertenecen al bloque de constitucionalidad o de normas constitucionales específicas*[48].

Las normas que han desarrollado del derecho al acceso a documentos públicos en Colombia son anteriores a la actual Constitución Política de 1991. En principio es la Ley 57 de 1985, por la cual se ordena la publicidad de los actos y documentos oficiales. Hay una serie de normas posteriores que tratan el acceso a información pública en diferentes ámbitos y materias[49].

Como se enunció anteriormente existe un reconocimiento constitucional pero hay una gran dispersión normativa que regula el derecho de acceso a información pública. Hay disposiciones sobre el derecho de petición en interés general y particular, el derecho de acceso a la información, de acceso a documentos públicos, las reservas o excepciones al acceso, el deber de publicación de información y las sanciones por el incumplimiento. El derecho de petición, le ha brindado su cauce procesal pero esto ha generado efectos colaterales no tan beneficiosos para la libertad informativa. Al derecho de acceso a la información no se le ha permitido tener un desarrollo autónomo. Y mientras no haya un desarrollo legislativo autónomo, acorde con los estándares internacionales, no contará el Estado colombiano con los requisitos necesarios para garantizar el ejercicio de este derecho

[48] http://www.bibliotecasvirtuales.com/biblioteca/constituciones/Colombiana/index.asp
[49] Ver Anexo 1. Normatividad en Acceso a Información Pública: https://docs.google.com/document/d/1SCJ3ArYI-cxEs4Z2XXJZIpCPhXkdhHL3HGO3Es0o2is/edit?hl=en_US

humano independiente[50].

Aunque hay un reconocimiento de este derecho en la constitución de 1991, las normas específicas sobre acceso a información existentes fueron creadas hace más de 30 años. La actual Constitución Política de 1991 reivindica el protagonismo de la persona y sus derechos, subordinando todos los aspectos del poder público al servicio de esta concepción. Los derechos y deberes consagrados en el ordenamiento constitucional reivindican el protagonismo del individuo y su participación en la cosa pública. En este marco, el derecho de acceso a la información consagrado en la normativa legislativa previa no es integral.

Estas son parte de las motivaciones para buscar la sanción de una la ley estatutaria de acceso a la información pública en Colombia, además porque una ley estatutaria va a estar dotada de una jerarquía superior que otras normas y éstas tienen que ser interpretadas de conformidad a esta.

En Colombia no existe un órgano rector que garantice el acceso a información pública, la garantía se resuelve por la jurisdicción de lo Contencioso-Administrativo o por acción de tutela. Actualmente, el código contencioso administrativo consagró el recurso de insistencia que es la continuidad de un mecanismo existente desde la ley 57 de 1985 (art. 21) y con el cual se mantiene el conocimiento de rechazos al acceso a información por motivo de reserva en la jurisdicción de lo contencioso administrativo. Los rechazos por otros motivos serían entonces objeto de la acción de tutela para hacer efectivo el cumplimiento de una ley o un acto administrativo, cuando sus derechos fundamentales han sido vulnerados o amenazados.

La dificultad mayúscula que se presenta en la práctica con el recurso de insistencia consiste en que el funcionario que ha alegado la reserva es el único que puede acudir ante un juez administrativo para solicitar su pronunciamiento. El ciudadano, que espera la resolución de su caso, depende de la actuación administrativa y no cuenta con ningún mecanismo para acudir directamente ante al juez. De esta manera, como ha sido corroborado por varios solicitantes de acceso a la información en la práctica, se hace ineficaz la posibilidad del ciudadano de insistir y el principio de recurrir, pues con demasiada frecuencia el funcionario no envía el expediente a la justicia[51].

Por las falencias en la garantía del derecho de acceso a información pública se hace necesario en Colombia la creación de una instancia encargada de regular y controlar el derecho. Precisamente una de las propuestas del proyecto de ley formulado por la Corporación Transparencia por Colombia y el Centro de Estudios de Derecho, Justicia y Sociedad-Dejusticia, es crear la Delegada de Información en la Procuraduría General de la Nación que tendría capacidad investigadora y sancionatoria, para que sea garante del derecho de acceso a la información.[52]

Protección de Datos Personales

[50] CORPORACIÓN TRANSPARENCIA POR COLOMBIA y DEJUSTICIA. Documento Interno Exposición de Motivos propuesta Proyecto de Ley Estatutaria de Acceso a la Información. Bogotá, septiembre 2010. Página 9.
[51] CORPORACIÓN TRANSPARENCIA POR COLOMBIA y DEJUSTICIA. Comentarios En Perspectiva Del Derecho De Acceso A La Información. Bogotá, Marzo de 2011
[52] CORPORACIÓN TRANSPARENCIA POR COLOMBIA y DEJUSTICIA. Documento Interno Exposición de Motivos propuesta Proyecto de Ley Estatutaria de Acceso a la Información. Capítulo IV Delegada de Información. Bogotá, septiembre 2010. Página 14.

En Colombia no ha sido aprobada una ley estatutaria que regule de manera integral la protección de datos en general. Actualmente "*muy pocas normas aluden al habeas data*[53] *y hacen referencia a los datos personales*[54] *en general. Todas las demás disposiciones*[55] *hacen referencia marginal a pocos temas sobre la materia. Se trata de regulaciones sectoriales que referencialmente mencionan ciertos aspectos en torno a determinados datos personales*"[56].

En el marco legal colombiano la protección de datos personales tiene reconocimiento constitucional en el artículo 15 de la Constitución de 1991:

> "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en 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. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley"

Existe una ley estatutaria 1266 de 2008 que se regula el manejo de la información contenida particularmente en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Dicha ley fue robustecida por medio de la Ley 1273 de 2009 que adicionó al Código Penal como nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Esta última se centra en los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, y los atentados informáticos.

Recientemente se discutió en el congreso el proyecto de ley 046 de 2010 Cámara, 184 de 2010 Senado, que tiene por objeto desarrollar el derecho constitucional que tienen todas personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a las que se refiere el artículo 15 de la Constitución Política. Fue radicado el mes de agosto de 2010, después de los cuatro debates en el Congreso y con la aprobación del texto de conciliación en Senado y Cámara es aprobado el mes de diciembre de 2010. En este momento se encuentra en revisión de la Corte Constitucional, por ser una ley estatutaria tiene que pasar por la revisión previa por parte de la Corte. Si la Corte estima que el proyecto es constitucional, será remitido por el Presidente de la Corte al Presidente de la República para que lo sancione. Si lo declara total o parcialmente inconstitucional, el

[53] Decreto 2591 de 1991.
[54] Decreto 4759 de 2005, Decreto 1151 de 2008, Ley 1266 de 2008, Ley 1341 de 2009.
[55] Ver Anexo 2 normatividad en protección de datos: https://docs.google.com/document/d/1THqWby6vwbtsquLKmsXtAGrM4FEIg2Q-40AdEH1o5Ig/edit?hl=en_US
[56] REMOLINA-ANGARITA NELSON. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010). Página 505.

Presidente de la Corte deberá enviarlo a la Cámara de origen con el fallo al respecto.

La importancia de este proyecto de ley es que tiene la categoría de ley estatutaria, es decir, el mismo regula el núcleo fundamental del derecho al habeas data y la protección de datos personales para el tratamiento de cualquier dato personal (salvo el comercial y financiero que se rige por la ley 1266 de 2008)[57].

Sobre la normatividad en protección de datos personales la Corte Constitucional concluyó que la ley 1266 de 2008 es de aplicación limitada y sectorial. La Corte dejo claro que "*para el tratamiento de otros tipos de datos personales debe observarse el conjunto de los principios desarrollados por ese tribunal desde la sentencia T-414 de 1992 a la fecha, los cuales se recopilaron y explicaron en el numeral 2.4 de la sentencia C-1011 de 2008. No obstante lo anterior, debe concluirse que por interpretación de la Corte, ratificada y acogida por autoridades públicas, Colombia carece de una Ley general sobre protección de datos*"[58].

Como lo anota un informe sobre antecedentes judiciales en Colombia desde una perspectivas de los derechos humanos de la Defensoría del Pueblo, la falta de una regulación estatutaria sobre datos personales resulta en deficiencias en la regulación, precisamente una de sus recomendaciones al Gobierno Nacional es expedir una reglamentación que tenga en cuenta los principios, criterios y parámetros constitucionales, legales y doctrinarios de la administración de datos personales[59].

Este argumento es también sostenido por el Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática- GECTI de la Universidad de los Andes. Consideran crucial aprobar una nueva ley estatutaria porque el marco jurídico actual es insuficiente. Para el GECTI la ley 1266 de 2008 exponen tiene unas disposiciones desfavorables como las enunciadas a continuación:[60]

- Autorizar cobrarle al ciudadano por conocer sus propios datos personales y ejercer el habeas data (Parágrafo 2 del artículo 10 de la ley 1266)
- Fijar reglas de transferencia internacional que no dan garantías al ciudadano sobre el tratamiento de sus datos en el exterior (Literal f del artículo 5 de la ley 1266)
- Crear mecanismos de peticiones, consultas y reclamos mas dispendiosos en el tiempo que en últimas abren las puertas para demorar "injustificadamente" la efectividad de los derechos de los titulares de datos personales. Los términos de la ley 1266 de 2008 no tienen presentación frente a bases de datos sistematizadas que pueden generar la información de inmediato. (Artículo 16 de

[57] REMOLINA ANGARITA NELSON, Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del habeas data y la protección de los datos personales. Documento GECTI No 11, Noviembre 24 de 2010. Página 3.
[58] REMOLINA-ANGARITA NELSON. ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010). Página 512.
[59] DEFENSORIA DEL PUEBLO. Informe Defensorial. La institución de los antecedentes judiciales en Colombia desde una perspectiva de los derechos humanos de la Defensoría del Pueblo. Diciembre de 2010. Página 87.
[60] REMOLINA ANGARITA NELSON, Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del habeas data y la protección de los datos personales. Documento GECTI No 11, Noviembre 24 de 2010. Página 6.

la ley 1266). Los términos del proyecto para estas cuestiones debería reducirse a una tercera parte de lo propuesto.

El GECTI también hace una observación al alcance de la ley estatutaria en trámite No 46 de 2010 de Cámara, 184 de 2010 Senado, porque se incurre de nuevo en el error de no establecer tipos de información y grados o niveles de acceso a la información. Exponen particularmente el caso del certificado de antecedentes judiciales que según el proyecto de ley en revisión de la Corte plantea que el titular, interesado o tercero pueden disponer de la misma certificación[61] la cual, además, según el artículo 29 no contendría los antecedentes penales[62].

En la intervención ciudadana del GECTI ante la Corte Constitucional solicitó declarar inexequible el articulo 29, entre las razones expuestas esta el Departamento Administrativo de Seguridad-DAS "en lugar de proteger de eventuales riesgos a la ciudadanía lo que hace es quitarle a la sociedad una herramienta de información que puede ser útil para la defensa de la vida y los bienes de las personas"[63]. Como ejemplo exponen que se estaría impidiendo a la ciudadanía conocer si una persona fue violador, torturador, secuestrador, etc. En este caso al DAS le tocará certificar que no registra antecedentes, ocultando frente a la ciudadanía que se trata de un asesino o violador[64].

Sobre este mismo tema se refiere la Defensoría del Pueblo en el informe enviado a la Corte Constitucional a propósito del estudio que se adelanta de la Ley, sugiere a propósito del artículo 29 seguir los principios de los principios de proporcionalidad, razonabilidad, finalidad como confidencialidad a fin de alcanzar la más adecuada caracterización de la información que reposa en los antecedentes de las personas.

Para la Defensoría se debe considerar una regulación que considere todos los extremos e intereses en conflicto, que defina los delitos y contravenciones de mayor y menor impacto, que generen o no antecedentes. Asimismo deben establecerse los términos definidos y razonables para la permanencia de los antecedentes, los cuales deben estar atados a la mayor o menor gravedad del antecedente. Esto con el fin de reconocer que el certificación es el medio idóneo para conocer el pasado de las personas y constituye un medio de alguna utilidad, para garantizar la idoneidad, honradez y lealtad de los servidores con la Función Pública, en actividades que pueden implicar riesgos a terceras personas como en los procesos de adopción o para la autorización de porte de armas, o para los partidos políticos al seleccionar adecuadamente sus candidatos. De esta forma se evita el desgaste innecesario de

[61] DEFENSORIA DEL PUEBLO. Informe Defensorial. La institución de los antecedentes judiciales en Colombia desde una perspectiva de los derechos humanos de la Defensoría del Pueblo. Diciembre de 2010. Página 41.
[62] Proyecto de ley estatutaria 46 de 2010 de Cámara, 184 de 2010 Senado Articulo 29, Parágrafo: Al expedir certificados judiciales por petición ciudadana, el Departamento Administrativo de Seguridad o quien ejerza esta función, se abstendrá de incluir como antecedente penal los registros delictivos del solicitante cuando este haya cumplido su pena o la misma haya prescrito".
[63] REMOLINA ANGARITA NELSON. GECTI-Observatorio de la Protección de Datos Personales. Universidad de los Andes. Intervención ante la Corte Constitucional Ref. Proyecto de Ley 46 de 2010 Cámara/184 de Senado. Bogotá, abril de 2011. Página 34.
[64] REMOLINA ANGARITA NELSON. GECTI-Observatorio de la Protección de Datos Personales. Universidad de los Andes. Intervención ante la Corte Constitucional Ref. Proyecto de Ley 46 de 2010 Cámara/184 de Senado. Bogotá, abril de 2011. Página 34.

esfuerzos públicos y privados en elegir a personas inhabilitadas por su comportamiento pasado[65].

Actualmente, no existe un órgano de control que garantice y regule la protección de datos. Precisamente dentro de los estudios del GECTI se recomienda contar con una autoridad de control de protección de datos personales que sea autónoma, independiente, técnica y con suficientes recursos humanos y económicos para que cumpla su cometido[66].

Actualmente las peticiones o reclamos se formulan mediante escrito dirigido al operador del banco de datos. En caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial mediante acción de tutela para amparar el derecho fundamental del hábeas data[67]. La ley 1266 de 2008 estableció en su artículo 17 que "la Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países". Y en la reciente ley aprobada en el Congreso[68] se prevé que la Superintendencia continúe ejerciendo la función de protección de datos, ahora en un sentido más amplio que la sola información financiera.

Las atribuciones de la Superintendencia serían, entre otras, adelantar las investigaciones y como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data, promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales; impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento. Adicionalmente, tendrá la capacidad imponer a personas privadas multas, podrá suspender u ordenar el cierre temporal o inmediato de las actividades relacionadas con el Tratamiento de datos. Ante el presunto incumplimiento de una autoridad pública a las disposiciones, se remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva[69].

Relación entre ambos derechos:

En Colombia el derecho de acceso a información pública y la protección de datos personales han tenido un desarrollo normativo disperso, no existe una ley estatutaria, un órgano que garantice y controle su cumplimiento. Ha sido la Corte Constitucional quien ha dirimido los conflictos existentes entre los dos derechos en diferentes sentencias de las cuales se destaca que en múltiples oportunidades ha

[65] DEFENSORIA DEL PUEBLO. Informe Defensorial. La institución de los antecedentes judiciales en Colombia desde una perspectiva de los derechos humanos de la Defensoría del Pueblo. Diciembre de 2010. Página 79.
[66] REMOLINA ANGARITA NELSON, Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del habeas data y la protección de los datos personales. Documento GECTI No 11, Noviembre 24 de 2010. Página 7.
[67] Ley 1266 de 2008, Art. 16. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html
[68] Ley 46 de 2010 de Cámara, 184 de 2010 Senado
[69] Informe de conciliación al proyecto de ley 046 2010 Cámara, 184 2010 Senado "Por medio del cual se dictan disposiciones generales para la protección de datos personales". Diciembre, 2010. Articulo 21 y 23. Disponible en: http://www.habeasdata.org.co/wp-content/uploads/2010/12/Informe-Conciliaci%C3%B3n1.pdf

declarado el carácter autónomo del derecho de acceso a la información[70]. La Corte anota que *"una disposición como la ley 1266 de 2010 no debe comprenderse de manera tal que afecte el principio general de publicidad de las actuaciones del Estado, el libre ejercicio del derecho a la información y, en últimas, la aceptabilidad de ámbitos de la actuación estatal que incorporen una "cultura del secreto", en todo incompatible con el carácter participativo del Estado Social y Democrático de Derecho*"[71].

Para la Corte los datos personales "*se encuentran fuera de la órbita de conductas protegidas por el régimen general del derecho constitucional a la información. En consecuencia, la colisión entre derecho al habeas data o derecho a la autodeterminación informática y derecho a la información, deberá resolverse atendiendo las particularidades tanto de la información, convertida en datos personales, como de los rasgos y poder de irradiación del derecho a la autodeterminación informática"[72]. Por tal motivo ha desarrollado una tipología de información y datos personales para dirimir conflictos entre ambos derechos*"[73]. Esta tipología es útil para los casos en que el derecho de acceso a la información puede colisionar con el derecho al habeas data. La sentencia 216 de 2004 retoma la sentencia T-729 de 2002 para exponer los tipos de información como se describe a continuación:

- "la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno".

- "La información semi-privada, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas".

- "La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los

[70] Corte Constitucional de Colombia. Sentencia T-1029 de 2005. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2010/t-1029-10.htm
[71] Corte Constitucional de Colombia. Sentencia 1011 de 2008 de control de constitucionalidad de la ley 1266 de 2010. Disponible en: http://www.cntv.org.co/cntv_bop/basedoc/cc_sc_nf/2008/c-1011_2008.html
[72] Corte Constitucional de Colombia. Sentencia T-729 de 2002. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9903
[73] Ibíd.

documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio".

- "Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc".

De otra parte la Corte ha indicado sobre los límites al derecho de acceso a información pública o el establecimiento de una reserva legal sobre cierta información – cuando:"i) la restricción está autorizada por la ley o la Constitución; ii) la norma que establece el límite es precisa y clara en sus términos de forma tal que no ampare actuaciones arbitrarias o desproporcionadas de los servidores públicos; iii) el servidor público que decide ampararse en la reserva para no suministrar una información motiva por escrito su decisión y la funda en la norma legal o constitucional que lo autoriza; iv) la ley establece un límite temporal a la reserva; v) existen sistemas adecuados de custodia de la información; vi) existen controles administrativos y judiciales de las actuaciones o decisiones reservadas; vii) la reserva opera respecto del contenido de un documento público pero no respecto de su existencia; viii) la reserva obliga a los servidores públicos comprometidos pero no impide que los periodistas que acceden a dicha información puedan publicarla; ix) la reserva se sujeta estrictamente a los principios de razonabilidad y proporcionalidad; x) existen recursos o acciones judiciales para impugnar la decisión de mantener en reserva una determinada información."[74].

A partir de la gradación de la información personal como de los límites al acceso, han permitido dirimir el conflicto entre los dos derechos. Como lo señala la Corte:

> *"Hay mayor o menor grado de aceptabilidad de la divulgación, así, la información pública, en tanto no está relacionada con el ámbito de protección del derecho a la intimidad, recae dentro del ejercicio amplio del derecho a recibir información (Art. 20 C.P.) y, en consecuencia, es de libre acceso. Ello, por supuesto, sin perjuicio que en relación con la divulgación de la información pública, resulten aplicables las garantías que el derecho al hábeas data le confiere al sujeto concernido, en cuanto resulten pertinentes. En contrario, los datos semiprivados y privados, habida cuenta la naturaleza de la información que contienen, se les adscriben restricciones progresivas en su legítima posibilidad de divulgación, que se aumentan en tanto más se acerquen a las prerrogativas propias del derecho a la intimidad De esta forma, el dato financiero, comercial y crediticio, si bien no es público ni tampoco íntimo, puede ser accedido legítimamente previa orden judicial o administrativa o a través de procedimientos de gestión de datos personales, en todo caso respetuosos de los derechos fundamentales interferidos por esos procesos, especialmente el derecho al hábeas data financiero"[75].*

[74] Corte Constitucional de Colombia. Sentencia 491 de 2007. Disponible en: www.andiarios.com/.../SENTENCIAS/Sentencias_Corte.../C-491-07.doc

[75] Corte Constitucional de Colombia. Sentencia 1011 de 2008 de control de constitucionalidad de la ley 1266 de 2010. Disponible en: http://www.cntv.org.co/cntv_bop/basedoc/cc_sc_nf/2008/c-1011_2008.html

Casos prácticos:

Con base en la tipología desarrollada, la Corte ha resuelto diferentes casos, como la tutela en el que un ciudadano solicitaba amparo de su derecho a la intimidad porque unas entidades públicas divulgaban en sus páginas Web, a través de un mecanismo público de consulta, la información económica sobre todas las propiedades registradas en Bogotá incluyendo detalles sobre las mismas y la información privada familiar de los afiliados al sistema de seguridad social en salud.

En este caso la Corte de Colombia analizó la relación entre el derecho a acceder a la información y el derecho a la autodeterminación informática o habeas data. Se encontró un desconocimiento de los principios de libertad, finalidad e individualidad, rectores de la administración de datos personales, y considero que la publicación de la base de datos sobre la información catastral de Bogotá en la Internet, tal y como está dispuesta, el Departamento administrativo de Catastro Distrital de Bogotá, vulnera el derecho fundamental a la autodeterminación informática del ciudadano. La decisión fue ordenar a las entidades evitar un acceso indiscriminado a la información, sin el consentimiento previo y libre, información personal del ciudadano[76].

Considera entonces la Corte que, la publicación de la base de datos sobre los afiliados al sistema integral de seguridad social en Salud, la Superintendencia Nacional de Salud vulnera el derecho fundamental a la autodeterminación informática. "Debido a que este tipo de datos personales está catalogado como información semi-privada, es decir que su acceso se encuentra restringido, la posibilidad de su conocimiento por parte de terceros totalmente ajenos al ámbito propio en el cual se obtuvo dicha información, a partir del sencillo requisito de digitar su número de identificación, desconoce los principios constitucionales de libertad, finalidad, circulación restringida e individualidad propios de la administración de datos personales"[77].

En la sentencia T-705/07 de la Corte Constitucional trata el caso de una de varias personas desplazadas que solicitan a Acción Social que les certifique su condición de personas desplazadas inscritas en el Registro Único de Población Desplazada-RUPD con el fin de poder participar en una asociación de desplazados. Acción Social contesta el derecho de petición indicando que no puede acceder a la solicitud presentada por cuanto la información del RUPD es de carácter reservado en virtud del artículo 9 del decreto 2131 de 2003 y el artículo 15 del decreto 2569 del 2000. En este caso la Corte considero que la entidad a su vez vulnera el derecho fundamental al habeas data al oponer la reserva de información al titular de la misma. Asimismo la Corte constató que sobre el RUPD pesa una reserva constitucional y en esa medida se limita el acceso a terceros a la información allí consignada. Sin perjuicio que, de la información que resulte derivada del RUPD y que haga relación al cumplimiento de la política pública de atención a la población desplazada, esto es información sobre la atención presentada, el grado de

[76] Corte Constitucional de Colombia. Sentencia T-729 de 2002. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9903

[77] Corte Constitucional de Colombia. Sentencia T-729 de 2002. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=9903

cobertura, la cantidad de personas inscritas y demás información impersonal no opera la reserva y por lo tanto se tiene libre acceso a ella[78].

Jurisprudencia:

1. *Caso de una sentencia de la corte sobre entrega de documentos con datos personales:*

En la Sentencia T-837 de 2008 la Corte Constitucional de Colombia revisó un proceso de tutela en el cual cuatro personas solicitaron la información médica de sus familiares, quienes no podían autorizar la divulgación de la historia clínica por haber fallecido o encontrase en estado de inconsciencia. En este caso la Corte reconoció que aunque ese tipo de información es reservada y sólo puede ser divulgada con la autorización de su titular, en algunos casos especiales los familiares pueden acceder a la misma:

"El acceso a la información médica de un paciente, por parte de sus familiares, no debe garantizarse en contravía del derecho a la intimidad y al libre desarrollo de la personalidad del paciente que se encuentra enfermo. Por tal razón, se debe atender a las circunstancias específicas de cada caso, y en principio, procurar que sólo cuando el paciente haya autorizado el acceso de su familia a su información médica, se les proporcione a éstos.

"Sin embargo, se pueden presentar eventualidades en las que los familiares, actuando en representación del paciente, tengan derecho acceder a esta información de manera inmediata. Tal sería el caso de un paciente que se encuentre en un estado mental o de salud que no le permita comprender cabalmente la información que se le está suministrando, o no esté en condiciones para dar su consentimiento frente el tratamiento que se le va a aplicar o en condiciones para autorizar que sus familiares sean enterados de su situación clínica"[79]

2. *Obligación de entregar de datos personales:*

Recientemente en la Sentencia T-511 de 2010 la Corte consideró que el derecho de acceso como una herramienta esencial para la satisfacción del derecho a la verdad de las víctimas de actuaciones arbitrarias y de violaciones de derechos humanos y para garantizar el derecho a la memoria histórica de la sociedad, con lo cual ordenó a la Policía Nacional entregar a dos ciudadanas, información sobre las patrullas que estaban asignadas a una determinada zona, las labores realizadas y los datos del personal que las estaba desempeñando.

Esta sentencia tiene como precedente la Sentencia T-1025 de 2007, el caso de un ciudadano, quien actuaba como representante de la Comunidad de Paz de San José de Apartadó, contra el Ministerio de Defensa Nacional. Manifiesta el actor que, inicialmente, solicitó al Ministro de Defensa "15 datos elementales, referentes a la identidad de oficiales, suboficiales y soldados o agentes de la Policía Nacional que estuvieron presentes en fechas, sitios y circunstancias precisas en que fueron

[78] Corte Constitucional de Colombia . Sentencia T-705 de 2007 Disponible en: http://www.acnur.org/biblioteca/pdf/5753.pdf?view=1

[79] Corte Constitucional de Colombia. Sentencia T-837 de 2008. Disponible en: http://www.sututela.com/jurisprudencia/sentencia-de-tutela-t837-de-2008-t-837-08

vulnerados gravemente los derechos de integrantes de la Comunidad de Paz de San José de Apartadó o de personas colaboradoras o cercanas a la misma Comunidad." La Corte concluye que la medida escogida para lograr la no identificación de los miembros de la Fuerza Pública – la reserva de los nombres de los efectivos que participan en determinadas acciones distintas a las de inteligencia – no cumple con los requisitos de necesidad y de proporcionalidad que incorpora el juicio estricto de proporcionalidad de la medida. En consecuencia se ordenó al Ministerio de Defensa suministrar al demandante la relación de los nombres de los miembros de la Fuerza Pública concernidos, con indicación de las fechas de servicio y el lugar donde fue prestada, según lo pedido por el demandante[80].

Rol de la Sociedad Civil:

En relación al rol de la sociedad civil en la promoción del derecho de protección de datos personales, el GECTI (Grupo de Estudios en internet Comercio electrónico, Telecomunicaciones e Informática) desde el año 2001 liderado por el profesor Nelson Remolina Angarita tiene dentro de sus objetivos procurar reflexiones y acciones en materia de la Internet, la Sociedad de la Información y temas convergentes. En desarrollo de este objetivo adelanta estudios y comunicaciones sobre la protección de datos personales[81]. Dentro de los cuales se destacan Documento GECTI No 11 de 2010 "Propuestas para mejorar y aprobar el proyecto de ley estatutaria sobre el derecho fundamental del habeas data y la protección de los datos personales", "Documentos GECTI sobre protección de datos personales" (2005), los cuales fijan una posición académica que el regulador debería analizar con miras a que se garantice un nivel adecuado de protección de los datos personales de las colombianas y los colombianos. Asimismo ha hecho un seguimiento permanente al trámite y aprobación del proyecto de ley estatutaria 042 de 2010 por la cual se dictan disposiciones generales para la protección de datos personales.

[80] Corte Constitucional de Colombia. Sentencia T-1025 de 2007. Ver Sentencia 511 de 2010. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2010/t-511-10.htm
[81] http://www.gecti.org/

1.6. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN COSTA RICA

Instituto de Prensa y Libertad de Expresión (IPLEX)
Secretario de la Junta Directiva: Raúl Silesky

Acceso a la Información Pública:

No existe una ley de acceso a información pública. no obstante la constitución política concretamente en el numeral 30, dispone: "artículo 30.- se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de estado." a partir se esta norma hay una amplia y consistente jurisprudencia de la Sala Constitucional que garantiza el acceso a información publica.

El derecho y sus alcances se han desarrollado a partir de la jurisprudencia constitucional.

No existe un órgano de control especifico, pero el sistema lo que prevé es recurso de amparo como medio para obligar a entregar información publica a quien la solicite y le sea negada.

Protección de Datos Personales:

Se acaba de aprobar la ley denominada "Ley para la protección de la Persona frente al tratamiento de sus datos personales" que se encuentra en trámite de publicación en el diario oficial y también se deberá de reglamentar

La normativa aprobada, se aplicará a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos. El régimen de protección de los datos de carácter personal que se establece la Ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean vendidas o de cualquier otra manera comercializadas. Establece y desarrolla los principios de Autodeterminación informativa, consentimiento informado, el de calidad de la información, entre otros.

a. La ley crea la Agencia de Protección de Datos de los Habitantes (PRODHAB), con personalidad jurídica instrumental para el desempeño de sus funciones, es un órgano con desconcentración máxima adscrito al Ministerio de Justicia y Paz. Se financia con los cánones, las tasas y los derechos obtenidos en el ejercicio de sus funciones, transferencias que el Estado realice a su favor, donaciones y subvenciones provenientes de otros Estados, instituciones públicas nacionales u organismos internacionales, siempre que no comprometan la independencia, transparencia y autonomía de la Agencia y lo generado por sus recursos financieros. De manera expresa se indica que los montos provenientes del cobro de las multas señaladas en esta ley, será destinado a la actualización de equipos y programas de la PRODHAB.

Son funciones de la Agencia:

a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos.
b) Llevar un registro de las bases de datos reguladas por esta Ley.
c) Requerir de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados.
d) Acceder a las bases de datos reguladas por esta ley, a efecto de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia, y excepcionalmente cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información.
e) Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales.
f) Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales.
g) Imponer las sanciones establecidas en el artículo 28 de esta ley a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de aquellas que puedan configurar delito.
h) Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales.
i) Dictar las directrices necesarias, las cuales deberán ser publicadas en el Diario Oficial La Gaceta, a efecto de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional.
j) Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, almacenamiento, transferencia y uso de sus datos personales.

Relación entre ambos derechos:

Ambos derechos se complementan, debe de tenerse presente que no hay legislación de acceso a información pública, hay un desarrollo jurisprudencial

El ejercio de ambos derechos se controla por medio del control de constitucional que ejerce la Sala Constitucional y también el de legalidad que se tramita ante los juzgados contencioso administrativos. En el primer caso, Recurso de Amparo ante al Sala Constitucional está establecido para garantizae los derechos y libertades undamentales, que no estén protegidos por el de hábeas corpus. El amparo procede contra toda disposición, acuerdo o resolución y, en general, contra toda acción, omisión o simple actuación material no fundada en un acto administrativo eficaz, de los servidores y órganos públicos, que haya violado, viole o amenace violar cualquiera de aquellos derechos. El amparo procederá no sólo contra los actos arbitrarios, sino también contra las actuaciones u omisiones fundadas en normas erróneamente nterpretadas o indebidamente aplicadas. Y no será necesaria la reposición ni ningún otro recurso administrativo para interponer el recurso de amparo.

El Amparo de legalidad se permite, ante los juzgados contenciosos cuando Hasta el año 2007, los amparos de legalidad, los trámites preferentes y las solicitudes de pronta respuesta y aquellas interpuestas ante las violaciones al artículo 41 de la

Constitución Política, se presentaban ante la Sala Constitucional. Los casos en los cuales no se está de acuerdo con la respuesta dada por la institución, no constituyen Amparos de Legalidad.

Esta instancia generalmente, fallaba a favor de la persona que presentaba el recurso de amparo en los casos de atrasos o fallas en la notificación de los trámites. Según lo estipulado por legislación: La Administración, a la luz del artículo 41 constitucional, tiene la obligación de garantizarle a la ciudadanía el cumplimiento de la justicia pronta y cumplida, sin denegación, lo que implica, en el ámbito de la justicia administrativa, su obligación de decidir con diligencia y celeridad los reclamos planteados por los administrados, de tal manera que su resolución sea congruente con los extremos alegados, así como de comunicarles a los interesados lo dispuesto, todo ello dentro de un plazo razonable.

A partir del año 2008 los conflictos por justicia pronta y cumplida entre las instituciones públicas y las y los ciudadanos y aquellas referencias al artículo 41 constitucional ya no son resueltos por la Sala Constitucional. La nueva normativa, a través del Código Procesal Contencioso-Administrativo (Ley No. 8508 de 24 de abril de 2006) establece que estos asuntos deben ser presentados ante el Tribunal Contencioso Administrativo. Con este Código la justicia administrativa trata de acelerar los procesos, procurando dar una respuesta más rápida y eficaz a las demandas de la población. El proceso contencioso administrativo busca de proteger los derechos de acceso a la justicia y de justicia pronta y cumplida, para ello se integraron al proceso fases de tramitación oral, lo que pretende contribuir con velocidad, humanización y transparencia en la resolución de los asuntos que se sometan a **e**ste tipo de demanda. El Amparo de Legalidad es un proceso judicial utilizado en casos específicos que tienen que ver con el derecho a la pronta respuesta. (...) Atiende situaciones en las cuales hay un trámite preferente, que estipula que se resuelvan en periodos muy cortos pues hay interés público que compromete (por ejemplo, interés superior del menor, trámites de migración, violencia doméstica). Asimismo, trámites en los cuales se solicita algún tipo de información o datos públicos a una instancia (información pura y simple), a los cuales todas las personas tienen derecho a acceder y que no tengan restricción de confidencialidad para ser accesados.

Cabe aclarar que el fallo a favor de que se conteste a una persona no implica que le resuelvan a favor su situación o trámite, pues se vela por la tramitación en el plazo que corresponde. A su vez, no se necesita la gestión por parte de un abogado/a para presentar este tipo de recurso.

Casos prácticos

Hay una clara jurisprudencia de la Sala Constitucional en los existía duda entre si la información solicitada era de carácter público o no, y por lo tanto si se debía de entregar por parte de las autoridades públicas:

a) **Sentencia 4005-05**. Se le negaba a periodista de un diario acceso a la información de las actas de la Junta Directiva de la CCSS. El caso se declaró con lugar ordenándose al Presidente Ejecutivo de la Caja Costarricense de Seguro Social la entrega inmediata de las actas solicitadas.[82]

[82] Para mayor información ver: https://docs.google.com/document/d/1TtqqUCwT_Wazd66pCSGkDadMy6dRSGASzqnWLYlAzUA/edit?hl=en_US

b) **Sentencia 9705-04.** Un banco privado negó a unos periodistas información sobre las cuentas corrientes de partidos políticos. Se declaró con lugar en cuanto parte de los dineros depositados eran fondos públicos por concepto de deuda política.[83]

Jurisprudencia:

Se presentó ante la Sección de Opciones y Naturalizaciones del Registro Civil, una solicitud a fin de iniciar los trámites de naturalización; no obstante, esta fue denegada, aduciendo que existen "anotaciones" en la Dirección de Inteligencia y Seguridad Nacional, por lo que no cumple con los requisitos para optar por la nacionalización en Costa Rica. Ante esta situación, el siete de julio del dos mil ocho, solicitó ante la Dirección recurrida, que le certificaran cuáles y qué clase de anotaciones aluden en su contra, que indiquen la procedencia de autoridad judicial o administrativa del país o país extranjero que ordenó tal disposición, a fin de conocer cuáles son los cargos que se le endilgan y corregir los datos en caso que sean incorrectos; no obstante, por medio del oficio N.° COP-182-2008 del diez de octubre del año en curso, la recurrida le informó que, de conformidad con los numerales 10 y 16 de la Ley General de Policía N.° 7410, no brindarían la información que se solicitó, pues lo informes que existen sobre su persona son confidenciales y podrían declararse secreto de Estado, omitiendo si fueron declarados o no, así como número de resolución, lo que estima que la omisión por parte de la autoridad recurrida lesiona sus derechos fundamentales.

La Sala Constitucional resolvió en este caso: “En el caso bajo estudio, se tiene que el recurrente presentó ante la Sección de Opciones y Naturalizaciones del Registro Civil, solicitud de naturalización, la cual según aduce le fue denegada por anotaciones existentes en la Dirección de Inteligencia y Seguridad Nacional, razón por la cual el tres de octubre de dos mil ocho, solicitó ante la mencionada Dirección, certificación de cuáles y qué clase de anotaciones aluden en su contra, y que se indicara la procedencia de la autoridad judicial o administrativa del país o país extranjero que ordenó tal disposición, certificación que le fue denegada en oficio No. COP-182-2008 del diez de octubre de dos mil ocho, con base en los numerales 10 y 16 de la Ley General de Policía. De lo esbozado en el considerando anterior, se desprende que es un derecho fundamental de todo administrado el tener acceso a los datos que le afecten de alguna forma, tal como sucede en la especie, que la información que retiene la Dirección de Inteligencia y Seguridad Nacional, inciden en la decisión del Registro Civil de otorgar o no la naturalización al accionante. En virtud de ello, los datos que tiene en su base la autoridad recurrida son de interés particular del recurrente, toda vez que lo afectan directamente. Resalta este Tribunal que si bien es cierto hay alguna información –como la que nos ocupa en este caso-, que no debe serle facilitada a todas las personas, pues es información sensible de una determinada persona, sí tiene esa persona en particular la potestad de solicitarla y el correspondiente derecho de que se le otorgue, no así a un tercero que no acredite su interés. Aunado a ello, es menester resaltar que no cuestiona esta Tribunal en esta oportunidad lo establecido en los numerales 10 y 16 de la Ley General de Policía; sin embargo, los alcances y la interpretación que a éstos se les de, no pueden de manera alguna ir en contra de un derecho fundamental

[83] Para mayor información ver: http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=XYZ&param2=1&nValor1=1&nValor2=288598&strTipM=T&lResultado=7

establecido en el Derecho de la Constitución. En mérito de lo expuesto, lo procedente es declarar con lugar el recurso, como en efecto se ordena. Por tanto. Se declara con lugar el recurso. Se ordena a Jorge Torres Carrillo, en su condición de Subdirector General de la Dirección de Inteligencia y Seguridad Nacional (DIS) del Ministerio de la Presidencia, o a quien en su lugar ejerza el cargo, brindarle acceso al amparado Carlos Arturo Meneses Reyes a la información por él solicitada en escrito del día tres de octubre de dos mil ocho, de forma INMEDIATA a partir de comunicación de esta sentencia, bajo el apercibimiento que con base en lo establecido en el artículo 71 de la Ley de la Jurisdicción Constitucional, se impondrá prisión de tres meses a dos años, o de veinte a sesenta días multa, a quien recibiere una orden que deba cumplir o hacer cumplir, dictada en un recurso de amparo y no la cumpliere o no la hiciere cumplir, siempre que el delito no esté más gravemente penado. Se condena al Estado al pago de las costas, daños y perjuicios causados con los hechos que sirven de fundamento a esta declaratoria, los que se liquidarán en ejecución de sentencia de lo contencioso administrativo. Notifíquese esta sentencia a Jorge Torres Carrillo, en su condición de Subdirector General de la Dirección de Inteligencia y Seguridad Nacional (DIS) del Ministerio de la Presidencia, o a quien en su lugar ejerza el cargo, EN FORMA PERSONAL. COMUNÍQUESE.-"[84]

Rol de la Sociedad Civil:

No existen iniciativas en la sociedad civil para promover la protección de datos.

[84] Ver Sentencia: 01426 Expediente: 08-017133-0007-CO Fecha: 04/02/2009 Hora: 3:31:00 PM Emitido por: Sala Constitucional
http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=XYZ&param2=1&nValor1=1&nValor2=445546&strTipM=T&lResultado=4

1.7. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

Fundamedios
Director Ejecutivo: César Ricaurte
Director de Proyectos: Mauricio Alarcón

Acceso a la Información Pública

La normativa que regula el ejercicio del derecho de acceso a la información pública (AIP) en Ecuador es la Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada en el Registro Oficial Suplemento 337 del 18 de Mayo de 2004[85].

La Ley garantiza y norma el ejercicio del derecho fundamental de las personas a la información conforme a las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes, de los cuales Ecuador es signatario.

La ley es aplicable a:

- Los organismos y entidades que conforman el sector público del Estado;
- Las personas jurídicas cuyas acciones o participaciones pertenezcan en todo o en parte al Estado, exclusivamente sobre el destino y manejo de recursos del Estado;
- El derecho de acceso a la información de los asambleístas de la República se rige conforme a lo dispuesto en la Constitución Política de la República, en la Ley Orgánica de la Función Legislativa y su Reglamento Interno;
- Las corporaciones, fundaciones y organismos no gubernamentales (ONG's) aunque tengan el carácter de privadas y sean encargadas de la provisión o administración de bienes o servicios públicos, que mantengan convenios, contratos o cualquier forma contractual con instituciones públicas y/u organismos internacionales, siempre y cuando la finalidad de su función sea pública; y
- Las personas jurídicas de derecho privado, que sean delegatarias o concesionarias o cualquier otra forma contractual de servicios públicos del Estado, en los términos del respectivo contrato.

El órgano de control del ejercicio del derecho de acceso a la información pública es la Defensoría del Pueblo, y sus atribuciones son:

- Ser el órgano promotor del ejercicio y cumplimiento del derecho de acceso a la información pública;
- Vigilar el cumplimiento de esta Ley por parte de las instituciones públicas, personas jurídicas de derecho público o privado y demás entes señalados en el artículo 1 de la presente Ley;
- Vigilar que la documentación pública se archive bajo los lineamientos que en esta materia dispone la Ley del Sistema Nacional de Archivos;
- Precautelar que la calidad de la información que difundan las instituciones del sector público, contribuyan al cumplimiento de los objetivos de esta Ley;
- Elaborar anualmente el informe consolidado nacional de evaluación, sobre la base de la información publicada en los portales o páginas web, así como

[85] http://www.transparencia.espol.edu.ec/documentos/L_acceso.pdf

todos los medios idóneos que mantienen todas las instituciones y personas jurídicas de derecho público, o privado, sujetas a esta Ley;
- Promover o patrocinar a solicitud de cualquier persona natural o jurídica o por iniciativa propia, acciones judiciales de acceso a la información pública, cuando ésta ha sido denegada; e
- Informar al Congreso Nacional en forma semestral, el listado índice de toda la información clasificada como reservada.

Protección de Datos Personales

En el Ecuador no existe una ley específica que regule el ejercicio del derecho de protección de Datos Personales. De todos modos, existen normas de carácter constitucional que tienen relación con la misma:

- Constitución de la República del Ecuador

Capítulo sexto- Derechos de libertad

Art. 66.- Se reconoce y garantizará a las personas:

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación

Sección quinta- Acción de hábeas data

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Las disposiciones mencionadas tienen un carácter y jerarquía constitucional y se encuentran direccionadas para que los ciudadanos a través de acciones judiciales hagan efectivos dichos derechos si llegaren a ser vulnerados.

No existe un órgano de control al respecto de las mencionadas disposiciones, sólo puede acudirse a las mismas a través de acciones judiciales.

Relación entre ambos derechos

La acción de acceso a la información pública contenida en el artículo 91 de la Constitución de la República del Ecuador[86], así como el precitado artículo 92 ibídem, que versa sobre la acción de hábeas data tienen la misma jerarquía jurídica al estar contenidos en la Carta magna ecuatoriana.

Jurisprudencia

De las búsquedas e investigaciones realizadas por Fundamedios no existe jurisprudencia en materia de acceso a la información relacionada con la existencia única del Recurso de Acceso a la Información Pública. A partir de 2008, año en que la nueva Constitución de la República entró en vigencia- y con ella, la Acción Constitucional de Acceso a la Información Pública-, la Corte Constitucional ha dictado una sola jurisprudencia en la materia que no se relaciona con entrega de información que se consideraba un dato personal.

Rol de la Sociedad Civil

La sociedad civil ecuatoriana atraviesa en estos momentos una situación un tanto crítica, producto de su desarticulación y cooptación por parte del Gobierno Nacional. Las organizaciones que aún se mantienen en su rol estricto de sociedad civil, se han enfocado en trabajar el acceso a la información pública (investigación, litigio estratégico, reformas a la ley, etc.) mas no ha habido iniciativa de promover la protección de datos personales.

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

1.8. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN EL SALVADOR

A) Asociación de Periodistas de El Salvador (APES)
Presidente: Nery Mabel Reyes

Acceso a la Información Pública
La normativa que regule el ejercicio del derecho de acceso a la información pública en El Salvador es la nueva Ley de Acceso a la Información Pública que fue aprobada en marzo de 2011 y entrará en vigencia en marzo de 2012[87].

La mencionada ley ofrece la posibilidad de que las personas puedan solicitar la información que requieran con base a los lineamientos que se establecen en la ley.

El órgano de control del ejercicio del derecho de acceso a la información pública será el Instituto de Acceso a la Información Pública, que estará encargado de resolver los casos de apelación cuando los solicitantes no obtengan una respuesta satisfactoria por parte de las unidades de acceso a la información. Dicho Instituto tendrá como máxima autoridad a 5 comisionados propietarios y sus respectivos suplentes.

Protección de Datos Personales
En relación a la Protección de Datos Personales (DP) en El Salvador, solamente existió una discusión de un proyecto de ley en el congreso pero no prosperó. Dicha propuesta buscaba evitar algunos abusos que se cometen por parte de empresas que registran bases de datos personales y venden la información.
De todos modos, se puede encontrar dentro de la ley de Acceso a la Información una sección dedicada a la protección de datos (arts. 31 y 32)

Relación entre ambos derechos
Por el momento en El Salvador solo se cuenta con una ley de acceso a la información que entrará en vigencia en marzo de 2012.
Asimismo, cabe señalar que no existe por, el momento, ningún tipo de control de la relación de ambos derechos.

Casos Prácticos y Jurisprudencia
La protección de datos personales estará incluida en la Ley de Acceso a la Información pero, por el momento, no contamos con un caso específico en el que se haya obligado al Estado a entregar la información.

Rol de la Sociedad Civil:
Algunas organizaciones como INDATA han estado trabajando en el tema para proteger los datos personales del accionar de organizaciones como INFORNET SA que recopilaba información personal y la vendia a otras empresas.

[87] Diario oficial tomo No. 391, 8 de abril de 2011

B) Fundación Salvadoreña para El Desarrollo Económico y Social (FUSADES)
Director Departamento de Estudios Legales: Javier Castro De León
Analista de Institucionalidad Democrática: Carmina Castro

Acceso a la Información Pública:

Desde el 8 de mayo de 2011 se encuentra vigente en El Salvador la Ley de Acceso a la Información Pública (LAIP) luego de una intensa campaña desde la sociedad civil para su aprobación. Su aprobación por todas las fuerzas políticas de la Asamblea Legislativa fue motivo de celebración nacional e internacional, puesto que El Salvador ingresaba a las filas de países que protegen este derecho con leyes de avanzada. Actualmente, el reto es que la ley aprobada se cumpla efectivamente. La ley tiene plazos escalonados para su entrada en vigencia, es fundamental cuidar que todos los plazos se respeten para no amenazar la entrada en vigencia plena de la normativa en mayo 2012[88].

Emisión de reglamento de elección de comisionados	5 de septiembre de 2011
Emisión de reglamento general de la ley	5 de septiembre de 2011
Designación de oficiales de información	4 de noviembre de 2011
Nombramiento de comisionados del Instituto de Acceso a la Información Pública	4 de noviembre de 2011
Presentación de solicitudes de información	7 de mayo de 2012
Publicación de información oficiosa	7 de mayo de 2012
Organización y funcionamiento de archivos	7 de mayo de 2012

La LAIP tiene como característica que es de obligatorio cumplimiento por todo sujeto público o privado que maneje fondos públicos o desempeñe una función pública (art. 7) por lo que se incluye el Gobierno central, las municipalidades, los órganos del Estado, los organismos constitucionalmente independientes e incluso entidades mixtas o privadas. La LAIP incluye un amplio listado de información que debe ser publicada oficiosamente, regula las causas de excepción del acceso a la información como información reservada o confidencial, establece un procedimiento para la solicitud de información a las entidades públicas y establece infracciones y sanciones.

El órgano de control de la LAIP es el Instituto de Acceso a la Información Pública (IAIP), una "institución de derecho público, con personalidad jurídica y patrimonio propio, con autonomía administrativa y financiera" (art. 50). El mismo está conformado por 5 comisionados electos por el Presidente de la República. Una característica que lo diferencia del resto de las instituciones públicas salvadoreñas es que todos sus miembros provienen de propuestas de organizaciones de la sociedad civil: por las asociaciones empresariales debidamente inscritas; por las asociaciones profesionales debidamente inscritas; por la Universidad de El Salvador y las universidades privadas debidamente autorizadas; por las asociaciones de periodistas debidamente inscritas; y, por los sindicatos autorizados por el Ministerio de Trabajo y Previsión Social. Uno de los reglamentos que deben emitirse es el que

[88] Ver Fusades (2011). "Urge aprobación de buenos reglamentos para la transparencia". En Posición Institucional. Antiguo Cuscatlán, El Salvador. http://www.fusades.org/get.php?id=2738&anchor=1

regulará la celebración de asambleas sectoriales en las cuáles se elegirá la terna por cada sector, de la cuál el Presidente de la República deberá elegir un comisionado y su suplente. El Instituto tiene una serie de facultades para asegurar el cumplimiento de la ley (art. 58), entre las cuáles resaltan: conocer los recursos de apelación de las decisiones de AIP de los sujetos obligados por la ley; dictar sanciones administrativas ante el cometimiento de infracciones a la LAIP; dar apoyo técnico a los entes obligados en la elaboración y ejecución de sus programas de transparencia y AIP; y establecer los lineamientos en ciertas materias de AIP, entre otras.

Protección de Datos Personales

La LAIP en su Título III regula la protección de datos personales (DP) en poder de las entidades públicas, pero no lo hace en el caso de las entidades privadas, considerándose en todo momento de su discusión que debía emitirse con posterioridad una Ley de Protección de Datos Personales más general que regulara también a los privados.

Asimismo, hay regulación dispersa sobre la temática en diversos cuerpos normativos como en la Ley de Protección al Consumidor, Ley de Bancos, entre otras. En junio de 2011 fue promulgada la Ley de Regulación de los Servicios de Información sobre el Historial de Créditos de las Personas (LRSIHCP). Esta ley que fue aprobada en abril de 2011, fue observada por el Presidente de la República en mayo de este año y la Asamblea aceptó las observaciones completamente el 23 de junio de 2011. Esta ley entrará en vigencia 90 días después de su publicación en el Diario Oficial, la cual a la fecha no se ha efectuado por el retraso habitual de esta publicación. La ley si bien tiene por objeto garantizar la confiabilidad, veracidad, y el buen manejo de los datos de las personas, hace referencia a los datos relativos al historial de crédito, por lo que continúa siendo un ámbito reducido y no la ley integral que se requiere.

Por otra parte, en este momento la Asamblea Legislativa tiene bajo su estudio dos proyectos de ley en materia de protección de datos personales, pero se desconoce que tan pronto se emitiría una normativa en esta temática. Por el momento, si una entidad privada mantiene bases de datos que no contuvieran información crediticia, no hay ley que regule esta actividad ni entidad que le supervise.

La LAIP establece el derecho a la protección de datos personales de toda persona frente a los entes obligados por la misma, es decir frente a entidades públicas o privadas que manejen fondos públicos. A estos últimos se les obliga a adoptar procedimientos que permitan la indagatoria, actualización, modificación y supresión de datos personales, a respetar la finalidad para la que se otorgan los datos personales, adoptar medidas para proteger la seguridad de los datos personales, entre otras.

En cuanto a entidades privadas, la LRSIHCP establece los requisitos para operar una agencia de información de datos, el procedimiento para la autorización para ejercer esta actividad, el registro de estas agencias, las obligaciones y prohibiciones a las que están sujetas. Se regulan los derechos de los consumidores sobre sus DP, incluyendo: la necesidad de su consentimiento para la recopilación y trasmisión, su derecho a su acceso, a la fidelidad de la información, al buen manejo de la misma, la rectificación, modificación, eliminación de la información y actualización, estableciendo un procedimiento para garantizarlos.

El órgano facultado para garantizar la protección de datos personales es el mismo IAIP, en cuanto a aquellos datos en poder de las entidades obligadas por la LAIP y cuando no se trate de información crediticia. Este podrá conocer las apelaciones en materia de DP cuando una entidad obligada se niegue a dar acceso a los DP de una persona, o a modificarlos o rectificarlos. La IAIP también deberá ser informado de las bases de datos que mantengan los entes obligados, podrá establecer lineamientos sobre el tratamiento DP, elaborar formularios para las solicitudes referentes a DP, desarrollar cursos de capacitación sobre DP a servidores públicos, entre otras.

La LRSIHCP establece como órganos de control la Superintendencia del Sistema Financiero y la Defensoría de Consumidor. La Superintendencia del Sistema Financiero es la entidad responsable de supervisar la actividad individual y consolidada de los integrantes del sistema financiero (art. 3 Ley de Supervisión y Regulación del Sistema Financiero, LSRSF). La Defensoría del Consumidor es la institución descentralizada de la administración pública encargada de velar por los derechos e intereses de los consumidores en las relaciones con los proveedores de bienes y prestadores de servicios (Art. 58 Ley de Protección al Consumidor). La LRSIHCP faculta a la Superintendencia para autorizar a personas jurídicas para ejercer la actividad de agencia de información, mantener un registro de las mismas, dictará las normas técnicas para su funcionamiento y fiscalizará su cumplimiento. La Defensoría del Consumidor, por su parte, conocerá las denuncias o quejas de los consumidores. Habrá que ver en la práctica que no haya dificultades por esta dualidad de competencias ya que a ambas se faculta para imponer las sanciones correspondientes a las infracciones en la ley.

Por otra parte la LRSIHCP establece que los particulares podrán acudir a los juzgados civiles y mercantiles para reclamar los daños y perjuicios en contra de los agentes económico y/o agencia de información de datos (art. 7 LRSIHCP).

Relación entre ambos derechos:

El derecho al acceso a la información pública y el derecho a la protección de los datos personales no son derechos absolutos, por lo que ambos deben coexistir en el ordenamiento jurídico salvadoreño. Tampoco existe una prevalencia de un derecho sobre el otro, sino que será caso por caso que se determine cual prevalece.

En la LAIP se considera información confidencial, “Los datos personales que requieran el consentimiento de los individuos para su difusión” (art. 24 literal c. LAIP). Por otro lado, sólo se puede difundir datos personales cuando haya consentimiento de parte del titular (Art. 25 y 33 LAIP) con excepción a los casos que determina la LAIP en los que no se requiere consentimiento para que sea divulguen DP, (art. 34 LAIP). De esta manera el rol del consentimiento es determinante.

El ejercicio de ambos derechos, frente a las entidades públicas, que manejan recursos o información públicos o que ejecuten actos de la función estatal (art. 7 LAIP) está regulado mediante la ley de Acceso a la Información Pública. El IAIP será el ente que determine el alcance de uno y otro derecho en los casos que se le presenten. Éste está facultado para conocer sobre la apelación o inconformidad con la clasificación de una información (art. 58 d. y g.). Por lo que si ante una solicitud de acceso a la información una entidad obligada arguye que dicha información está clasificada como información confidencial por tratarse de datos personales, el solicitante podrá acudir ante el IAIP.

Casos prácticos

No se han presentado casos aún en los que se involucren ambos derechos. Actualmente, diversas instituciones que manejan bases de datos y que estarán obligadas por la LAIP se encuentran evaluando como se conciliarán ambas obligaciones. Por ejemplo, la Dirección de Centros Penales está evaluando como conciliar la información del perfil de los imputados con la protección a datos personales. Lo mismo está sucediendo en el Órgano Judicial para el tema de sentencias. Por tanto, se deberá estudiar cómo lo ha resuelto la experiencia internacional.

Jurisprudencia

Como se ha mencionado la LAIP entrará en vigencia de manera integral hasta el 7 de mayo de 2012, por lo que no se tiene jurisprudencia al respecto.

Rol de la Sociedad Civil

En El Salvador ha habido una iniciativa de parte de la sociedad civil para promover la protección de datos personales llevada adelante por una organización en particular, INDATA, haciendo uso del litigio estratégico frente a la Sala de lo Constitucional de la Corte Suprema de Justicia, el último intérprete de la Constitución en El Salvador. En la sentencia definitiva del Amparo 934-2007, emitida el 4 de marzo de 2011, se dio por finalizado un proceso de más de 3 años, en el que se admitió que actuara en virtud de un interés difuso o colectivo. En su fallo, la Sala ordena a INFORNET S.A. de C.V., que permita a los particulares interesados el acceso a la base de datos que tiene en su poder, para que puedan actualizar, rectificar o anular aquellos datos estrictamente personales, que no constan en registros o aquellos que no estén actualizados. Esto lo deberá realizar de forma gratuita. La Sala también ordena a INFORNET S.A. de C.V. que se abstenga de utilizar y transferir los datos personales que consten en su base sin la autorización expresa de los titulares de dichos datos.

Por otra parte, la Sala de lo Constitucional insta al legislador a que desarrolle procedimientos que garanticen especialmente la protección de los datos personales. Establece que el Órgano Legislativo "está obligado a establecer las condiciones" para garantizar el derecho de autodeterminación informativa y señala los principios que deben guiar dicha legislación: principio de transparencia sobre el tipo, dimensión, uso y fines del procesamiento de datos, el principio de sujeción al fin del procesamiento consentido, el principio de prohibición del almacenamiento con el fin de facilitar e un tratamiento no autorizado posterior, prohibición de la construcción de perfiles, el principio de olvido (o de temporalidad) mediante la implementación de reglas de destrucción de los datos personales una vez cumplido el fin de su recopilación.

Este es el tercer caso de amparo que la Sala conoce en amparo una caso en el que se reclama el derecho a la autodeterminación informativa, es decir, el derecho de las personas a recibir protección frente a la amenaza que supone la distribución de sus datos personales sin su consentimiento. En los tres casos INDATA ha intervenido. Sin embargo, es el primer caso en el se obtiene una sentencia estimatoria. Como ya se mencionó, aún se encuentran en estudio dos iniciativas de ley en la Asamblea Legislativa que buscarán dar respuesta a lo señalado en la sentencia.

1.9. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN GUATEMALA

Para información sobre la implementación de Ley de Acceso a la Información Pública en Guatemala, consultar el informe Saber Más[89] y el Saber Más II[90], así como la siguiente página web:

Acción Ciudadana
http://www.accionciudadana.org.gt/

[89] http://alianzaregional.net/site/images/stories/saber_mas.pdf
[90] http://www.said-on-net.com/alianza/septiembre_2010/SABERMASII.pdf

1.10. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN HONDURAS

Para informacion sobre la implementación de la Ley de Transparencia y Acceso a la Información Pública en Honduras, consultar el informe Saber Más[91], así como las siguientes páginas web:

Comité por la Libre Expresión (C-Libre), Honduras
http://www.clibre.info/

Fundación Democracia sin Fronteras (FDsF), Honduras
http://www.fdsf.hn/

[91] http://alianzaregional.net/site/images/stories/saber_mas.pdf

1.11. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

Fundar, Centro de Análisis e Investigación, A. C.
Director Ejecutivo: Miguel Pulido

Acceso a la Información Pública:

En México existen 33 leyes que regulan el ejercicio del derecho de acceso a la información pública (1 federal –LFTAIPG- y una por cada entidad federativa). Además existe un artículo constitucional (el 6º) que prevé el acceso a la información.

El texto constitucional, a partir de la reforma constitucional de 2007, prevé lo siguiente:

"*Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por lo siguientes principios y bases: I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes."*[92]

Más detalle sobre la calidad de las leyes y estudios comparados se puede encontrar en: www.checatuley.org y en www.metricadelatransparencia.org.mx

En el caso de la legislación federal, la ley se destaca por contar con una amplia cobertura de sujetos obligados pero de carácter dual (en tanto tiene un doble sistema de órganos de garantía) y al mismo tiempo es habilitante de múltiples formas de acceso y no establece mayores requisitos para las y los solicitantes. Sobre el primer punto podemos detallar que el primero es el artículo 13 fr. XIV de la LFTAIP que expresamente identifica como sujetos obligados a los siguientes:

"*a) el Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República*
b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos
c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;
d) Lo órganos constitucionales autónomos
e) Los tribunales administrativos federales y
f) Cualquier otro órgano federal"

No obstante, sólo los previstos en el inciso a) son sujetos obligados en términos lisos y llanos. Es decir, están bajo el imperio del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y su conducta se rige en directamente por la Ley Federal de Transparencia. Por su parte, el artículo 61 establece que "*El Poder Legislativo Federal, a través de la Cámara de Senadores, la Cámara de Diputados, la Comisión Permanente y la Auditoría Superior de la Federación; el Poder Judicial de la Federación a través de la Suprema Corte de Justicia de la Nación, del Consejo de la Judicatura Federal y de la comisión de Administración del Tribunal Federal*

[92] Constitución Política de los Estados Unidos Mexicanos: http://info4.juridicas.unam.mx/ijure/fed/9/7.htm?s

Electoral, los órganos constitucionales autónomos y los tribunales administrativos, en el ámbito de sus respectivas competencias, establecerán mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios establecidos en esta Ley." A esto es a lo que se hace referencia cuando se menciona el sistema dual en términos de órganos garantes.

El IFAI tiene como mandato el "*promover y difundir el ejercicio del derecho de acceso a la información; resolver la negativa a las solicitudes de acceso a la información; y proteger los datos personales en poder de las dependencias y entidades*" (artículo 33 de la LFTAIPG).
Una esquematización de las funciones principales derivadas de ese mandato legal, puede ser la siguiente:
1. Funciones *resolutivas y reguladoras.* El Instituto conoce de los recursos de revisión y de las controversias respecto a la interpretación de la Ley, función que deberá realizar con apego a lo establecido en la Constitución y los Tratados Internacionales. Además, debe resolver en los procesos que tengan por objeto la tutela de datos personales. En lo que hace a la función reguladora, le corresponde la expedición de lineamientos.
2. Funciones de *vigilancia y de coordinación* esenciales para impulsar avances en la transparencia del gobierno federal. La Ley le refiere atribuciones que se relacionan con otros poderes (por ejemplo, en la integración de los informes de transparencia de la totalidad de los Sujetos Obligados), así como con la Secretaria de la Función Pública en lo que hace al régimen de sanciones.
3. Función de *promoción* es fundamental para fomentar y difundir los beneficios del derecho de acceso a la información pública gubernamental e impulsar una cultura de transparencia y rendición de cuentas (en los artículos 33, 37 y 38 de la Ley, haciendo valer los objetivos previstos en el artículo 4).
4. Por último, funciones *operativas y administrativas* que son necesarias para la buena operación del Instituto y asegurar el cumplimiento de sus demás funciones. Entre estas están las funciones para definir su estructura orgánica y ocupacional, designar funcionarios, etc. Es importante señalar que en el caso de las funciones de control interno, estas son realizadas por un Titular de Unidad que no puede interferir en las decisiones sustantivas de la entidad (artículo 10 del Decreto).

Protección de Datos Personales:

El 5 de julio de 2010 se publicó el Decreto promulgatorio de la Ley Federal de Protección de Datos.[93] Este instrumento prevé los mecanismos en función de los cuáles los particulares tienen obligaciones explícitas en la protección y tutela de datos personales, prevé, además, los llamados derechos ARCO (acceso, rectificación, cancelación y oposición)

Es importante precisar que previo a la aprobación de la ley de protección de datos hubo uno reforma al artículo 16 de la Constitución en la que se incluyó expresamente el derecho a la protección de los datos personales. El artículo constitucional incorporó el siguiente texto:

"*Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismo, así como a manifestar oposición en los*

[93] El texto puede consultarse aquí:
http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."[94]

Este antecedente es importante, pues en el artículo transitorio tercero de dicha reforma se previó que tendría que existir una Ley. Sumado a ello, sin duda esta será una fuente relevante de interpretación. A la luz de lo anterior, lo que tenemos en México es una Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Un breve resumen del contenido y características de le ley sería el siguiente:

Sobre el alcance.
Se trata de una Ley de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares. La propia Ley reconoce como finalidad el regular el "tratamiento legítimo, controlado e informado (de los datos) a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas."

Sujetos obligados.
En realidad en el ámbito de la tutela de datos, se les conoce como sujetos regulados y por las características particulares de esta Ley es evidente que son los particulares (no importa si son personas físicas o morales) de carácter privado que lleven a cabo el tratamiento de datos personales.
Es importante aclarar que en tanto que ya existe una legislación particular para las sociedades de información crediticia (bancos y buros de crédito) la ley expresamente señala en el artículo 2 que no serán de su ámbito de aplicación.

La materia de la ley. La protección de los datos personales
Un aspecto importante de esta legislación es que nos remite a los principios internacionales que serán aplicables para determinar cuáles son las obligaciones que tienen los responsables del tratamiento de datos. Estos principios son la licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

En el caso Federal, a partir de 2010, las funciones (y el nombre del Instituto) cambiaron, ampliándose su mandato en materia de datos personales, como resultado de la aprobación de la Ley Federal de Protección de Datos Personales.

A grandes rasgos las característica de la intervención institucional del IFAIPD serán (a partir de enero de 2012) las siguientes:

El Instituto será la autoridad garante en materia de protección de datos. En este sentido vigilará a los sujetos regulados, podrá además realizar estrategias de intervención preventiva y resolverá las controversias en la materia.

El IFAI garantizará la no injerencia arbitraria o ilegal en la vida privada de las personas, provocada por el mal uso de los datos personales, tal como está previsto en el artículo 16 de la Constitución.

[94] Adicionado mediante decreto publicado en el DOF el 1 de junio de 2009. El texto puede consultarse aquí: http://info4.juridicas.unam.mx/ijure/fed/9/17.htm

El IFAI estará facultado para imponer infracciones y sanciones a quienes hagan mal uso de los datos personales que obren en sus bases de datos o en su poder.

Para lograr estos resultados, el IFAI podrá realizar actividades de capacitación así como establecer estándares de seguridad. En el aspecto contencioso atenderá quejas, llevará a cabo procesos conciliatorios, inspecciones sobre el manejo de las bases de datos y en los casos en los que detecté el incumplimiento de la normatividad, emitirá sanciones.[95]

Relación entre ambos derechos

Existen diversos tipos de relación tanto entre los derechos de acceso a la información y el de protección de datos como entre las normativas que los regulan.

En el caso de los datos personales en posesión de dependencias del gobierno federal, al igual que para el acceso a la información, el órgano garante y responsable de la interpretación es el IFAI. La Ley, para ambos casos es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. En ese caso, la ley no prevé propiamente una prelación de un derecho sobre otro, no obstante sí establece guías de interpretación en los principios de máxima publicidad y de máxima disponibilidad (ver artículo 6 de la LFTAIPG) que pueden tener un impacto al momento de resolver casos de posible enfrentamiento entre ambos. También contiene las reglas de excepción en las cuáles los datos personales podrán ser divulgados (previa autorización expresa) o cuando obren en fuentes de acceso público (ver artículos 18 y 19 de la LFTAIPG).

Por otra parte, el IFAI también es el órgano regulador de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. En éste caso, al no existir un derecho de acceso a documentos públicos en poder de particulares (o alguna otra consideración similar) no es fácil identificar casos en los que exista colisión de derechos.

Es importante señalar que desde hace varios años está pendiente una reforma a la LFTAIPG. En los dictámenes que se discuten en la Cámara de Diputados (uno de ellos ya aprobado en la Cámara de Senadores) se incluye una prueba de daño y una prueba de interés público. Ambas reglas estarían destinadas a resolver problemas de interpretación entre estos derechos.

Casos prácticos:

En la resolución 6030/09, el 10 de marzo de 2010, el Instituto resolvió un caso de acceso a la información en el que un solicitante requirió el nombre de las personas a las que se hubieran cancelado créditos fiscales para el año 2007, sin embargo, el Servicio de Administración Tributaria se ha negado en forma tajante a entregar la información sobre los montos y nombres de los beneficiados por la cancelación de los créditos fiscales. El argumento central, además del de datos personales, es que si se revela esta información se estaría violando el secreto fiscal. Es importante señalar que la cancelación de los créditos fiscales en 2007 es del orden de cerca de 74 mil millones de pesos.

[95] Documentos y herramientas que explican el papel del IFAI en la protección de los datos personales están disponibles en: http://www.ifai.org.mx/Particulares/faq

La postura del IFAI es que no hay violación al secreto fiscal y sostiene que esta información sí debe divulgarse por ser de obvio interés público y porque permitirá saber si realmente las autoridades no actuaron con discrecionalidad.

Otros casos relevantes se encuentran relacionados con la publicación de datos personales de los servidores públicos. Estos fueron de los primeros casos resueltos por el IFAI. Como ejemplo se puede mencionar el Recurso de Revisión 129 sobre la Cédula profesional de los mandos altos y medios de la SSP (Secretaría de Seguridad Pública) y PFP (Policía Federal) con relación del puesto desempeñado. La Secretaría de Seguridad Pública originalmente clasificó la información argumentando que con fundamento en los artículos 44 y 45 de la LFTAIPG, la información solicitada no puede ser proporcionada debido a que es confidencial, porque afecta la vida privada y la intimidad de las personas. Dicha respuesta también se fundamenta en los artículos 27, 28 y 40 del Reglamento de la LFTAIPG. No obstante, el IFAI revocó la resolución instruyendo que se entregara la información, en caso de obrar en sus archivos.

También han sido destacados los casos sobre los nombres de beneficiarios de programas sociales y el acceso a los padrones que contienen dicha información. El caso del Recurso 2431/09 sobre el acceso a los nombres de beneficiarios del Seguro Popular es uno de los más destacados. En dicho caso, la discusión en el pleno efectivamente versó sobre el equilibrio entre acceso a la información y protección de datos personales.[96]

Jurisprudencia

En relación a jurisprudencia que haya obligado al Estado a entregar infomacion que haya considerado (o sea) dato personal, se puede señalar el Recurso de Revisión 12997 sobre la Cédula profesional de los mandos altos y medios de la SSP (Secretaría de Seguridad Pública) y PFP (Policía Federal) con relación del puesto desempeñado- mencionada anteriormente.

Asi tambien se puede mencionar lo resuelto por el Poder Judicial en cuanto al juicio de amparo respecto al derecho a conocer las actas de asamblea del Consejo Consultivo de la Comisión Nacional de los Derechos Humanos.98 En ese caso, el juez resolvió que dado que “los miembros del consejo de la CNDH desempeñan una función pública dentro de un organismo público, cuyas facultades se encuentran plenamente definidas”, por lo que la información solicitada “se relaciona con una reunión de interés público”. Por tanto, “la negativa a proporcionar esos datos viola la garantía de acceso a la información pública”

Rol de la Sociedad Civil:

Los esfuerzos de incidencia y de participación de la sociedad civil en procesos legislativos más destacados han sido en el área de transparencia y acceso a la información. De todos modos, existen algunas iniciativas menores para promover la

[96] Lo recuperado por la prensa se puede consultar en la siguiente liga: http://www.jornada.unam.mx/2009/07/16/sociedad/037n1soc
[97] http://www.ifai.org.mx/resoluciones/2003/129.pdf
[98] Referencias de prensa pueden ser consultadas aquí: http://www.jornada.unam.mx/2007/10/12/index.php?section=politica&article=025n2pol

protección de datos personales, principalmente desde la perspectiva de los derechos del consumidor y el derecho a la privacidad e intimidad.

Asimismo, en los últimos años algunos órganos de transparencia han abierto procesos de promoción del derecho a la protección de datos en los que han participado organizaciones de la sociedad civil, tales como seminarios, conferencias, talleres y capacitaciones. Es posible que en el mediano plazo haya un rol más activo de organizaciones de la sociedad civil.

1.12. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN NICARAGUA

Fundación Violeta Barrios de Chamorro (FBVCH)
Directora Ejecutiva: Cristiana Chamorro
Coordinador del Programa AIP: Guillermo Medrano

Acceso a la Información Pública

En Nicaragua el derecho de Acceso a la Información Pública se encuentra regulado por la Ley de Acceso a la Información Pública, Nro. 621, aprobada por la Asamblea Nacional el día 16 de mayo del año 2007 y publicada en la Gaceta Diario Oficial del 22 de junio 2007. Dicha ley norma, garantiza y promueve el ejercicio del derecho de acceso a la información pública. Esta Ley regula a los cuatro Poderes del Estado: Ejecutivo, Legislativo, Judicial y Electoral, en todas sus dependencias, nacional, departamental y municipal. También se aplica a los Gobiernos Regionales y Gobiernos Municipales (Alcaldías).

La Ley mandata que en cada una de las dependencias del Estado, Gobierno Regional y Gobiernos Municipales deberá crear una Oficina de Acceso a la Información Pública, la que funcionará de manera independiente; y dependerá directamente de la máxima autoridad superior de cada entidad estatal.

Protección de Datos Personales

En Nicaragua, la Protección de Datos Personales se encuentra contemplada en la Constitución Política en su arto. 26:
"Toda persona tiene derecho:
a) A su vida privada y a la de su familia"

Asimismo, en la mencionada Ley de Acceso a la Información Pública, en su Arto. 4 Literal m, se hace mención a:

"m. Información privada: La compuesta por datos personales referidos a la vida privada o de la familia, tales como salud, raza, preferencia política o religiosa, situación económica, social o familiar o a su honra y reputación; así como todos aquellos datos personales que están tutelados y protegidos por la Constitución Política y la Ley."

En términos de alcance, en el caso de la Constitución de la República protege a todos los ciudadanos, mientras que en el caso de la Ley de Acceso a la Información Pública, regula solamente a los funcionarios públicos.

Relación entre ambos derechos:

El derecho de Acceso a la Información Pública es complementario de la Protección de Datos Personales, dado que en la Constitución de la República de Nicaragua, se contemplan ambos derechos. En su Art. 26, la Constitución establece que toda persona tiene derecho a su vida privada y a la de su familia, al igual que en el Arto. 66 de nuestra carta magna menciona que los nicaragüenses tienen derecho a una información veraz. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas, ya sea de manera oral, por escrito o gráficamente o por cualquier otro medio de su elección. Es decir, ningún derecho predomina sobre el

otro, porque ambos están concebidos en igualdad de oportunidades en la Constitución. Aunque el derecho a la vida privada se concibe como un derecho individual y el de información se concibe como un derecho social.

Ambos derechos están contemplados en la Ley de Acceso a la Información pública, pero lamentablemente nuestro sistema judicial está politizado y ninguno de esos mencionados derechos se cumple actualmente debido que predomina la tendencia política del funcionario ante los derechos del ciudadano.

En caso de disputas, el procedimiento es acudir ante la sala de lo contencioso administrativo de la Corte Suprema de Justicia- donde puede llevar hasta 8 años para que se dicte una sentencia-. "Una sentencia tardía, no es hacer justicia"

Casos prácticos:

En Nicaragua se pueden encontrar numerosos casos en los que el Estado se niega a entregar información aludiendo que se trata de datos personales. Uno de los casos mas relevantes es el del actual presidente del Consejo Supremo Electoral. Dicho funcionario ha sido denunciado reiteradamente debido a su enriquecimiento ilícito, a través de su cargo en el Estado. La ciudadanía ha preguntado reiteradamente a cuánto asciende su riqueza, pero la Contraloría General de la República, no revela el total de su patrimonio aduciendo que se trata de información personal.

Jurisprudencia:

En cuanto a jurisprudencia no se cuenta con ningún caso. Aún mas, en el año 2007 un grupo de ciudadanos demandó al Consejo Supremo Electoral para que diera a conocer el 100 % de los resultados totales de las elecciones presidenciales del 2006. Hasta la fecha no se tiene repuesta, porque predomina el interés político, sobre el derecho ciudadano de solicitar información pública.

Rol de la Sociedad Civil:

En el año 2009 se introdujo ante el Parlamento nicaragüense un anteproyecto de Ley[99], pero hasta la fecha (2 años después) no ha sido considerado pero ni en la comisión dictaminadora.

99

https://docs.google.com/document/d/1yBM5GPZ75TUH3YiWpuWWkNbxuEEaoxIEnMNLANT81CE/edit?hl=en_US

1.13. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN PANAMÁ

Para informacion sobre el derecho de Acceso a la Información Pública en Panamá, consultar el informe Saber Más[100] y Saber Más II[101], así como la siguiente página web:

Consejo Nacional de Periodismo:
www.cnppanama.org

[100] http://alianzaregional.net/site/images/stories/saber_mas.pdf
[101] http://www.said-on-net.com/alianza/septiembre_2010/SABERMASII.pdf

1.14. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN PARAGUAY

Instituto de Derecho y Economía Ambiental (IDEA)
Director Ejecutivo: Ezequiel Santagada

Acceso a la Información Pública

Actualmente, Paraguay no cuenta con una ley que regule el ejercicio del derecho de Acceso a la Información Pública. Sin embargo, cualquier habitante de la República puede fundar una solicitud de acceso a la información pública ante las reparticiones públicas del gobierno sobre la base de previsto en la Constitución de la República de Paraguay en sus artículos 28 (derecho a informarse), 40 (derecho a peticionar a las autoridades) y 45 (operatividad de los derechos y garantías constitucionales)[102]. Además, sobre la base del Art. 137 (primacía de la Constitución y categoría supra-legal de los tratados internacionales), pueden invocarse los artículos 19 del Pacto Internacional de Derechos Civiles y Políticos y 13 de la Convención Americana de Derechos Humanos.

Desde la promulgación de la Ley 3966/10 "Ley Orgánica Municipal" (art 68), los gobiernos municipales deben "*proporcionar toda información pública que haya creado u obtenido, de conformidad al Artículo 28 "Del derecho a informarse" de la Constitución Nacional, dentro del plazo que se les señale, el cual no podrá ser mayor de quince días*" [103].

Asimismo, algunos gobiernos municipales cuentan con Ordenanzas que regulan el acceso a la información pública municipal (Asunción, Villarrica, Pilar, Bahía Negra, entre otros). A su vez, algunos ministerios del Poder Ejecutivo han regulado el acceso a la información que generan u obtienen por medio de Resoluciones (por ejemplo, Ministerio de Agricultura y Ganadería, Res. 1216/07).

Es conveniente destacar que en los casos no abarcados por las normas municipales, se deben realizar peticiones ante la autoridad pública de la cual se necesite obtener información. Ante la negativa o silencio, sólo cabe acudir al Poder Judicial.

En cuanto al control del ejercicio del derecho de Acceso a la Información Pública en Paraguay, al no haber una ley en la materia, no existe un órgano de control.

Protección de Datos Personales

En Paraguay, la protección de datos personales está regulada en la Ley 1.682/01 "*Que reglamenta la información de carácter privado*"[104] (texto según Ley 1.969/02 que modifica a la mencionada ley)

La Ley tiene "*por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro*

[102] Constitución de la República de Paraguay: http://www.periodismo-aip.org/images/documentos/constituciondeparaguay.pdf
[103] Ley Orgánica Municipal: http://www.glin.gov/download.action?fulltextId=278452&documentId=236661&glinID=236661
[104] http://www.morinigoyasociados.com/todas_disposiciones/2001/leyes/ley_1682_01.htm

medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares" (Art.1).

La Ley no se aplica a "*las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar*" (Art.1).

La Ley distingue entre datos personales públicos y privados. Los primeros son *"los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional*" (Art. 6, inciso "a"). Entre los segundos, también se distingue entre datos sensibles y datos patrimoniales.

La Ley define como datos sensibles a *"los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten perjuicios y discriminaciones, o afecten la dignidad, la privacidad la intimidad doméstica y la imagen privada de personas o familias*" (Art. 4). Con relación a estos, la Ley prohíbe "*dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables*".

"*Los datos de personas físicas o jurídicas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente: a) cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; b) cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas; y, c) cuando consten en las fuentes públicas de información*" (Art. 5).

La Ley obliga a las empresas, personas o entidades que almacenan, procesan y difunden esa información a actualizar permanentemente los datos personales patrimoniales (Art. 7) y establece que no transmitirán ni divulgarán datos: a) pasados tres años de la inscripción de deudas vencidas no reclamadas judicialmente[105]; b) pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal; c) sobre juicios de convocatoria de acreedores después de cinco años de la resolución judicial que la admita (Art. 9).

En cuanto al control de la protección de datos personales, la Ley 1.682/01 no prevé órgano de control.

Asimismo, cabe destacar que el art. 135 de la Constitución consagra la garantía a toda persona de "*acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos*".

[105] Las obligaciones reclamadas judicialmente surgen de fuentes públicas de información y, por lo tanto, son libremente publicables (Ver, Corte Suprema de Justicia, Sala Constitucional. Acuerdo y Sentencia número 528 del 26 de junio de 2007).

Relación entre ambos derechos:

La regulación sobre protección de los datos personales tiene por finalidad garantizar el efectivo goce del derecho a la intimidad establecido en el Art. 33 de la Constitución, derecho de igual rango que el derecho de acceso a la información pública (Art. 28).

Al no existir órganos administrativos que controlen el ejercicio de estos derechos, los eventuales conflictos entre ambos derechos los dirime el Poder Judicial, ponderando, equilibrando y definiendo los contornos de uno y otro en casos concretos.

Casos prácticos

Caso Picco Portillo: El ciudadano Picco solicitó a la Municipalidad de Lambaré información sobre el listado de todos los funcionarios municipales con indicación de su nombre, documento de identidad, funciones que realizaban y salario que percibían. Ante el silencio de la Municipalidad, Picco acudió a la justicia y, en segunda instancia, se consideró que la información que él había solicitado era información pública y que el gobierno municipal debía entregársela de inmediato[106].

Caso Vargas Télles: El ciudadano Vargas solicitó la misma información que Picco pero a la Municipalidad de San Lorenzo. Ésta se opuso a entregarla argumentando que, de hacerlo, estaría violando el derecho a la intimidad de sus funcionarios; puntualmente, consideró que entregar la información sobre el salario que los funcionarios percibían podía generar tal afectación. Un tribunal de segunda instancia le dio la razón a la Municipalidad. El caso se encuentre pendiente de resolución ante la Corte Suprema.

Jurisprudencia:

En el caso Picco, la Municipalidad no consideró que la información que él había solicitado se tratara de datos personales que podrían afectar el derecho a la intimidad de sus funcionarios. Si bien la información sobre los salarios que los funcionarios percibían no era un dato personal público, según como están definidos por la Ley 1682/01 (Art. 6, inciso "a"), tampoco se trataba de "datos sensibles" (Art. 4). En consecuencia, sólo podrían ser calificados como información sobre datos personales de libre divulgación por constar en una fuente pública de información (Art. 5) o bien, datos personales carentes de una protección específica que, al constar en una fuente pública de información (como lo es una agencia estatal o gubernamental) son de acceso libre para todos.

Este parecería haber sido el razonamiento del Tribunal de Apelaciones, que sostuvo: "*Por su parte, la ley de Información Privada Nº 1682/01, modificada por la Ley 1969 de fecha septiembre de 2002, establece en su art. 2º "Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado. Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley 879 del 2 de diciembre de 1981, la Ley Nº*

[106] El gobierno municipal nunca sostuvo que podía haber una afectación a la intimidad de sus funcionarios. Sólo argumentó que la vía procesal para cuestionar los efectos jurídicos de su silencio no era la adecuada.

608 del 18 de julio de 1995, y sus modificaciones" cuya fórmula es una repetición de la norma constitucional, con ciertas aclaraciones y precisiones, que no son restrictivas, sino por el contrario.

Entonces, cualquier negativa a proporcionar información respecto de la estructura de la organización – incluso del personal- o de la aplicación de los recursos presupuestarios, que no caiga en una de las causales de reserva arriba reseñadas, constituye una medida injustificada y violatoria del derecho a la información consagrado en nuestra Constitución. En este caso no ha sido argüida ninguna de las eximentes permitidas por la normativa"[107].

Por otra parte, no se conoce jurisprudencia en Paraguay que haya obligado a entregar, mediando una solicitud de acceso a la información pública, datos personales sensibles o datos que revelen, describan o estimen la situación patrimonial de una persona, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras aún cuando esa persona no haya autorizado su divulgación y no se trate de obligaciones reclamadas judicialmente.

[107] Tribunal de Apelaciones en lo Civil y Comercial del 3er. Turno, Asunción. Acuerdo y Sentencia número 51 del 2 de mayo de 2008 (decisión firme y ejecutoriada). Caso *Picco Portillo vs. Municipalidad de Lambaré* s. /Amparo. Disponible en http://www.idea.org.py/gfx/espanol/descargas/normativa_ambiental/jurisprudencia/nacional/Caso_Picco_Portillo_acceso_Informacion.pdf . Este caso ha sido citado en el Informe de la Relatoría Especial para la Libertad de Expresión en el Informe Anual de la Comisión Interamericana de Derechos Humanos 2010. Ver Capítulo IV Buenas Prácticas Judiciales en Materia de Acceso a la Información en América, página 313, puntos 34 y 35, disponible en: http://www.cidh.oas.org/annualrep/2010sp/RELATORIA_2010_ESP.pdf

1.15. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN PERÚ

Instituto Prensa y Sociedad (IPYS)
Director Ejecutivo: Ricardo Uceda
Coordinadora de Libertades Informativas: Mayumi Ortecho

Acceso a la Información Pública:

En el año 2002 se promulgó la Ley 27806, denominada Ley de Transparencia y Acceso a la Información Pública[108], la cual regula el mencionado derecho en todas las entidades públicas a nivel nacional y a todo nivel.

La Ley 27806 es una norma de carácter general y de aplicación obligatoria a toda entidad pública sin excepción. Asimismo, es aplicable a los tres poderes del Estado y demás organismos constitucionales.

La Ley de Transparencia y Acceso a la Información Pública contiene las políticas generales en materia de transparencia, uniformiza el procedimiento de solicitud de acceso a la información pública en todas las entidades públicas, y establece altos estándares a ser cumplidos por los funcionarios correspondientes.

Dicha ley no establece una institución que sea la encargada de manera expresa y específica de la aplicación y control de la normativa del acceso a la información pública. Sin embargo, en la práctica, la Defensoría del Pueblo, en el marco de sus funciones constitucionales generales de defensa de los derechos constitucionales y fundamentales, así como de supervisión del cumplimiento de las funciones de la administración estatal, ha asumido algunas funciones de supervisión del cumplimiento de la normativa de Acceso a la Información Pública (AIP).

En el ámbito del Poder Ejecutivo nacional, existen dos dependencias que si bien no constituyen en estricto organismos de aplicación y cumplimiento de la normativa sobre AIP, cumplen algunas funciones puntuales en materia de transparencia y acceso a la información pública. Se trata de la Secretaría de Gestión Pública y de la Secretaría de Coordinación, ambas pertenecientes a la Presidencia del Consejo de Ministros (PCM). Se trata de dos organismos dependientes de la Secretaría General de la PCM, instancia que a su vez depende de Presidente del Consejo de Ministros, por lo que las referidas secretarías forman parte del tercer nivel en la escala jerárquica de la PCM, institución que coordina a todos los órganos del Poder Ejecutivo.

La Secretaría de Coordinación tiene a su cargo la coordinación de la PCM con el Congreso de la República, los organismos constitucionales autónomos distintos al Poder Judicial y Ministerio Público, los organismos públicos descentralizados adscritos al Sector Presidencia del Consejo de Ministros, las entidades del Estado distintas al Poder Ejecutivo, las entidades gremiales y las demás entidades de la sociedad civil. Entre sus once funciones normativamente establecidas, tiene el encargo de *"recabar de todas las entidades de la Administración Pública la información sobre las solicitudes y pedidos de información atendidos y no atendidos, en el marco de la Ley de Transparencia y acceso a la información Pública y elaborar un informe anual a ser presentado al Congreso de la República*". Es decir, se

[108] http://www.peru.gob.pe/normas/docs/LEY_27806.pdf

encarga de acopiar la información de todas las entidades públicas para elaborar el Informe Anual al que se refiere el artículo 22° del TUO de la Ley N°27806.

Protección de Datos Personales:
El 02 de julio de 2011, se promulgó la Ley Nº 29733, Ley de Protección de Datos Personales[109] que regula el mencionado derecho en Perú.

La Ley Nº 29733 es una norma de carácter general, que tiene como objetivo el garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2º inciso 6º de la Constitución Política del Perú. La ley es bastante completa, define conceptos, establece procedimientos y ordena el manejo de la protección de datos en todos sus supuestos.

En cuanto al control, En su artículo 32º, la Ley establece que el órgano encargado de esa tarea es el Ministerio de Justicia, a través de la Dirección Nacional de Justicia. Es un órgano administrativo, pertenece al Poder Ejecutivo, tiene capacidad sancionadora y ha previsto detalles como la confidencialidad que deben guardar sus funcionarios.

Relación entre ambos derechos:

La relación entre ambas normativas tiene como sustento la calificación de pública que puede tener un determinado tipo de información sobre una persona en concreto. Es decir que la Ley de Protección de Datos busca salvaguardar el derecho a la intimidad reconocido en la Constitución, mientras que la Ley de Transparencia establece que en casos de acceso a la información pública, las excepciones deben ser las menores e incluso en un hecho referido a información personal, esta puede tener carácter público sin necesidad de permiso del propietario de la información. En este aspecto, ambas normas coinciden en que es el funcionario o el administrador de justicia quien, basado en un test de proporcionalidad y razonabilidad, debe buscar satisfacer ambos derechos. Sin embargo, el derecho de la sociedad a conocer información que considere relevante y que pertenezca al ámbito personal de una persona, prevalece.

En ambos casos, la norma prevé la presentación de informes para medir los avances y controlar el ejercicio de ambos derechos. En el caso de la Ley de Transparencia, la Presidencia del Consejo de Ministros, debe presentar el informe anual que el artículo 22° del TUO de la Ley 27806 le encarga con la finalidad de ser remitido al Congreso. En el caso de la Ley de Protección de Datos Personales, la norma menciona presentar informes periódicos sin especificar cada cuanto tiempo. Los informes los presenta la Dirección General de Justicia al Ministerio de Justicia.

Cabe mencionar además que la Constitución ha previsto el recurso de hábeas data para la protección constitucional de estos dos derechos.

En primera instancia, se encuentra la vía administrativa. La autoridad que posee la información es la que determina si esta es pública o reservada. Existe un mecanismo de apelación ante una primera respuesta. Agotada esta vía, ambos derechos pueden ser defendidos en vía judicial, la cual puede terminar en el Tribunal

109
http://www.municipioaldia.com/facipub/upload/fpmod_boletin/normas/1219/file_norma/Ley_29733.pdf

Constitucional, que es el máximo ente de interpretación constitucional en nuestro país. Sus decisiones son vinculantes y crean precedente.

Casos prácticos:

Existe en la jurisprudencia dos casos relevantes donde se han visto en conflicto ambos derechos. El primero recae sobre la sentencia 1480-2003-HD/TC[110], que hace referencia a una solicitud de acceso a la información pública que buscaba se entregue al solicitante, la historia clínica de un paciente de un hospital público. En este caso, se argumentó que el pedido era infundado dado que dicha información y toda la información perteneciente a historiales clínicos (banco de datos) es considerada información privada.

Por otro lado, tenemos el caso que concluyó con la sentencia 5379-2006-PHD-TC[111], en el cual un profesional, mediante solicitud de acceso a la información pública, solicitó a la Morgue de Lima, el registro con el nombre de los fallecidos en un determinado accidente automovilístico. El pedido fue negado en todas las instancias, dado que se consideró que esa base de datos estaba también protegida por el derecho a la intimidad de las personas.

Jurisprudencia:

En cuanto a jurisprudencia relevante en la materia, contamos con la sentencia 05060-200-HD/TC[112], emitida el 06 de julio de 2011 por el Tribunal Constitucional donde se señala que:

"se ha de concluir que la información contenida en la base de datos de un registro de requisitorias es pública y, por consiguiente, ingresa dentro del alcance del ejercicio del derecho fundamental de acceso a la información pública, reconocido en el artículo 2.°, inciso 6, de la Constitución. En tal sentido, el emplazado, al negarse a brindar la información referida a si don Carlos Eduardo Valdizán Paredes tiene alguna requisitoria (orden de ubicación y captura), identificando (en caso de que así sea) al órgano jurisdiccional que emitió la orden, así como la fecha de su emisión y el número del expediente judicial del que proviene, con el costo que suponga el pedido, ha violado el derecho fundamental de acceso a la información pública del demandante, por lo que corresponde estimar la demanda."

Hay que considerar que en este caso, las instancias inferiores consideraron la información solicitada como personal y protegida por el derecho a la intimidad.

Por otra parte, hasta la fecha la postura de organismos que administran justicia ha sido priorizar el derecho a la intimidad por sobre el derecho de acceso a la información pública. Esto se ve reflejado en sentencias como:

- Acceso a información sobre titulares de cuentas bancarias, extractos de su movimiento y de documentos proporcionados por su titular (STC No. 2237-2003-HD/TC[113]).

[110] http://www.justiciaytransparencia.pe/upload/iblock/fac/1480-2003.pdf
[111] http://www.justiciaytransparencia.pe/sentencias/categoria_juridica/index1.php?SECTION_ID=282&ELEMENT_ID=889
[112] http://www.tc.gob.pe/jurisprudencia/2011/05060-2009-HD.html
[113] http://www.tc.gob.pe/jurisprudencia/2003/02237-2003-HD.html

- Acceso a información detallada relativas a ahorros, colocaciones, depósitos, e inversiones así como ingresos de origen privado de funcionarios públicos. (derecho a la intimidad) (STC No. 04407-2007-PHD/TC[114]).

Rol de la Sociedad Civil:

Debido a la reciente promulgación de la Ley de Base de Datos y el aún incipiente desarrollo sobre el tema no se han podido identificar organizaciones de a sociedad civil peruana que se encuentre trabajando en la promoción de la protección de datos.

Por su parte, en lo referido al derecho de Acceso a la Información Pública y la transparencia, se pueden identificar varias organizaciones de la sociedad civil que promueven ese derecho. Entre ellas se puede mencionar instituciones como el Instituto Prensa y Sociedad – IPYS, Transparencia, Ciudadanos al Día, Proética, entre otros.

[114] http://www.infopublica.pe/?pag=jurisprudencia&idn=20

1.16. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN REPÚBLICA DOMINICANA

Participación Ciudadana
Director del Área de Transparencia
y Gobierno: Carlos Pimentel

Acceso a la Información Pública:

En República Dominicana el derecho de acceso a la información publica se encuentra normado por la Ley General de Libre Acceso a la Información Pública, No. 200-04 y el Reglamento No.130-05[115].

La característica principal de la Ley General de Libre Acceso a la Información Pública es que cumple con los requisitos o elementos esenciales que debe tener toda normativa de acceso a información, tales como a) el reconocimiento que toda persona puede solicitar información; b) que existe una obligación de publicación previa; c) que la denegación de información debe responder a razones limitativas indicadas en dicha normativa; d) establece taxativamente las excepciones o limitaciones para acceder a información pública; e) Dispone de plazos breves para la entrega de información y la posibilidad de interponer recursos administrativos y judiciales ante la denegación de la misma.

La mencionada ley alcanza a toda información que produzca el Estado a través de sus instituciones u organismos y toda actividad que implique el uso de fondos públicos- desde las actividades de las instituciones hasta los Partidos Políticos-.

Por otra parte, la Ley General de Libre Acceso a la Información Pública no establece un órgano de control para la aplicación de la misma, aunque cabe señalar que existen recursos administrativos y judiciales que de manera difusa ejercen la salvaguarda del derecho de acceso a información.

Protección de Datos Personales

República Dominicana no cuenta con una ley que regule el derecho de protección de los datos personales. Sin embargo, se puede mencionar la existencia de un anteproyecto de ley que procura la protección de datos personales, aunque el mismo no ha sido objeto de debate público.

Relación entre ambos derechos

En cuanto a la relación de ambos derechos se puede mencionar que la ley de Libre Acceso a Información Pública restringe el acceso a información, en una de sus disposiciones, cuando se refiera al acceso a datos personales que pudiera considerarse como una intromisión a la privacidad personal. De todos modos, al no ser la protección de datos personales objeto de una legislación independiente se podría llegar a interpretar que el acceso a la información es un derecho preponderante sobre el acceso a datos personales.

Casos prácticos y Jurisprudencia

[115] http://www.dgii.gov.do/legislacion/LeyesTributarias/Documents/Ley200-04.pdf
http://onapi.gob.do/pdf/marco-legal/trasparencia/decreto-130-05.pdf

No se conocen casos o jurisprudencia en relación a la relación entre el derecho de Acceso a Información Pública y la protección de los Datos Personales en República Dominicana.

Rol de la Sociedad Civil

No se conocen iniciativas, en República Dominicana, desde la sociedad civil para promover la protección de datos personales.

1.17. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN URUGUAY

Centro de Archivos y Acceso a la Información Pública (CAInfo)
Director Ejecutivo: Edison Lanza

<u>Acceso a la Información Pública</u>:

En Uruguay el derecho de acceso a la información pública está regulado por la ley 18.381.
La ley establece un procedimiento administrativo específico para acceder a información pública regulado 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 el interesado solo pagará el precio del costo del soporte, sin ningún arancel adicional (art. 17). La definición incluye la prohibición a texto expreso de no cobrar ningún otro costo que el del soporte en el que se entrega la información, lo que la administración imponga una barrera económica al acceso y se la protege a su vez 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 que habilita a declararla 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.

La ley 18.381 estableció la creación de la Unidad de Información (UAIP) –un organismo descentralizado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic)[i] con 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, protegerán su independencia, eficacia, objetividad e imparcialidad. Estos dos individuos durarán cuatro años en sus cargos, y podrán 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 estos dos miembros (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 la total autonomía del Consejo del gobierno. (Fumega, Lanza y Scrollini, 2010).[116]

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, alguien del sector privado 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. Asimismo, a pesar de contar con independencia técnica, la UAIP no cuenta con presupuesto propio. Actualmente el Consejo de la UAIP está intentando trabajar sobre este tema:
"Estamos tratando de ver cómo se puede armar explícitamente el presupuesto. Hicimos un plan de trabajo, para atender las necesidades presupuestales y después vamos a ver si eso se explicita en el presupuesto [de Agesic]" (Funcionario de la Unidad de Acceso a la Información Pública).

Protección de Datos Personales:

La ley 18.331 regula la protección de los datos personales en Uruguay.
La LPDP regula el tratamiento de los repositorios que contengan datos personales sensibles. De acuerdo a esta norma las personas públicas o privadas deberán registrar sus bases de datos, ante la Unidad de Protección de Datos Personales en el Registro de Bases Personales de la Unidad Reguladora de Control de Datos Personales (URCDP)[117].

La misma norma define las distintas categorías (artículo 18) de datos personales (personales y sensibles), su forma de recolección, acceso y transmisión y también reguló la acción de habeas data (artículos 37 y siguientes): "Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder".

Según la LPDP y otras experiencias en el derecho comparado[118], hay una serie de datos personales que no tienen especial protección y por ende pueden ser publicitados y abierto al acceso público por parte de los organismos estatales, aún cuando están asociados a la percepción de recursos públicos.

[116] Centro de Archivos y Acceso a la Información Pública (2011). "Venciendo la Cultura del Secreto".
[117] Artículo 8 y sgtes. de la Ley 18.331.
[118] 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.

CAinfo ha propuesto la siguiente clasificación en oportunidad de estudiar algunos casos específicos como los del Ministerio de Desarrollo Social (Mides)[119]:

i) 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) Constituyen datos "especialmente protegidos": Según la LPDP y siguiendo el derecho comparado, 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 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.

El órgano de control de la protección de datos personales funciona como un espejo de la unidad de control de acceso a la información pública. En el caso de la protección de datos la ley creó la URCDP (Unidad Reguladora y de Control de Datos Personales) De hecho, el director de Agesic integra tanto la URCP como de la Unidad de Acceso a la Información Pública es el mismo. Este diseño institucional facilita la coordinación, consulta y deliberación cuando ambas unidades se enfrentan a un problema de definición de los límites y armonización de ambos derechos.

Relación entre ambos derechos:

La ley PDP se aprobó como parte de un mismo sistema de protección de derechos relacionados con el manejo de la información, el Parlamento aprobó la Ley de Protección de Datos Personales (LPDP – N° 18.331) en forma contemporánea a la ley de AIP (18.381).

Como se dijo, 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 del Estado que pueda vulnerar datos personales sensibles.

El sistema de leyes de Acceso a la Información Pública y la Protección de Datos Personales aprobado en Uruguay prevé dos mecanismos para dirimir conflictos y

[119] Centro de Archivos y Acceso a la Información Pública: Informes de Auditoria- Cumplimiento y funcionamiento de la Ley 18.381 "Derecho de Acceso a la Información Pública" en el Ministerio de Desarrollo Social (www.Mides.gub.uy, 2010)

armonizar ambos los derechos en juego entrono al acceso a la información y la protección de datos personales.

Por una parte la institucionalidad creada por ambas normas, que establecieron dos unidades de control, una para Acceso a la Información y otra para Protección de Datos Personales, al tiempo que el director de la AGESIC forma parte de ambos Consejos Directivos, ha llevado a desarrollar la práctica de la consulta en casos dónde se dirimen denuncias que incluyen conflictos entre ambos derechos. Aunque las resoluciones emitidas por cualquiera de estas dos unidades no son vinculantes, si generan estándares que siguen la mayor parte de los organismos públicos.

En segundo lugar, la Acción de Acceso a la Información Pública permite plantear una reclamación judicial sumaria y efectiva para dirimir un conflicto entre el acceso a la información y la protección de datos personales. Las sentencias emitidas por el juez competente en esta materia es vinculante y apelable ante un tribunal superior.

Casos prácticos:

Deudores BCU y datos personales de la base de casos del Poder Judicial. Dos casos tomaron notoriedad bajo la vigencia de las leyes de Acceso a la Información Pública y Protección de Datos Personales. Uno refiere a la publicación por parte del Banco Central del Uruguay del nombre, la categorización y el monto adeudado por cada persona física o jurídica deudora (en situación de incumplimiento) del sistema financiero. La publicación en la web del organismo de estos datos personales levantó una polémica sobre la necesidad o no de mantener reserva de los mismos. La autoridad monetaria definió la situación alegando que tiene habilitación legal expresa para proceder a publicar esa base de datos. Finalmente se estableció que para acceder a la denominada "central de riesgo" la URDPDP requiere que los solicitantes se registren en la web del Banco Central.[120]

El Poder Judicial se negó durante años a publicar y dar acceso al público general a su base de datos sobre casos tramitados en las diversas materias y sedes judiciales. Unicamente franqueaba el acceso a la información cuando la solicitud sobre el trámite judicial era realizada por el directamente interesado o su asesor letrado. Ante diversos reclamos de la sociedad civil y un dictamen contrario de la Unidad de Acceso a la Información Pública, el Poder Judicial conformó una comisión con integrantes de la sociedad civil que finalmente armonizó el acceso a la información pública y los datos personales. La Suprema Corte de Justicia habilitó mediante una resolución expresa el acceso a la información pública de la Oficina Distribuidora de Turnos del Poder Judicial (ORDA). La información deberá ser entregada en el momento de la consulta o a más tardar en tres días hábiles.[121] De este modo, se abrió el acceso a la información sobre los expedientes judiciales tramitados en Montevideo.

Muchas de las situaciones conflictivas entre Acceso a la Información Pública y Datos personales en Uruguay han tenido que ver mayormente con datos de personas jurídica en poder de organismos estatales. De este modo, es frecuente que el Estado se ampare en la ley de protección de datos personales para negar información que requieren los ciudadanos para proteger el medio ambiente o para investigar sobre diversos asuntos.

[120] http://consultadeuda.bcu.gub.uy/consultadeuda/
[121] Acordada de la Suprema Corte de Justicia N° 7707 de 30 de junio de 2011.

Recientemente la Unidad Reguladora de Servicios de Comunicación Audiovisual se negó a informarle a integrantes del sindicato de periodistas, la cantidad de abonados que cada empresa de televisión habilitada tiene en los distintos departamentos del país. Respondió que se trataba de datos sensibles por parte de la empresa, Este caso se encuentra a consideración de la Justicia.

Jurisprudencia:

En el siguiente caso una empresa agropecuaria solicitó que se declararan datos personales sensibles, y por ende reservados, una serie de formularios que contienen los registros individualizantes de las transacciones comerciales de empresas que comercializan determinadas semillas de maíz transgénico.

La sentencia hace lugar parcialmente a la solicitud de reserva de las empresas. Aduce que los datos genéricos sobre los volúmenes de maiz transgénico que se comercializan son públicos, pero deben disociarse de aquellos que refieren a los volúmenes que comercializa casa empresa.

"*Se trata entonces de lograr un equilibiro entrela exhibición de datos necesarios para la protección del medio ambiente para lo que median razones de interés general y el derecho de los accionantes de que no se divulgue información relativa a las operaciones comerciales realizadas, en cuánto a los derechos de las empresas y los productores tienen también protección constitucional*"[122]

Resolución de la Unidad de Acceso a la Información Pública No. 26/2010, evacuando una denuncia sobre la falta de acceso a la información de determinados datos en poder del Poder Judicial relacionados con expedientes de acciones de acceso a la información:

1. Que el Poder Judicial se encuentra alcanzado por las obligaciones establecidas en la ley de Acceso a la Información Pública, Ley N° 18.381 y por tanto debe dar cumplimiento a las mismas.

2. Sugerir al Poder Judicial que entregue al denunciante la información requerida, en el caso que la Oficina Receptora y Distribuidora de Asuntos (ORDA) tenga organizados los juicios por asunto. Asimismo, elaborar versiones públicas de los documentos y en el caso que los mismos contengan datos personales proceder a su disociación. [123]

Rol de la Sociedad Civil:

El Instituto de Derecho Informático de la Facultad de Derecho de la Universidad[124] de la República es la organización que ha estudiado y promovido en profundidad la protección de datos, junto a otros aspectos relacionados con el derecho informático. Básicamente se trata de un instituto académico, formado por docentes interesados en esta disciplina, que desarrolla foros, seminarios y publicaciones.

[122] Sentencia 273/10 del Tribunal de Apelaciones en lo Civil de 4° turno. Autos: Fanidur S,A y otros contra
Ministerio de Vivienda, Ordenamiento Territorial y Medio Ambiente.Habeas Data Ley 18.331. https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=1aSwuTTBWztj2eeKnv2KlBTEvJwR9nt_alBDn7rSkUAJL-oKqODT7Mqeja958&hl=en_US

[123] Ver resolución en: http://www.informacionpublica.gub.uy/sitio/descargas/consejo-resolucion/2010/resolucion-26-010_14-09.pdf

[124] http://www.fder.edu.uy/contenido/idi/

1.18. EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN VENEZUELA

Transparencia Venezuela
Directora Ejecutiva: Mercedes De Freitas

Acceso a la Información Pública:

En Venezuela no existe una ley nacional que regule el derecho de acceder a la Información Pública. Sin embargo, el pasado 31 de marzo, un grupo de diputados de la Comisión de Contraloría introdujo un Proyecto de Ley de Acceso a la Información Pública que espera ser aprobado para su pronta discusión. Dicho instrumento se basa en la Ley Modelo de la OEA y su Guía de Implementación. Aún más, durante mayo y junio de 2011, la Coalición Proacceso[125] desarrolló una serie de eventos que sirvieron de promoción y consulta del proyecto de ley en distintos sectores y regiones del país.

Actualmente el derecho de Acceso a la Información está protegido por los artículos 28, 51 y 143 de la Constitución de la República Bolivariana de Venezuela[126]. El artículo 51 establece que *"toda persona tiene el derecho a representar o dirigir peticiones ante cualquier autoridad, funcionario público o funcionaria pública sobre los asuntos que sean de la competencia de éstos o éstas, y de obtener oportuna y adecuada respuesta*". Entretanto, el artículo 143 expresa que los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública. Refiere también que tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática. Además expresa que "*no se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad*".

Asimismo, en Venezuela se cuenta con basamento jurídico que detalla los procedimientos a realizar para hacer peticiones de información, en cuanto a plazos, denegación, silencio administrativo, etc.

- **LOPA**: Ley Orgánica de Procedimientos Administrativos (Art. 2,3, 5, entre otros);
- **LOAP**: Ley Orgánica de Administración Pública (Art. 9);
- **LOPC**: Ley Orgánica de Poder Ciudadano (Art. 28); y
- Decreto con Fuerza de Ley Orgánica de Planificación.

Sin embargo, en 2010 se aprobaron dos leyes de opacidad, que limitan en derechos de acceso a la información:

1. Creado por Decreto Presidencial, el Centro de Estudio Situacional de la Nación (CESNA), es un organismo que tiene entre sus funciones la revisión de toda información pública y decidir sobre la clasificación de reserva, con criterios arbitrarios, no definidos con claridad en el decreto.
2. Se aprobó la *Normativa para la Clasificación y Tratamiento de la Información en la Administración Pública* (Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.578, del 21 de diciembre de 2010), que ordena clasificar las informaciones que reposen en instituciones públicas

[125] http://www.proacceso.org.ve/
[126] http://www.tsj.gov.ve/legislacion/constitucion1999.htm

según su uso como: "uso público", "uso interno", "confidencial" y "extremadamente confidencial". La información de “uso público” para ser difundida o entregada requiere la aprobación “formar” y directa de la máxima autoridad del órgano público.

Sin embargo, se han visto significativos progresos en la garantía al acceso a la información en el ámbito local, con la aprobación y promulgación de ordenanzas de transparencia y acceso a la información pública en seis municipios (San Diego, Chacao, Baruta, Maneiro, Campo Elías y Los Salías) y en cinco estados (Zulia, Nueva Esparta, Lara, Anzoátegui y Miranda) que han dado resultados positivos en la gestión y participación de la ciudadanía.

A pesar de que no existe una legislación especial nacional en materia de acceso a la información pública, se cuenta con el reconocimiento del derecho de petición, la obligación de los funcionarios de proveer la información veraz y oportunamente, el principio de rendición de cuentas.

En las legislaciones estadales y ordenanzas municipales se regula más específicamente el derecho, incluyendo las sanciones a los funcionarios que no den acceso a la información, la calificación de reserva de la información, la información mínima que debe difundirse proactivamente, las excepciones al acceso a la información pública, los plazos, etc.

Las normativas aprobadas en el país en el ámbito local se han caracterizado por ser instrumentos que ofrecen participación y control social a la comunidad fortaleciéndose la democracia e impulsando las buenas prácticas de los gobiernos locales. Asimismo, se ha logrado un mayor compromiso por parte de las autoridades regionales y locales, a dar respuesta a las solicitudes de sus ciudadanos.

Es conveniente destacar que no existe un órgano de control independiente que administre y haga seguimiento al cumplimiento de las leyes que regulan el acceso a la información pública. En este sentido son los organismos de administración de justicia del Estado quienes procesan los casos y toman acciones al respecto. De todos modos, los entes públicos bajo las jurisdicciones de las leyes estadales y las ordenanzas municipales están obligados a tener funcionarios que se encarguen de procesar las solicitudes de información, pero no tienen un ente de control propiamente dicho.

Protección de Datos Personales:

No existe una normativa especial que regule la Protección de Datos Personales. No obstante, la Constitución de la República Bolivariana de Venezuela (CRBV) en su artículo 60 establece: “*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 para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos*”.

Asimismo, el artículo 28 (CRBV) indica que: “*Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente,*

podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

Por otra parte, la Ley Orgánica del Tribunal Supremo de Justicia en su Artículo 167 establece que "*Toda persona tiene derecho a conocer los datos que a ella se refieran así como su finalidad, que consten en registros o bancos de datos públicos o privados; y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes. El Habeas Data sólo podrá interponerse en caso de que el administrador de la base de datos se abstenga de responder el previo requerimiento formulado por el agraviado dentro de los veinte días hábiles siguientes al mismo o lo haga en sentido negativo, salvo que medien circunstancias de comprobada urgencia*".

En el año 2004 la comisión de Ciencia, Tecnología y Medios de Comunicación Social, de la Asamblea Nacional (Poder Legislativo) hizo una consulta pública de un proyecto de Ley de Protección de Datos y Hábeas Data, promovido por el Diputado Guillermo Berdugo (Acción Democrática), pero no prosperó.

Casos prácticos

Si bien no existen leyes que rijan los derechos al acceso a la información pública y a la protección de datos personales, en Venezuela, el Tribunal Supremo de Justicia ha conocido casos en los que se ha evidenciado un uso inadecuado de datos públicos, que han sido vinculados con datos personales, como la orientación política de una persona, con fines discriminatorios.

Un ejemplo de lo mencionado es el caso Gustavo Azocar versus la página web "LUISTASCON.COM[127]": El 6 de mayo de 2004, el ciudadano Gustavo Azocar elevó ante el Tribunal Supremo de Justicia, una acción de habeas data para solicitar la destrucción de sus datos contenidos en la página electrónica denominada "LUISTASCON.COM", creada por el ciudadano Diputado Luis Tascón; que contenía los datos de más de 3 millones de personas, que consignaron sus firmas para solicitar la activación de un referendo revocatorio para el Presidente Hugo Chávez.

El caso fue admitido por la Sala Constitucional del Tribunal Supremo de Justicia, el 14 de septiembre de 2004[128]. Si bien en Venezuela los datos del registro electoral se encuentran publicados en la página del Consejo Nacional Electoral[129], en este caso llevado ante el TSJ, el ciudadano Gustavo Azocar reclamaba la destrucción de sus datos publicados en la referida página web en la que se acusaba a todas las personas presentes en dicho listado como parte de un "fraude". Azocar solicitó la destrucción de ese archivo y la desincorporación de sus datos del mismo, al considerar que esa página era contraria a principios constitucionales.

Jurisprudencia:

[127] Actualmente fuera de funcionamiento
[128] La decisión sobre admisión del caso se puede ver en: http://www.tsj.gov.ve/decisiones/scon/Septiembre/2151-140904-04-1154%20.htm
[129] http://www.cne.gob.ve/web/registro_electoral/mayo_2010/index.html

En cuanto a la jurisprudencia en relación a la entrega de información considerada como dato personal, se puede mencionar la sentencia de la Corte Primera de lo Contencioso Administrativo del 01 de agosto de 2000, confirmada por la Sala Constitucional del Tribunal Supremo de Justicia en sentencia de fecha 20 de enero de 2004, en la cual se le exige al Vice-Ministerio de Turismo del Ministerio de Industria y Comercio y a la Corporación de Turismo de Venezuela conceder documentos contentivos de datos personales de la sociedad Olimpia Tours and Travel, C.A.

"Estima la Corte que la empresa accionante tiene derecho de ser informada del contenido de tales actas siempre y cuando '...estén directamente interesados o interesadas...' tal como lo expresa la Carta Magna; es por ello que al haberle impedido CORPOTURISMO a la presunta agraviada conocer el contenido de las mismas le ha cercenado su derecho a la información sólo en la medida en que su interés esté plenamente establecido y así se declara."

Asimismo, es conveniente mencionar la sentencia de la Sala Constitucional del Tribunal Supremo de Justicia de fecha 7 de febrero de 2007 en la cual se ordena a la Oficina de Control de Estudios de la Escuela "Luis Razetti" de la Facultad de Medicina de la Universidad Central de Venezuela que permita a William Uribe la revisión de su expediente académico, la cual había sido negada bajo el pretexto de que era necesario un procedimiento administrativo para mostrar dicha información personal[130].

"*De la norma que precede no se observa, como lo interpretó la Corte Segunda de lo Contencioso Administrativo, que para su violación deba existir "necesariamente, la instauración de un procedimiento administrativo". Así, el hecho de que se supedite la vulneración al derecho a la información a la sustanciación de un procedimiento administrativo, equivale a la imposición de una limitación, de manera infundada, a un derecho constitucional, toda vez que la regla no circunscribe el derecho sólo para los casos en que la información que se requiera provenga, necesariamente, de las actas que conforman el expediente que recoge el trámite administrativo. Por el contrario, expresamente hace referencia al acceso a los archivos y registros administrativos y dispone las limitaciones aceptables en casos que preceptúa*."

Rol de la Sociedad Civil:

El tema de protección de datos personales ha cobrado mayor fuerza en Venezuela durante los últimos meses con la proximidad del inicio del XIV Censo Nacional de Población y Vivienda 2011, que llevará a cabo el Instituto Nacional de Estadística y al que un alto porcentaje de personas ha manifestado no tener confianza en el uso que se le dará a la información del Censo.

Dicha expectativa viene dada por la ausencia de una ley que regule la protección y reguardo de datos personales, lo cual genera que el venezolano no posea garantías sobre el uso de la información que ofrezca.

Ante esta inquietud, dirigentes del Partido Político Copei han manifestado públicamente su preocupación por varias de las preguntas planteadas en el cuestionario del Censo, las cuales catalogan de "invasivas, discriminatorias y

[130] http://www.tsj.gov.ve/decisiones/scon/Marzo/304-060301-00-2271.htm

violatorias de los artículos 2, 19, 22 y 23 de la vigente Constitución Nacional". En este sentido, han introducido un recurso de nulidad ante el Tribunal Supremo de Justicia (TSJ), que incluye una medida cautelar de suspensión, en contra de dichas interrogantes las cuales explican ser 1 de cada 10 y el censo consta de 68 preguntas agrupadas en tres temas: vivienda, personas y hogar.

Diferentes movimientos como el Frente Patriótico[131] también ha hecho un llamado a la población a no ofrecer información hasta tanto no se garantice el resguardo de los datos personales con una ley. Según afirman a través de un artículo publicado en su portal web: "*los venezolanos terminamos de perder el Derecho Universal a la Autodeterminación Informativa, que es algo que ya forma parte de la batería de Derechos Humanos internacionalmente reconocidos*"[132].

[131] http://www.frentepatriotico.com/inicio/?p=3746
[132] Ver: http://ticsddhh.blogspot.com/2011/07/porque-no-abrire-mi-puerta.html

1.19. CUADRO DE SÍNTESIS

Este cuadro ha sido construido con la información provista por las organizaciones que conforman la Alianza Regional por la Libre Expresión e Información.

	AIP (Acceso a la Información Pública)	PDP (Protección de Datos Personales)
Argentina	- Constitución Nacional http://www.senado.gov.ar/web/consnac/consnac.htm - Decreto 1172/03 http://www.infoleg.gov.ar/infolegInternet/anexos/90000-94999/90763/norma.htm	- Ley 25.326 de Protección de Datos Personales http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
Bolivia	- Constitución Política del Estado (CPE) (vigente desde 2009) http://www.oas.org/Juridico/mla/sp/bol/sp_bol-int-text-const.html - Dos decretos supremos (Decreto Supremo 28168, de 17 de mayo de 2005, y el Decreto Supremo 0214, de 22 de julio de 2009) que se complementan para definir el ámbito de los sujetos obligados. http://www.sns.gob.bo/documentacion/normativas/DS%2028168.pdf http://www.ypfb.gob.bo/documentos/2010_transparencia/normativa/decreto-supremo-0214-d.pdf	- Constitución Política del Estado (CPE) art. 21 numeral 2. Art. 130 http://www.oas.org/Juridico/mla/sp/bol/sp_bol-int-text-const.html - Código Civil art. 18 http://bolivia.infoleyes.com/shownorm.php?id=821 - Ley de Telecomunicaciones http://www.itu.int/ITU-D/treg/Legislation/Bolivia/ley_tlc.pdf
Brasil	-Artículo 5º XXXIII de la Constitución Federal de 1988. http://www.constitution.org/cons/brazil.htm - Leyes 11.111/2005: https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11111.htm y l8.159/1991: http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%208.159-1991?OpenDocument	-Constitución Federal y Codigo Civil http://www.constitution.org/cons/brazil.htm http://edutec.net/Leis/Gerais/ccb.htm
Chile	-Artículo 8 de la Constitución. http://www.resdal.org/Archivo/d000008d.htm - La ley Nº 20.285, sobre transparencia de la función pública y de acceso a la información de la Administración del Estado. http://www.leychile.cl/Navegar?idNorma=276363	- Ley Nº 19.628 “Ley sobre protección de la vida privada” http://www.leychile.cl/Navegar?idNorma=141599
Colombia	- Constitución Nacional: Artículo 74. http://www.bibliotecasvirtuales.com/biblioteca/constituciones/Colombiana/index.asp	- Constitución Nacional: Artículo 15. - Ley 1266 de 2008 que regula el derecho al habeas data.

	- Ley 57 de 1985 (publicidad de los actos y documentos oficiales) https://www.privacyinternational.org/countries/colombia/ley57-foi.doc	http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html - Proyecto de ley estatutaria No.184 de 2010 (se encuentra actualmente en control previo por parte de la corte constitucional) http://www.habeasdata.org.co/wp-content/uploads/2010/12/Informe-Conciliación1.pdf
Costa Rica	- Constitución Nacional: Art. 30. http://www.constitution.org/cons/costaric.htm	**-** Ley de protección de la persona frente al tratamiento de sus datos personales - Expediente no. 16679 (se encuentra en tramite de publicación y deberá ser reglamentada) http://www.conare.ac.cr/proyectos/16679%20dic.htm
Ecuador	- Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada en el Registro Oficial Suplemento 337 del 18 de Mayo de 2004. http://www.transparencia.espol.edu.ec/documentos/L_acceso.pdf	- Constitución de la República del Ecuador http://www.oas.org/juridico/mla/sp/ecu/sp_ecu-int-text-const.pdf
El Salvador	- Ley de acceso a la Información Publica (Decreto No. 534) LAIP http://www.soportelinuxdeguate.com/cms/attachments/081_LEYDEACCESOALAINFORMACIONELSALVADORDECRETO534.pdf	- Ley de acceso a la Información Publica (Decreto No. 534) LAIP Titulo III. http://www.soportelinuxdeguate.com/cms/attachments/081_LEYDEACCESOALAINFORMACIONELSALVADORDECRETO534.pdf
México	Ley Federal de Transparencia y Acceso a la Información Pública http://www.ifai.org.mx/transparencia/LFTAIPG.pdf	Ley Federal de Protección de Datos http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010
Nicaragua	- Ley de Acceso a la Información Pública. N. 621 http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2?OpenDocument	Constitución Política, art. 26 http://www.resdal.org/Archivo/d0000027.htm - Ley de Acceso a la Información Pública. N. 621 en su art 4: http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2?OpenDocument
Paraguay	- Constitución Nacional (art. 26, 28, 45 y 137) http://www.constitution.org/cons/paraguay.htm - Art. 68 de la ley orgánica municipal 3966/10 http://www.decidamos.org.py/index.php?option=com_k2&view=item&task=download&id=49&Itemid=31	- Ley 1682/01 reglamenta la Información de Carácter Privado con las modificaciones introducidas por la ley 1969/02: http://www.morinigoyasociados.com/todas_disposiciones/2001/leyes/ley_1682_01.htm
Perú	- Ley de Transparencia y Acceso a la Información Pública. Ley Nro. 27.806 http://www.congreso.gob.pe/archivo/normatividad/Ley_27806.pdf	- Ley 29733 de 2011 http://derechoperu.files.wordpress.com/2011/07/ley-29733.pdf

República Dominicana	- Ley General de Libre Acceso a la Información Pública 200-04 y su reglamento 130-05 http://www.dgii.gov.do/legislacion/LeyesTributarias/Documents/Ley200-04.pdf http://onapi.gob.do/pdf/marco-legal/trasparencia/decreto-130-05.pdf	-
Uruguay	Ley 18.381 de Derecho al Acceso a la Información Pública http://www.impo.com.uy/bancodatos/informacion.htm#e1	Ley 18.331 Protección de Datos Personales y Acción de "Habeas Data" http://www.datospersonales.gub.uy/sitio/leyes/Ley-18.331.pdf
Venezuela	- Constitución de la República Bolivariana de Venezuela (CRBV) artículos 28, 51 y 143 http://www.tsj.gov.ve/legislacion/constitucion1999.htm	Constitución de la República Bolivariana de Venezuela (CRBV) artículo 60 http://www.tsj.gov.ve/legislacion/constitucion1999.htm - Ley Orgánica del Tribunal Supremo de Justicia en su Artículo 167 http://imagenes.globovision.com/archivos/147810_leytsj2.pdf

Parte II

EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA

Helen Darbishire y Victoria Anderica Caffarena
Access Info Europe[133]

La protección de datos personales en Europa

La protección de datos se encuentra regulada en Europa en distintos tratados internacionales, del Consejo de Europa y de la Unión Europea, y al nivel nacional en cada país europeo con leyes que desarrollan los estándares mínimos establecidos en los tratados internacionales y de fuerza vinculantes para estos países.

Este estudio presenta la experiencia europea en cuanto a regulación de datos personales a nivel internacional y su desarrollo e implementación a nivel nacional. Esta experiencia europea puede servir como ejemplo para otras regiones que estén en proceso de adopción de este tipo de leyes.

A continuación se presentan las características mínimas que establecen estas leyes; como el acceso a los datos personales, el derecho a consultar, comentar, corregir y eliminar los mismos por parte de los interesados y los límites de traspaso de estos datos a terceros países con legislaciones y sistemas de protección de datos personales insuficientes.

Además se presentan la figura de las agencias de protección de datos, también a nivel nacional e internacional, que han jugado y siguen jugando un papel esencial en la implementación y desarrollo de la protección de datos en Europa.

El desarrollo del derecho en Europa

Desde el reconocimiento del derecho a la intimidad en el artículo 12 de la Declaración Universal de Derechos Humanos en 1948, la protección de datos personales como medida para proteger a la intimidad de las personas comenzó su andadura legislativa.
La formulación del derecho a la intimidad no menciona los datos personales sino la vida privada de una persona:

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

En Europa, el reconocimiento general de este derecho vino de la mano del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa (el equivalente Europeo de la Organización de Estados Americanos, que cuenta actualmente con 47 países miembros) en 1950. El Convenio establecía en su artículo 8 que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

[133] La traducción del inglés al español de este artículo ha sido realizada bajo la responsabilidad del equipo de traducción de la Secretaría Ejecutiva de la Alianza Regional.

Durante los años sesenta y setenta, gobiernos y empresas de los países de la Unión Europea empezaron a utilizar medios mecánicos para procesar información sobre personas: receptores de subsidios, clientes y otros contactos. La introducción de ordenadores en la vida diaria de entidades públicas así como empresas privadas aumentó la facilidad de recopilar y compartir con otros datos sobre personas privadas.
En 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), preocupada porque la disparidad entre leyes nacionales pudiera obstaculizar la libre circulación de datos personales, particularmente en sectores importantes de la economía como son la banca y los seguros donde las restricciones sobre el movimiento de información podría causar un trastorno en la economía, desarrolló una guía en un esfuerzo por crear un sistema de protección de datos exhaustivo para Europa.

Las Recomendaciones del Consejo de la OCDE sobre una guía que rija la protección de la privacidad y la circulación transfronteriza de protección de datos contenían siete principios que se convertirían en la base de los estándares internacionales para la protección de datos:

1. Notificación: los titulares de los datos deben ser notificados de que sus datos están siendo recolectados;
2. Motivo: Los datos recabados solo pueden ser utilizados para los motivos mencionados y no para otros motivos;
3. Consentimiento: Los datos no deben ser publicados sin el consentimiento del titular de los mismos;
4. Seguridad: Los datos recolectados deben ser guardados de forma segura para prevenir cualquier abuso;
5. Publicación: Los titulares de la información deben ser informados sobre quién está recabando sus datos;
6. Acceso: Los titulares de los datos deben poder acceder a sus datos y corregir cualquier dato incorrecto; y
7. Responsabilidades: Los titulares de los datos, deben poder acceder a un mecanismo para exigir el cumplimiento de estos principios a los responsables de tratar la información.

Al mismo tiempo, preocupado por el impacto negativo que podían tener las nuevas tecnologías informáticas sobre el derecho a la intimidad, el Consejo de Europa negoció y adoptó el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos persona, del 21 de enero de 1981. Este Convenio establecía en el artículo primero que habría que:

"…garantizar… a cualquier persona física… el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona".

Estos primeros reconocimientos, basados en la necesidad de reconocer el carácter fundamental de la protección de datos personales para asegurar un futuro desarrollo legislativo acorde con la importancia que se merece, se vieron pronto desarrollados por regulaciones más concretas que tanto a nivel internacional como a nivel nacional aseguraban el respeto del mismo.

El desarrollo de normas sobre protección de datos por la Unión Europea

La evolución de la Unión Europa como entidad económica y política integrada, y el consiguiente crecimiento del flujo de datos personales en Europa, hizo necesario asegurar una armonización de las normas para proteger la protección de datos personales dentro de la Unión.

Al mismo tiempo, la creciente cesión de competencias por parte de los Estados Miembros a la UE, hizo necesario regular en el seno de las instituciones europeas una normativa protección de datos personales y del tratamiento de los mismos.

Adoptando una nueva regulación en 1995, la UE presentaba la Directiva de Protección de Datos personales como medida necesaria para asegurar "el equilibrio entre un alto grado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea"[134].

Siguiendo el ejemplo de la OCDE y el Consejo de Europea, la UE desarrolló en su Directiva los principios que los estados miembros (hoy en día 27 países) tenían que transponer a su legislación nacional, asegurándose que las mismas normas serán de aplicación a todas las entidades públicas y privadas que manejan datos privados en la UE.

La directiva define claramente los datos personales 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."

Esta definición permite el procesamiento de datos para fines estadísticos siempre que no identifique a ningún individuo, para ello debe cumplir con los estrictos criterios establecidos en su artículo 7 que establece las bases para recopilar y procesar datos personales:

"Los Estados miembros dispondrán que el tratamiento de los datos personales solo pueda efectuarse si:
(a) El interesado ha dado su consentimiento de forma inequívoca;
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o;
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o;
d) es necesario para proteger el interés vital del interesado, o;
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o;
f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades

[134] EU Data Protection Directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."

La directiva prohíbe explícitamente procesar datos personales especialmente sensibles "*datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad*" a menos que el interesado haya dado su consentimiento expreso o que la información se encuentre ya en dominio público, o a menos que el interesado haya "publicado manifiestamente" los datos, este puede ser el caso de personajes famosos, políticos incluidos, que hayan hecho pública esta información utilizando por ejemplo algún medio de comunicación.

El derecho de los interesados a saber qué información se tiene sobre este y a rectificar información incorrecta es uno de los elementos esenciales de la legislación europea de protección de datos.

La normativa de la UE también prohíbe la transmisión de datos personales a países no miembros del Área Económica Europea a menso que este país asegure un adecuado nivel de protección de los derechos y libertades ligados a la protección de datos personales.

Hasta la fecha, solo un pequeño grupo de países han sido aprobados completamente: Suiza, Guernsey, Argentina, Isla de Man, Islas Faroe, Jersey, Andorra e Israel. Canadá ha sido aprobaba pero solo para cierto tipo de datos personales. Con los Estados Unidos existe un acuerdo especial sobre cierto tipo de datos, que incluye la transmisión de datos de compañías aéreas, que también pueden ser transferidos a Canadá y a Australia. Para otro tipo de datos y otros países, los titulares de los datos deben tomar precauciones especiales para asegurar la protección de sus datos.

La Unión Europea incluye algunas excepciones que permiten el procesamiento de datos personales en algunas ocasiones, entre otros, para proteger otros intereses protegidos como:
a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
g) la protección del interesado o de los derechos y libertades de otras personas.

Estos límites fueron considerados razonables cuando fueron aprobados en 1995 pero han sido puestos en cuestión por los grupos de libertades civiles y de derechos humanos tras la masiva recolección de datos personales aprobada por ley durante la implementación de las llamada "guerra al terrorismo".

Órganos garantes del derecho y garantías jurisdiccionales del derecho de protección de datos personales

Uno de los pilares de la protección de datos personales es la creación de un órgano independiente garante del derecho re querido por la Directiva Europea de Protección de Datos en todos los estados miembros de la Unión Europea.
Esta figura ha resultado ser esencial para la debida implementación de las leyes de protección de datos y sobre todo para el respeto generalizado de este derecho fundamental.

Todos los países miembros de la Unión Europea tienen un organismo especial que supervisa la protección de datos personales[135]. Cada Estado Miembro debe crear una autoridad supervisora, un órgano independiente que monitoree el nivel de la protección de datos en ese Estado Miembro, así como aconsejar al gobierno sobre medias administrativas y regulaciones e iniciar procesos judiciales cuando la regulación de protección de datos ha sido violada (art.28). Los individuos pueden interponer quejas ante esta autoridad supervisora o en los tribunales.
De forma similar, la UE cuenta con la figura del Supervisor Europeo de Protección de Datos (SEPD), creado en 2001. El SEPD tiene como mandato la responsabilidad de garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales[136]. La garantía de la protección de los datos personales en las instituciones europeas se ve completada por la protección judicial. Las decisiones del SEPD pueden ser recurridas ante el Tribunal de Justicia de la UE.

Los controladores de datos deben notificar a la agencia de protección de datos nacional antes de comenzar a procesar datos personales. La notificación debe incluir la siguiente información:

- *El nombre y la dirección del controlador de datos o su representante, si lo hubiera;*
- *el motivo para procesar los datos en cuestión;*
- *una descripción de la categoría o las categorías de los interesados y de los datos o categorías de datos que les afectan;*
- *los receptores o las categorías de receptores a los que los datos pueden ser publicados;*
- *las propuestas de transferencias de datos a terceros países;*
- *una descripción general de las medidas tomadas para asegurar la seguridad de los datos.*

Las agencias de protección de datos nacionales deben tener una serie de funciones y poderes básicos para garantizar el efectivo respeto de la protección de datos. La regulación europea también establece los estándares mínimos en su artículo 28:

"La autoridad de control dispondrá, en particular, de:
- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una

[135] Listado de los órganos independientes de los países miembros de la UE: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm
[136] Página oficial del SEPD: http://www.edps.europa.eu/EDPSWEB/edps/lang/es/EDPS

publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;
- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial."

Además la garantía de la protección de datos personales, se ve completada con la posibilidad de recurso de las decisiones de la autoridad de control lesivas ante los tribunales.

La protección de la privacidad y el derecho a la información

La protección de datos personales es una de las excepciones oponibles a una solicitud de acceso a la información pública, todas la leyes de acceso a la información de Europa así lo reconocen. Además el Convenio del Consejo de Europa sobre Acceso a Documentos Oficiales también lo reconoce en su artículo 3.1.f que la intimidad y otros intereses legítimos privados serán un límite al acceso a la información pública[137].

La mayor parte de la información en poder de organismos públicos no constituye datos personales, sin embargo, un número significativo de documentos, bases de datos y otros dispositivos de guarda de datos contiene nombres y otras informaciones sobre individuos particulares. Algunos de estos datos están ya en el dominio público (por ejemplo, las direcciones de personas que pueden estar en los catastros o en los registros electorales) mientras que algunos de ellos son datos particularmente sensibles (por ejemplo, datos sobre el estado de salud de la persona).

Los conflictos surgen cuando la información personal, que inevitablemente, y de forma creciente en un estado de bienestar, forma parte de la gestión pública; es en ese punto en el que puede ser objeto de publicación. Para lidiar con estos conflictos, no existe una fórmula matemática sino que hay que estudiar cada caso por separado. Esta es un área compleja que en Europa sigue desarrollándose a través de la jurisprudencia y las decisiones de los comisionados de la información.

Una pregunta más profunda es qué es lo que un solicitante está autorizado a hacer con información obtenida a través de una solicitud de acceso y si esto eventualmente constituye procesamiento de los datos.

El derecho de acceso a la información

El derecho de acceso a la información ha sido reconocido a nivel internacional como un derecho fundamental, algo más tarde que el derecho a la privacidad y la protección de datos personales. En años recientes, la Corte Interamericana de Derechos Humanos (caso Claude Reyes vs. Chile, 19 de septiembre de 2006) y la jurisprudencia de la Corte Europea de Derechos Humanos (en particular en el caso Hungarian Civil Liberties Union vs. Hungary del 14 de abril de 2009) confirmaron el

[137] Convenio del Consejo de Europa: http://www.access-info.org/documents/Access_Docs/Advancing/Council_of_Europe/Convention_on_Access_to_Official_Documetnts_CofE._es.pdf

derecho de acceder a la información en poder de organismos públicos, especialmente cuando esta información está en manos de monopolios y es necesaria para el ejercicio del derecho a la libertad de expresión. En 2011 el Comité de Derechos Humanos de Naciones Unidas también reconoció el derecho del acceso a la información, y lo relacionó con el Artículo 19 que sostiene la libertad de expresión e información en la Declaración Universal de Derechos Humanos de 1948.

Ni el derecho al acceso a la información, ni el derecho a tener datos personales protegidos son derechos absolutos. Esto implica que ambos están sujetos a excepciones que surgen de los tratados internacionales, y que cuando ambos derechos entran en conflicto, será necesario establecer cuál de ellos prevalece.

Estándares internacionales del derecho de acceso a la información permiten limitaciones con una variedad de fundamentos, tales como seguridad nacional, protección de relaciones internacionales, secreto comercial y la integridad de investigaciones penales y procedimientos judiciales en curso. Estos son todos intereses legítimos. El único derecho fundamental que puede entrar en conflicto con el acceso a la informaicón es la protección de la privacidad.

La mayoría de la información en poder de organismos públicos no constituye datos personales, y los datos personales que se encuentren allí puede ser fácilmente neutralizados (tachados) del documento. Habrá, sin embargo, ocasiones en las que la información sobre individuos deberá ser hecha pública. Este es un caso particular, cuando la información se refiere a figuras públicas que ejercen poder o son responsables por fondos públicos.

Existe una considerable jurisprudencia de la Corte Europea de Derechos Humanos sobre el derecho de los medios de comunicación a publicar información sobre figuras públicas, cuando hay un interés público en el caso. Hay decisiones en casos de libertad de expresión, como el mencionado Hungarian Civil Liberties Union v. Hungary en el que consideró si la información sobre un miembro del parlamento constituía datos personales. La Corte tomó posición definidamente, sosteniendo que:

"*sería fatal para la libertad de expresión en la esfera de la política si las figuras públicas pudieran censurar a la prensa y al debate público en nombre de sus derechos personales, alegando que sus opiniones en asuntos públicos están relacionadas con sus personas y, por lo tanto, consituyen datos privados que no pueden publicarse sin su consentimiento*".[138]

En otras palabras, cuando la información requerida es sobre individuos particulares puede estar protegida, mientras que los estándares son significativamente diferentes si son individuos públicos, en cuyo caso la información debería proveerse. Esto es cierto aún para el caso en que la figura pública no haya dado su *consentimiento manifiesto* a que se "procesaran" los datos al hacerlos públicos.

El derecho de acceso vs. el derecho a la protección de datos

En países de Latinoamérica que ya tienen leyes de acceso a la información, la introducción de una legislación para la protección de datos se plantea de un modo inevitable la cuestión de si los datos deberían revelarse, dadas las restricciones en el

[138] Caso de *Társaság a Szabadságjogokért v. Hungary*, no. 37374/05, 14 Abril 2009, para 36

procesamiento de datos personales. La cuestión es si la publicación de datos constituye "procesamiento" y si, en caso de que sea sí, esto significa que los datos personales ya no pueden publicarse bajo la ley de acceso a la información.

Los estándares internacionales y las mejores prácticas de países que ya tienen leyes de acceso a la información y leyes de protección de datos personales pueden resultar guías útiles. Una serie de países en Europa se han ganado la reputación de saber encontrar un equilibrio adecuado para ambos derechos, incluyendo aquellos que tienen órganos de control responsable por proteger el acceso a la información y proteger los datos personales, como es el caso de Slovenia, Hungría, Suiza y Reino Unido. En particular, el Comisionado de Información del Reino Unido desarrolló fuertes posiciones en la jurisprudencia.

Un principio importante que fue establecido es que si los datos son recolectados por una autoridad pública para uno o más propósitos, la puesta a disposición de esos datos no viola el requerimiento de que no sean procesados de un modo incompatible con el o los propósitos para los cuales fueron recolectados.[139] En otras palabras, la puesta a disposición de datos de conformidad a una solicitud de acceso a la información es, usualmente, una parte inherente del propósito del funcionamiento del órgano público en cuestión, y de los propósitos para los cuales recolectó los datos.

La siguiente cuestión es si el procesamiento es "justo" y "legal". Tanto la Convención 108 del Consejo de Europa como la Directiva de la Unión Europea requieren que los datos sean procesados de un modo justo y legal (EU DIRECTIVE 95/46/EC, Article 6.1.a).

El procesamiento será normalmente legal a la luz de los principios internacionales de protección de datos personales si existió consentimiento. Por lo tanto, si la autoridad pública está inequívocamente segura de que el consentimiento fue dado para posterior puesta a disposición del público de todos los datos personales bajo la ley de acceso a la información, no son necesarias mayores consideraciones y los datos deben ser puestos a disposición.

El caso de que no haya existido un consentimiento no implica *per se* que se excluya la puesta a disposición de los datos. La autoridad pública tiene que considerar si la puesta a disposición de los datos es legal en el sentido de que sea consistente con un interés legítimo. La Directiva de la Unión Europea define estos casos como aquellos en que el procesamiento es necesario para la consecución de propósitos de interés legítimo perseguidos por la autoridad controlante o por tereceras partes a las que los datos le son revelados, excepto cuando estos intereses sean superados por intereses de derechos fundamentales y libertades del sujeto de los datos (EU Directive 95/46/EC Article 7.f).

El ejercicio del derecho de acceso a la información representa un interés legítimo aunque debe, por supuesto, equilibrarse con la protección de otros derechos. Así, es posible revelar datos personales en respuesta a un requerimiento de acceso a la información en tanto otros derechos sean respetados.

Caso de estudio:

[139] Ver por ejemplo la guía "The exemption for personal information" publicada por UK Information Commissioner's Office, Version 3 of 11 November 2008.

Un ejemplo de establecimiento del equilibrio mencionado viene del Reino Unido, en el caso del "Escándalo de los gastos"[140].
Este caso, tratado por el Tribunal de Información del Reino Unido, tres periodistas pidieron información sobre los gastos de diversos miembros del Parlamento. El tribunal decidió que la información contenida en los archivos de los gastos eran datos personales y, también, que había intereses públicos legítimos en juego: la transparencia, la rendición de cuentas y el seguimiento del gasto de fondos públicos. El Tribunal halló que aún cuando parte de la información remitía a la vida privada de miembros del Parlamento (tales como su casa y vida familiar, y sus finanzas personales), existía interés público en esta información. Sin embargo, consideró de modo distinto la información sobre la vida privada de otras personas (parejas, hijos) y datos sobre cuentas bancarias (sus números reales, que pueden crear riesgo de fraude)[141].

La misma clase de consideraciones debería hacerse cada vez que hay una solicitud de datos personales. Es necesario dar especial atención a las categoría especiales de información referidas en el texto, más arriba. Estas categorías de datos no deberían ser procesadas, como regla, y debería merituarse la protección especial y las medidas de seguridad.

Sin embargo, en algunos casos, aún los datos que caen en estas categorías podrían ser revelados, particularmente cuando existió consentimiento explícito o cuando la información es de dominio público. Un ejemplo podría ser cuando es públicamente sabido que un funcionario público es miembro de un sindicato, en cuyo caso no hay necesidad de exceptuar este dato.

De modo similar, para los funcionarios públicos es probable que su afiliación política sea conocida, pero esto no es necesariamente así para empleados públicos de menores rangos. Podrían existir fotos en los medios de comunicación de un ministro en un viaje oficial con su amante, y si el viaje fue hecho con fondos públicos y él o la amante viajaron en uso de esos fondos, sería inapropiado rechazar la publicación de esos datos basándose en la protección de la vida sexual del ministro o ministra. En cualquier caso, habría un interés público superador, la necesidad de transparencia en el gasto de fondos públicos.

Estos son sólo algunos ejemplos, las autoridades públicas deben encontrar el equilibrio justo en cada caso, incluyendo muchos casos de perfil más bajo. Es aquí cuando el rol de un comisionado de información puede ser particularmente valioso para asegurar que el equilibrio sea encontrado.

[140] Caso de Corporate Officer of the House of Commons vs. Information Commissioner and Brooke, Leapman, and Ungoed-Thomas [2008] EWHC 1084 (Admin)

[141] Finalmente el Parlamento fue moroso en la provisión de la información y fue filtrada, con muchos datos personales revelados también. Es una lección de lo que puede ocurrir si no se cumple con las órdenes judiciales de poner la información a disposición.

Parte III

EL ACCESO A LA INFORMACIÓN Y LA PROTECCIÓN DE DATOS PERSONALES EN ESTADOS UNIDOS DE AMÉRICA

Reporte para la Alianza Regional
facilitado por el **Cyrus R. Vance Center for International Justice of the New York City Bar**[142]

I. Introducción

a. El acceso a la información frente a la privacidad de los datos

En los Estados Unidos, la historia de la reglamentación sobre privacidad se ha caracterizado por la autorregulación del sector y la legislación reactiva[143]. *"La naturaleza exacta y el alcance del derecho a la privacidad [en los Estados Unidos], sin embargo, nunca han sido enteramente definidos"*[144]. Los representantes empresariales y quienes proponen incrementar el acceso a la información personal se apresuran a señalar los múltiples beneficios de la autorregulación y de un mayor acceso y uso de la información personal –como, por ejemplo, los números de seguridad social. El acceso a bases de datos computarizadas que contienen información de identificación permite que los organismos obtengan datos sobre los individuos que, de otra manera, no podrían ser localizados. Algunos de estos beneficios son: posibilitar que las agencias de la ley ejecuten sentencias; que los grupos de interés público hallen a niños desaparecidos; que los bancos, compañías de seguros y de crédito prevengan el fraude; que los periodistas brinden infor3mación precisa; que los abogados localicen a testigos e identifiquen a las partes involucradas; y que los ciudadanos encuentren a sus familiares perdidos[145].

En paralelo, hay quienes exigen una mayor protección de la información personal (incluso en los registros públicos) en vista del rápido desarrollo de las redes computarizadas y de Internet. Dada la facilidad con que la información se puede obtener, compartir y difundir a amplia escala geográfica, es factible que los errores sean replicados o magnificados, y así se dañe a un individuo por tiempo indefinido. La promulgación, por parte del Congreso, de la Ley de Gobierno Electrónico de 2002[146] es sólo un ejemplo de la reacción del Gobierno de los EE.UU. a los reclamos del público por mayores medidas de privacidad. La Sección 205(c)(3) requiere que la Corte Suprema de los EE.UU. establezca reglas *"para proteger la privacidad y la seguridad en cuestiones relacionadas con la clasificación electrónica de documentos y la disponibilidad pública… de los documentos clasificados por medios electrónicos"*.

b. La introducción de Internet

[142] La traducción del inglés al español de este artículo ha sido realizada bajo la responsabilidad del equipo de traducción de la Secretaría Ejecutiva de la Alianza Regional.
[143] Lauren B. Movius y Nathalie Krup, U.S. and EU Privacy Policy: Comparisons of Regulatory Approaches, 3 Int'l Journal of Comm. Volumen 169 (2009).
[144] Barry contra N.Y., 712 F.2d 1554, 1558 (2d Cir. 1983).
[145] 1 Ley de Seguridad y Privacidad de los Datos (Data Sec. & Privacy Law) § 7.45 (2011), citando el Informe al Congreso de la Comisión Federal de Comercio (FTC), Servicios de Referencia Individual (diciembre de 1997), Disponible en: http://www.ftc.gov/bcp/privacy/wksh97/irsdoc2.htm.
[146] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 44 U.S.C.A. § 101.

El deseo de salvaguardar la información personal no es un fenómeno nuevo. Pero la tecnología digital afecta a la privacidad de manera inédita, pues facilita y economiza la recolección, búsqueda, almacenamiento, concentración y comercialización de la información[147]. Los sistemas de información en red (NIS, por sus siglas en inglés) eran prácticamente desconocidos fuera de las universidades y los sectores gubernamentales. Hoy, estos sistemas vinculan a las computadoras entre sí, y las vinculan asimismo a una enorme cantidad de otros dispositivos, como teléfonos móviles, vehículos y electrodomésticos[148]. Cientos de millones de usuarios en todo el mundo ingresan regularmente a Internet –el NIS más conocido–, y millones de personas se conectan a su lugar de trabajo a través de redes de área local u otras similares. Las inquietudes con respecto a la privacidad provienen, en parte, del surgimiento de nuevas y sofisticadas tecnologías de recolección de datos y confección de perfiles de los usuarios. Con millones de servidores, cientos de millones de usuarios y una infinidad de redes secundarias, todas ellas accesibles mediante la conexión a Internet, las redes se han vuelto más valiosas y democráticas, pero también, inherentemente menos seguras[149]. La percepción del público con respecto a la privacidad del correo electrónico y la navegación también se ha corrido: hoy en día, es mucho más probable que los usuarios de Internet estén conscientes de las "*cookies*", los "*bugs*" y otras herramientas de recolección de información en la web. Una "*cookie*" es un mensaje que se coloca en un navegador de Internet, cuyo propósito es identificar al usuario y, posiblemente, confeccionar páginas web y publicidades a su medida. Un "*bug*" –también conocido, en términos técnicos, como "*clear GIF*" (gif transparente) o "*tracker GIF*" (gif rastreador)– es un gráfico en un sitio web o en un mensaje de correo electrónico diseñado para identificar a quien visita el sitio o lee el mensaje. Los *bugs* y otras etiquetas electrónicas se están convirtiendo en herramientas estándares de marketing en la web, y sus objetivos van desde la inocua medición del tráfico hasta la más invasiva recolección de datos personales.

c. El interés público como catalizador de la reglamentación en los EE.UU.

La preocupación del público por la erosión de la privacidad ha forjado un apoyo significativo a la regulación gubernamental de la información recolectada y difundida a través de Internet. En contraste, las empresas se han opuesto a estos reclamos inclinándose, en cambio, por la autorregulación mediante controles tecnológicos e independientes, además de otros medios. Hasta fines de la década de 1990, el Gobierno Federal se abstuvo mayormente de emitir reglamentaciones directas sobre la privacidad en Internet. Un estudio realizado por la Comisión Federal de Comercio (FTC, por sus siglas en inglés), dado a conocer en 2000, mostró que la mayoría de los sitios web examinados no cumplían con las disposiciones mínimas de privacidad recomendadas por la FTC[150]. Por consiguiente, a partir del año 2000, principalmente en función de las quejas del público y el fracaso de las empresas en autorregularse, creció el apoyo del Congreso y de la administración Clinton a una mayor reglamentación gubernamental de la privacidad *online*.

d. Privacidad de los datos en los EE.UU.

[147] Movius y Krup, *op.cit.*, pp 170.
[148] 1 Ley de Seguridad y Privacidad de los Datos (Data Sec. & Privacy Law) § 2:1 (2011).
[149] Ídem, § 2:2 (2011).
[150] Ver: Federal Trade Commission Division of Financial Practices, Bureau of Consumer Protection, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress 2 (Mayo 2000). Disponible en: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (visitado por última vez el 15 de septiembre de 2011).

No hay una sola ley en los EE.UU que provea un tratamiento exhaustivo de la protección de datos o de los asuntos de privacidad[151]. En este país, la legislación sobre protección de la privacidad no se ha desarrollado adecuadamente, y se puede caracterizar como una manta hecha de retazos (*patchwork)*[152]. Por lo tanto, la privacidad de los datos nunca es pensada en el vacío; *"siempre se la considera en el marco de un contexto social, político, económico y cultural específico"* [153].

El derecho de acceso a la información no está presente en la Constitución de los EE.UU. Sin embargo, otras libertades garantizadas por la Primera Enmienda –como la libertad de expresión, la libertad de prensa y el derecho a la reparación de agravios– implican inherentemente la responsabilidad y el derecho de los ciudadanos estadounidenses a cuestionar al Estado y a obtener información no censurada sobre su accionar.

Dado que el término "privacidad" no figura en la Constitución estadounidense ni en la Declaración de Derechos, este derecho no queda garantizado de manera directa por la Carta Magna. No obstante, sí está reconocido en diversos tratados internacionales. El artículo 12 de la Declaración Universal de los Derechos del Hombre y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas establecen, ambos, que *"nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques*". Un notable artículo del *Harvard Law Review* publicado en 1890 es reconocido ampliamente por haber establecido el derecho a la privacidad como una tradición de la *common law*[154]. En dicho artículo, Samuel Warren y Louis Brandeis definieron este derecho como "el derecho a que a uno lo dejen en paz" [155]. Ellos argumentaron que el derecho a la privacidad, que se desprende de la propiedad intelectual y artística en la *common law,* no se funda en el principio de protección de la propiedad privada, sino en el de "inviolabilidad de la persona"[156].

La falta de reglamentación uniforme sobre privacidad de los datos no ha impedido que las cortes estadounidenses emitieran fallos sobre el tema. El análisis al respecto por parte de la Corte Suprema de los EE.UU. se ha focalizado en el equilibrio entre el interés del individuo en proteger su información personal y el interés público en permitir el acceso gubernamental a los registros personales. En 1965, un fallo del Tribunal Supremo reconoció judicialmente el derecho implícito del individuo a la privacidad en relación al gobierno en un caso que despenalizaba el uso de dispositivos anticonceptivos[157]. La Corte resolvió que el derecho a la privacidad amparada por la cláusula del debido proceso de la 14.ª Enmienda de la Constitución[158] se extiende a la decisión de una mujer de interrumpir un embarazo,

[151] Jean Slemmons Stratford y Juri Stratford, Data Protection and Privacy in the United States and Europe, IASSIST Quarterly, Volumen 17 (1998).
[152] Movius y Krup, *op.cit.*, pp 174.
[153] Ídem, 171.
[154] "Common law" es ley desarrollada por jueces mediante decisiones de las cortes o tribunales similares, en lugar de a través de procesos legislativos o accionar del Poder Ejecutivo. El cuerpo de precedentes se denomina "common law" y normalmente condiciona las decisiones judiciales futuras.
[155] Samuel D. Warren y Louis D. Brandeis, "The Right to Privacy" Harvard Law Review Volumen 4 (1890): 193-220. [Nota de traducción: en español, se encuentra publicado como "El derecho a la intimidad"].
[156] Warren y Brandeis, *op.cit.*, pp. 205.
[157] Roe v. Wade, 410 U.S. 113 (1973).
[158] La cláusula de debido proceso de la 14.ª Enmienda prohíbe a los gobiernos locales y estatal privar a cualquier persona de "su vida, libertad o propiedad sin mediar el debido proceso legal".

pero que ese derecho debe sopesarse en función de dos intereses legítimos del Estado a la hora de reglamentar el aborto: la protección de la vida prenatal y la protección de la salud de la madre.

En el caso Whalen contra Roe, la Suprema Corte de los EE.UU. reconoció por primera vez el derecho a la privacidad de la información[159]. El fallo observó que la 14.ª Enmienda protegía dos tipos de intereses individuales: "*Uno es el interés individual en evitar la divulgación de cuestiones personales, y otro es el interés en permitir la adopción de ciertas decisiones importantes con entera independencia*" [160]. El Tribunal Supremo ratificó asimismo una ley de Nueva York que exigía que el Estado mantuviera un registro computarizado de la prescripción de determinadas drogas, ya que el programa no implicaba "*una amenaza suficientemente gravosa*"[161]. En el caso Nixon contra Administradores de Servicios Generales, la Corte ratificó la ley federal que permitía a los archiveros nacionales inspeccionar toda información escrita y grabada del presidente[162]. Dictaminó que, aunque "*el apelante tiene una legítima expectativa de privacidad con respecto a sus comunicaciones personales",* ese derecho debe ser sopesado en función del esencial interés público de preservar los materiales[163]. La Corte no consideró que la expectativa de privacidad del apelante tuviera el mismo peso que el interés público[164].

El documento original desarrollado para este informe Saber Mas III, Se encontraba dividido en las principales áreas legislativas sobre privacidad de los datos en los Estados Unidos: (1) Privacidad en línea; (2) Acceso a los registros públicos; (3) Privacidad financiera; (4) Privacidad de los servicios médicos; (5) Privacidad de los niños; y (6) Comunicaciones electrónicas[165]. Sin embargo, por razones de espacio y formato, en las páginas subsiguientes se publica un extracto del informe original, que se concentra sólo en el tema de privacidad de los datos y acceso a los registros públicos.

II. Privacidad de la información personal en los registros públicos[166]

Los registros públicos gubernamentales, incluyendo registros judiciales, informan a los miembros de una sociedad sobre el accionar oficial del gobierno e incentivan la rendición de cuentas (*accountability*)[167]. Aunque los registros públicos constituyen una poderosa herramienta para que los ciudadanos vigilen el accionar responsable de organismos y funcionarios gubernamentales, el riesgo potencial que se

[159] Whalen contra Roe, 429 U.S. 589 (1977).
[160] Ídem, 599-600.
[161] Ídem, 600.
[162] Nixon contra Administradores de Servicios Generales, 433 U.S. 425 (1977)
[163] Ídem, 465.
[164] Ídem.
[165] El memorándum original también incluye una sección aparte sobre la relación, implementación y cumplimiento de la ley federal y de las leyes de cada estado de los Estados Unidos. Aunque no se describe explícitamente la contraposición entre intereses personales y política de gobierno, se efectúa una evaluación del equilibrio inherente entre la protección de la información individual y el interés público en el acceso gubernamental a la información que se evidencia en la reglamentación y la jurisprudencia en cada área en los Estados Unidos.
Para leer el memorándum completo, acceda a:
https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=0B49ZtmN-sAd2NTE3M2Y1YWMtYzE0YS00YWU2LThkZjAtMzM0NWJkNWYwMTYz&hl=en_US (en inglés).
[166] Esta sección se compone, en general, de información proveniente de 1 Data Sec. & Privacy Law §7.
[167] Ver: Beth Givens, A Review of Current Privacy Issues, marzo de 2001. Disponible en: http://www.privacyrights.org/ar/Privacy-IssuesList.htm. (Una descripción del gobierno abierto como una de las características notables de la democracia).

desprende de la publicación de información personal en línea, instantáneamente accesible a millones de personas, inquieta a quienes abogan por la privacidad.

La legislación para proteger la privacidad de la información personal no ha evolucionado con el mismo ritmo con el que lo ha hecho la tecnología que afecta a dicha privacidad[168]. Ciertas leyes limitan el uso de datos de identificación personal en poder del gobierno, pero no hay un único esquema legislativo que establezca el derecho a la privacidad de la información y que resguarde el uso de los números de seguridad social por parte del sector privado.

Existen leyes que se aplican a la recopilación, uso y divulgación de la información de identificación personal disponible en los registros públicos[169]. Dos de los estatutos más importantes sobre conducta gubernamental con respecto a los registros públicos de información personal son la Ley de Libertad de la Información (*Freedom of Information Act*; FOIA, por sus siglas en inglés)[170] y la Ley de Privacidad de 1974 (*Privacy Act*) [171]. Ambas establecen cierta protección al uso y divulgación de información de identificación personal por parte de organismos públicos.

a. La Ley de Libertad de la Información (FOIA)

El propósito de la Ley de Libertad de la Información es "*asegurar una ciudadanía informada, vital para el funcionamiento de una sociedad democrática, necesaria para controlar la corrupción y exigir que los gobernantes rindan cuentas a sus gobernados*" [172]. Promulgada en 1966, la ley establece el acceso presunto de toda persona a registros gubernamentales, existentes o inéditos, sobre cualquier tema[173]. Constituye la vía principal para que los individuos obtengan acceso a los registros de dependencias federales[174]. El Congreso intentó así crear un sistema de monitoreo para que el público pudiera controlar a los organismos públicos a través de los documentos que estos publican[175]. Los legisladores asumieron que, si el gobierno se veía obligado a brindar información al público, entonces no excedería las limitaciones legales al recolectar y usar información personal. Para cumplir con este objetivo, la ley requiere que las agencias gubernamentales hagan publicos sus registros ante la solicitud de un individuo[176]. Este estauto se aplica a todos los registros compilados por entidades del gobierno federal, e incluye la información en formato electrónico. La ley reconoce, no obstante, la necesidad de salvaguardar la información personal, y protege la privacidad restringiendo el acceso o eximiendo registros públicos en determinadas instancias.

---

[168] La Ley de fraude y abuso informático (*Computer Fraud & Abuse Act*) podría haber sido una fuente indirecta de protección de la información personal compilada por agencias federales. Ver: 18 U.S.C.A. § 1030(a)(2). (Prohíbe a los individuos acceder a computadoras sin autorización, o excediendo los límites de su autorización, y así obtener "información de cualquier departamento o agencia de los Estados Unidos").

[169] Ver: Maureen S. Dorney, Privacy and the Internet, 19 Hastings Comm. & Ent. L.J. 635, 642 (1997). (Se observa que no existe una ley de privacidad exhaustiva en los EE.UU. con respecto a la información personal).

[170] 5 U.S.C.A. § 552.

[171] 5 U.S.C.A. § 552a.

[172] NLRB contra Sears, Roebuck & Co., 421 U.S. 132, 152 (1975).

[173] Wendy R. Ginsberg, Cong. Research Serv., RL 7-5700, Access to Government Information in the United States, 97-71 (2009). Debe tenerse en cuenta que la mayoría de los estados también cuentan con legislación similar a la Ley de Libertad de la Información (FOIA).

[174] Ver: James T. O'Reilly, Expanding the Purpose of Federal Records Access: New Private Entitlement of Threat to Privacy?, 50 Admin.L.Rev. 371, 372 (1998).

[175] Ídem.

[176] 5 U.S.C.A. § 552(a).

La ley enumera nueve categorías de registros que pueden ser lícitamente eximidos de divulgación –entre ellas, se pueden encontrar restricciones relacionadas principalmente con la seguridad nacional de los EE.UU. y con asuntos sensibles de las agencias de la ley. Las excepciones son las siguientes:

1. Información sobre defensa nacional o para fines de política exterior, clasificada adecuadamente como secreta según criterio establecido por orden del Ejecutivo.

2. Información relativa únicamente a reglas de manejo y prácticas del personal interno de los entes gubernamentales.

3. Datos específicamente eximidos de su divulgación por medio de estatuto que requiera evitar la revelación de tales asuntos de modo no discrecional, o que establezca un criterio determinado para que permanezcan ocultos, o que refiera a tipos particulares de asuntos que deben permanecer ocultos.

4. Secretos industriales o información financiera o comercial privilegiada o confidencial que haya sido obtenida de una persona.

5. Memorandos y cartas entre, o al interior de, entidades gubernamentales que legalmente no estarían disponibles, excepto a pedido de otra agencia en un litigio.

6. Archivos del personal y archivos médicos o similares cuya divulgación constituiría una invasión injustificada de la privacidad personal.

7. Ciertos tipos de registros de investigación recopilados con el fin de asegurar el cumplimiento de la ley.

8. Cierta información referida a la regulación de las instituciones financieras.

9. Información y datos geológicos y geofísicos[177].

Se han establecido centros federales y organizaciones no gubernamentales (ONG) para asistir al público en sus pedidos de información (según lo determina la ley FOIA). Por ejemplo, el Centro Federal de Información de la Administración de Servicios Generales de los EE.UU. está preparado para ayudar a las personas a detectar el organismo u oficina que necesitan y su dirección postal[178]. El Manual del Gobierno de los EE.UU., documento oficial del gobierno federal, provee información sobre los programas que se desarrollan en cada organismo y detalla los nombres del personal de mayor jerarquía y la dirección postal de cada ente[179]. Además, la Guía del Departamento de Justicia sobre la Ley de Libertad de la Información incluye un resumen exhaustivo de la ley y ofrece orientación general.

Otras leyes promulgadas por el Congreso en relación al acceso a la información promueven la transparencia mediante el acceso del público a las reuniones de los organismos federales y a las transcripciones de dichas reuniones. La Ley federal del Comité Asesor (*Federal Advisory Committee Act*; FACA por sus siglas en inglés)[180] fue promulgada en 1972 y exige que las reuniones de todos los consejos asesores de entidades que trabajan para el Poder Ejecutivo sean abiertas al público, y que

[177] 5 U.S.C.A. § 552(b)(1)-(9).
[178] Ginsberg, 6.
[179] Ídem
[180] 5 U.S.C. App.

todos los registros de tales comités sean accesibles. La ley fue elaborada para que los cuerpos asesores del Poder Ejecutivo tuvieran mayor transparencia[181]. Especifica ciertas categorías de registros y debates –categorías idénticas a las eximidas en la Ley de Libertad de la Información– que admiten que un comité celebre reuniones cerradas al público o prohíba la divulgación de ciertos documentos. La Ley de "Gobierno bajo el sol" (*Government in the Sunshine*, o *Sunshine Act*) fue promulgada en 1976 y abrió al escrutinio público la deliberación de políticas públicas que realizan los organismos federales dirigidos por cuerpos colegiados –tales como juntas directivas, comisiones o consejos[182]. Los organismos deben publicar avisos sobre reuniones inminentes, con suficiente antelación, para que estas sean accesibles al público.

En 1996, el Congreso aprobó la Ley de Libertad de la Información electrónica (E-FOIA por sus siglas en inglés). El estatuto anterior fue así enmendado para ampliar el acceso del público a todos los registros, incluyendo aquellos en formato electrónico[183]. Se definió, por primera vez, el término 'registro', estableciendo claramente que todo documento, en cualquier tipo de formato electrónico, debe ser considerado un registro, regulado por lo tanto por la Ley de libertad de información (FOIA)[184]. La nueva ley obliga a los organismos federales a entregar la información en el formato requerido por el solicitante, ya sea papel, disco, CD o algún otro tipo de formato electrónico[185].

La Ley de Libertad de la Información ha recibido creciente atención por parte de las compañías financieras de capital privado (*private equity funds*), dado que determinados fondos de capital –tales como los fondos de retiro– son considerados entidades públicas y, por lo tanto, sujetos a los requerimientos del estatuto. En este sentido, algunas empresas se han visto obligadas a entregar información sobre sus inversiones en respuesta a solicitudes realizadas en el marco de FOIA[186]. La reacción frente a esta divulgación forzada no es uniforme. Quienes apoyan la divulgación argumentan que una mayor transparencia incentivará la responsabilidad y el rendimiento de cuentas. No obstante, las compañías desean limitar la apertura de información sobre sus fondos para proteger estrategias de inversión y evitar riesgos a sus rendimientos[187]. Ambas partes coinciden en que la divulgación potencial que la ley trae aparejada ha contribuido a incrementar el escrutinio público sobre las inversiones de capital privado.

b. Aplicación de la Ley de Libertad de la Información (FOIA) en las cortes de los EE.UU.

La Corte Suprema de los Estados Unidos sostuvo que hacer públicas las declaraciones de testigos a quienes la Junta Nacional de Relaciones del Trabajo pretendía convocar a una audiencia sobre prácticas laborales injustas "interferiría" con los "procedimientos de seguridad" que lleva a cabo el organismo y, por lo tanto,

[181] Ginsberg, 3.
[182] 5 U.S.C. § 552b.
[183] Ver: Pub. L. No. 104-231, §§ 1 to 12, 100 Stat. 30448-54 (enmienda de las secciones de 5 U.S.C.A. § 552).
[184] Ver Pub. L. 104-231, § 3, 110 Stat. 3049.
[185] Ídem
[186] Ver: The Complexities of Venture Capital Investment Disclosure, 14 de noviembre de 2002. Disponible en: http://www.sri-advisor.com/article.mpl?sfArticleid=969.
[187] Ver: VC Funds Face Investors' Demands for Greater Transparency, marzo de 2003. Disponible en: http://www.bowne.com/newsletters/newsletter.asp?storyID=616.

este no estaba obligado a anunciar los testimonios antes de la audiencia[188]. La Junta argumentó que estos testimonios quedaban eximidos en el marco de la excepción 7(A) de la Ley de Libertad de la Información, que establece que no se debe exigir la divulgación de "registros de investigación recopilados a los fines de asegurar el cumplimiento de la ley, siempre y cuando la revelación de tales registros… pudiera interferir con los procedimientos de seguridad". La Corte dictaminó que, en el litigio pendiente sobre prácticas laborales injustas, los testimonios quedaban eximidos de la divulgación establecida por la ley FOIA –al menos, hasta la finalización de la audiencia– dado que la publicación de las declaraciones necesariamente "implicaría el tipo de daño que el Congreso considera constituiría una 'interferencia' con los procedimientos para asegurar el cumplimiento de la ley que lleva a cabo la Junta: la de darle a su oponente un acceso anticipado al caso de la Junta que el que tendría de otro modo" [189]. La Junta logró demostrar exitosamente que la divulgación de los testimonios "interferiría con los procedimientos para asegurar el cumplimiento de la ley", tal como se estipula en la excepción 7(A), siendo el riesgo más evidente el que empleados o sindicatos coaccionaran a los testigos para cambiar su testimonio o dejar de testificar[190].

El Tribunal Supremo de los EE.UU. sostuvo que las empresas no tienen derechos de privacidad personal según lo establecido por la Ley de Libertad de la Información[191]. El caso fue el resultado de una investigación llevada a cabo por la Comisión Federal de Comunicaciones (FCC por sus siglas en inglés), en la que se buscó determinar si AT&T le había cobrado de más al Gobierno por determinados servicios. Durante la pesquisa, AT&T entregó a la Comisión, entre otros elementos, información sobre facturación, y los nombres y descripción de tareas de ciertos empleados. AT&T argumentó que no estaba obligada a entregar registros de su personal dado que se encontraban protegidos por la excepción 7(c) de la Ley de Libertad de la Información, que cubre los registros recopilados para asegurar el cumplimiento de la ley e impide toda divulgación que "*pudiera constituir una invasión injustificada a la privacidad*"[192]. Finalmente, la Corte aceptó la posición de la Comisión, afirmando que la excepción 7(c) no se aplicaba a AT&T puesto que "las empresas no son portadoras de los intereses de privacidad personal que estipula la excepción".

La Corte Suprema del estado de Washington dictaminó que los metadatos de los documentos electrónicos de registros públicos gubernamentales han de ser considerados "registros públicos" en el sentido establecido por la Ley de Libertad de la Información y, por lo tanto, sujetos a divulgación[193]. Esta corte sostuvo que, en ocasión de solicitudes de información en el marco de la Ley de registros públicos (*Public Records Act*), los residentes tienen derecho a recibir una copia del mensaje de correo electrónico con todos sus metadatos. Los metadatos contienen información que incluye direcciones de correo electrónico, autores, destinatarios, tipo de documento y fecha en que el archivo fue creado o modificado.

La Corte de Apelaciones de Michigan decidió que el correo electrónico personal entre funcionarios de gobierno no está sujeto a divulgación, según la Ley de Libertad de la Información de ese estado[194]. Afirmó que el uso indebido de recursos tecnológicos provistos por el empleador por parte del empleado "no transforma las

[188] NLRB contra Robbins Tire and Rubber Co., 437 U.S. 214 (1978).
[189] Ídem, 241.
[190] Ídem, 242-43.
[191] FCC contra AT&T Inc., et al., 131 S.Ct. 1177, slip op., N.° 09-1279 (1 de marzo de 2011).
[192] 5 U.S.C.A. § 552(b)(7)(C).
[193] O'Neill contra Ciudad de Shoreline, 240 P.3d 1149 (Wash. 2010).
[194] Howell Educ. Ass'n v. Howell Bd. of Educ., 789 N.W.2d 495 (Mich. Ct. App. 2010).

comunicaciones personales en registros públicos. En efecto, el hecho de que la comunicación haya sido enviada violando las políticas de uso incide a favor de la conclusión de que el correo electrónico no es un registro público, ya que excede expresamente las tareas de la función oficial como, por ejemplo, el fomento de los objetivos educativos del distrito" [195].

c. La Ley de Privacidad de 1974 (*Privacy Act*)

La Ley de Privacidad acompaña y amplía lo establecido por la Ley de Libertad de la Información. Esta última fue diseñada para brindar acceso a la información gubernamental. La Ley de Privacidad fue adoptada tanto para proteger la información personal en bases de datos federales, como para asegurar a los individuos ciertos derechos sobre la información allí contenida. Dicha ley especifica medidas de prevención contra la invasión de la privacidad mediante el uso indebido de los registros por parte de los organismos del gobierno federal. El objetivo general de esta ley es ofrecer un equilibrio entre la necesidad del gobierno de contar con información sobre los individuos y el derecho de estos individuos a protegerse contra invasiones injustificadas a la privacidad causadas por la recopilación de información por parte de los organismos federales.

La Ley de Privacidad reglamenta la divulgación, por parte del gobierno, de información contenida en sus bases de datos. Exige que los organismos federales que recopilan información personal destinada a los registros públicos cumplan con las siguientes condiciones: (1) asegurar la veracidad de toda información personal compilada; (2) recopilar únicamente la información necesaria y relevante a la función específica del organismo; y (3) establecer procedimientos específicos para proteger la seguridad de la información[196]. También prohíbe que el gobierno divulgue registros de los organismos federales sin consentimiento por escrito, aunque sujeto a ciertas excepciones, como aquellos casos en que los registros sean utilizados con fines "rutinarios"[197], con el propósito de asegurar el cumplimiento de la ley o para proteger la salud o la seguridad del sujeto de los registros[198]. "Registro" se define como "todo elemento, recopilación o conjunto de información sobre un individuo que está en poder de un organismo, incluyendo –pero sin limitación– su educación, transacciones financieras, historial médico e historial criminal o de empleo, y que contenga su nombre, número de identificación, símbolo u otro elemento especial de identificación, tal como una impresión digital o vocal, o una fotografía"[199].

Esta ley otorga al individuo un mayor control sobre la recopilación y uso de información personal que efectúa el gobierno. Garantiza tres derechos básicos: (1) el derecho a ver los registros y la información compilada, sujeto a excepciones establecidas por la ley; (2) el derecho a corregirlo en caso de inexactitudes u omisiones; y (3) el derecho a entablar una demanda contra el gobierno por violación del estatuto, por ejemplo, casos en que el gobierno permite que otra persona vea los registros[200].

La Sección 7 de la Ley de Privacidad constituye la restricción fundamental al uso de números de seguridad social individuales por parte del gobierno: prohíbe que un

[195] Ídem, 242.
[196] 5 U.S.C.A. § 552a(e).
[197] 5 U.S.C.A. § 552a(b)(3); ver también: 5 U.S.C.A. § 552a(a)(7) que define "uso rutinario" como "el uso de estos registros para fines compatibles con el propósito con que fueron recopilados".
[198] 5 U.S.C.A. § 552a(b)(7)-(8).
[199] 5 U.S.C.A. §552a(a)(4).
[200] Ver: 5 U.S.C.A. § 552a(c), (d) y (g).

organismo gubernamental prive de un derecho, un beneficio o un privilegio a un individuo meramente porque este se rehúsa a dar a conocer su número de seguridad social[201]. Los organismos gubernamentales –tanto locales como estatales– no pueden exigir que las personas informen sus números de seguridad social, a menos que: (1) el pedido sea realizado a causa de alguna ley federal, o (2) el sistema de registro que solicita el dato existiera previamente a 1975 y utilizara entonces estos números para identificar a las personas[202].

La Ley de Privacidad especifica diez categorías de información eximidas del acceso del público:

1. Información recopilada con razonable antelación a acciones o procedimientos civiles; excepción directa (autoejecutable).

2. Registros de la Agencia Central de Inteligencia (CIA por sus siglas en ingles): información concerniente a registros poligráficos, fuentes y métodos para obtener información de inteligencia –incluyendo las instalaciones, organización, funciones, nombres, títulos oficiales, salarios o números del personal empleado por el organismo– y documentos o información provistos por gobiernos extranjeros.

3. Registros de los organismos de aplicación del derecho penal recopilados durante el curso de un procedimiento de aplicación de la ley y que se relacionen directamente con las funciones específicas del organismo.

4. Información clasificada por orden del Poder Ejecutivo en interés de la defensa nacional o la política exterior.

5. Registros de aplicación del derecho civil; registros de organismos de aplicación del derecho penal que no se relacionan directamente con las funciones específicas del organismo; la cobertura es menos amplia allí donde el individuo haya sido privado de un derecho, privilegio o beneficio como resultado de la información buscada.

6. Información pertinente a la protección del Presidente de los Estados Unidos u otros individuos según lo establecido en la sección 3056 del Título 18.

7. Información recolectada y utilizada únicamente con fines estadísticos y requerida por ley.

8. Material de investigación utilizado únicamente para determinar la idoneidad, elegibilidad y calificaciones de los potenciales empleados civiles de organismos federales, o el acceso a información clasificada cuando el material proviene de fuentes confidenciales.

9. Material de evaluación utilizado para decidir el nombramiento o promoción de empleados federales, siempre y cuando su divulgación comprometa la objetividad y equidad del proceso.

10. Registros de evaluación militares[203].

[201] Ver: Pub. L. No. 93-579, § 7, 5 U.S.C.A. § 522a.
[202] Ídem.
[203] 5 U.S.C. § 552a (j-n).

La Ley de Privacidad obliga a los organismos federales a publicar una lista anual de los sistemas que utilizan para compilar información personal. La supervisión central del cumplimiento de este requisito ha sido asignado a la Oficina de Gerencia y Presupuesto (*Office of Management and Budget*), aunque la dependencia ha ejercido un liderazgo relativamente débil en la implementación. Se exige asimismo la designación de funcionarios de la Ley de Privacidad al interior de los organismos federales ejecutivos para manejar los pedidos y asegurar el cumplimiento del código de prácticas. En última instancia, el cumplimiento depende de las cortes, ya que los individuos pueden entablar demandas para la reparación de agravios percibidos[204].

d. Aplicación de la Ley de Privacidad en las cortes de los EE.UU.

Con respecto a la verificación de antecedentes efectuada por el Gobierno a sus potenciales empleados, el Tribunal Supremo de los EE.UU. dictaminó que los datos que algunos objetaban no constituían una divulgación injustificada y que, por lo tanto, no violaban el derecho a la privacidad de los empleados. El interés del Gobierno como empleador y dueño del manejo de su funcionamiento interno, sumado a la protección contra la difusión pública prescrita por la Ley de Privacidad de 1974[205], satisfacen todo "interés de evitar la divulgación" que pudiera "ser considerado como emanado de la Constitución"[206]. La Corte rechazó el argumento de los demandantes, según quienes las excepciones establecidas por la Ley de Privacidad constituían una protección "demasiado porosa" para frenar significativamente las "divulgaciones injustificadas" –"el solo hecho de que el requisito de no divulgación de la Ley de Privacidad sea sujeto a excepciones no demuestra que el estatuto provea protección insuficiente contra la divulgación" [207].

La Suprema Corte de los EE.UU. sostuvo que revelar la dirección postal de ciertos empleados a los sindicatos está prohibido por la Ley de Privacidad[208]. Los demandantes (sindicatos) se apoyaron en la excepción que permite la divulgación de información que sería requerida por la Ley de Libertad de la Información[209]. La Corte determinó que, si bien revelar la dirección de los empleados puede facilitar la comunicación entre ellos y el sindicato, este tipo de divulgación "cae por fuera del ámbito del interés público que la Ley de Libertad de la Información pretende defender, por ejemplo, el interés por fomentar la comprensión del público acerca de las operaciones o actividades del gobierno" [210]. Se afirmó que "está claro que [los acusados] tienen *algún* interés no trivial de privacidad al querer evitar la divulgación", y que el hecho de que su dirección postal pueda ser obtenida por medio de fuentes públicas y accesibles no diluye el deseo de los empleados de controlar la divulgación de sus asuntos personales[211]. Dado que el interés de privacidad de los empleados con respecto a sus direcciones postales supera con creces el insignificante interés público que se desprende de su revelación, la Corte dictaminó que la divulgación constituiría una "invasión claramente injustificada de la privacidad personal" [212]. "La Ley de Libertad de la Información, por lo tanto, no requiere que los

[204] Stratford & Stratford, pp.18.
[205] 5 U.S.C. § 552a.
[206] Nat'l Aeronautics and Space Admin. contra Nelson, 131 S.Ct. 746 (2011).
[207] Ídem, 762.
[208] U.S. Dept. of Def., et al. contra Fed. Labor Relations Auth. et. al., 510 U.S. 487 (1994).
[209] 15 U.S.C.A. § 552a(b)(2).
[210] U.S. Dept. of Def., 510 U.S. at 500 *op.cit.*
[211] Ídem, 501.
[212] Ídem, 502 (citando 5 U.S.C. § 552(b)(6)).

organismos divulguen las direcciones postales, y la Ley de Privacidad, en adelante, prohíbe que sean reveladas a los sindicatos"[213].

e. Conclusión

Aunque ambas leyes fueron sancionadas con propósitos diferentes, hay cierta similitud en sus previsiones. Tanto la Ley de Libertad de la Información como la Ley de Privacidad otorgan al individuo el derecho de solicitar acceso a registros de los organismos del gobierno federal. La Ley de Libertad de la Información otorga derecho de acceso, en general, a "cualquier persona", pero la de Privacidad lo brinda solamente al individuo que es sujeto de los registros en cuestión (siempre que se trate de un ciudadano de los Estados Unidos, o de un extranjero con residencia permanente adquirida legalmente). La Ley de Libertad de la Información se aplica a todos los registros de organismos federales. La de Privacidad, sin embargo, solo se aplica a aquellos registros de organismos federales que contienen información sobre los individuos, que son conservados en un sistema y que son localizados a través del nombre o la identificación personal del individuo.

Ambos estatutos encarnan el esfuerzo del Gobierno de los EE.UU. por mantener un equilibrio entre el derecho inherente del público a tener información sobre el gobierno y, al mismo tiempo, la protección de "la divulgación injustificada [y potencialmente dañina]" de los datos de identificación personal de un individuo. Con la Ley de Libertad de la Información, el Congreso ha aceptado el derecho del público a acceder a la información recopilada en registros de organismos gubernamentales, pero también reconoce que determinada información no puede ser revelada cuando no está en riesgo el interés del público. La Ley de Privacidad garantiza a los individuos el acceso y control de la información concerniente a su propia persona en los registros públicos. Es poco probable que llegue a fin en el corto plazo la batalla entre los defensores de la autorregulación y el del público en general por una mayor regulación gubernamental. Sin embargo, está claro que el Gobierno y el Poder Judicial de los Estados Unidos pretenden respetar el derecho del individuo a la privacidad, a la vez que buscan asegurar que el concepto legal de privacidad no sofoque el derecho de contar con información sobre los registros de los organismos federales y el funcionamiento interno del gobierno.

[213] Idem.