Karin Castro Cruzatt(*)

El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú

«EL CONOCIMIENTO Y USO DE LA INFORMACIÓN PERSONAL HACE POSIBLE LA ADOPCIÓN DE DECISIONES QUE AFECTAN LOS DERECHOS FUNDAMENTALES DE SUS TITULARES, QUIENES QUEDARÍAN EN UNA SITUACIÓN DE VIRTUAL INDEFENSIÓN FRENTE A ELLO».

1. El derecho a la protección de datos personales: origen y definición

El derecho a la protección de datos personales surgió en el marco del desarrollo tecnológico que tuvo lugar a partir de la década de los sesenta y que se tradujo en la aparición y desarrollo de sistemas informáticos capaces de procesar, relacionar y transmitir información a gran velocidad; configurando una auténtica revolución. Y es que, con el advenimiento del desarrollo tecnológico quedaron atrás las barreras espaciales y temporales que limitaban la utilización y acumulación de la información. En la actualidad, "los recursos tecnológicos no conocen el olvido, ni se detienen ante la lejanía y son capaces de almacenar, relacionar y comunicar en tiempo real ingentes masas de datos de todo tipo, incluidos los de carácter personal y de utilizarlos para las más diversas finalidades"(1).

Resulta innegable que las tecnologías informáticas han aportado diversos beneficios a la sociedad y que hoy están presentes en casi todas las actividades de nuestra vida(2). Tampoco cabe cuestionar que el Estado precisa contar con un considerable flujo de información para desempeñar con mayor eficiencia sus funciones y ello supone, por tanto, el registro y uso de información de tipo personal de los administrados y administradas. Así, labores como la recaudación tributaria, la gestión de la seguridad social y la prevención de las actividades delictivas, entre muchas otras,

(*) Abogada. Profesora de Derecho Constitucional en la Pontificia Universidad Católica del Perú. Miembro de la Asociación Peruana de Derecho Constitucional.

(1) MURILLO DE LA CUEVA, Pablo Lucas. *Diez preguntas sobre el derecho a la autodeterminación informativa y el derecho a la protección de datos de carácter personal"*. Agencia Catalana de Protección de Datos. Conferencia realizada el día 24 de octubre de 2005. Disponible en: http://www.apd.cat

(2) SERRANO PÉREZ, María Mercedes. *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Civitas, 2003. p. 18

son tareas a las que la informática viene aportando mayores dosis de eficacia y predictibilidad(3).

Pero en el contexto del creciente desarrollo informático y tecnológico se advirtió también que el registro indiscriminado de datos personales, su interrelación y posterior transmisión descontrolada, confiere un alto poder de control sobre los titulares de dichos datos, llegando a representar una nueva forma de dominio social a la que le ha denominado Poder Informático(4).

De este modo, quedó en evidencia que el conocimiento y uso de la información personal hace posible la adopción de decisiones que afectan los derechos fundamentales de sus titulares, quienes quedarían en una situación de virtual indefensión frente a ello. Así, por ejemplo, con el registro no consentido de la filiación política de una persona que tiene expectativas de acceder a un puesto de trabajo y el posterior acceso de su potencial contratante a dicho dato, se podría generar una afectación a su derecho a la no discriminación y eventualmente una afectación a su derecho al trabajo.

Si bien la gravedad de los riesgos antes descritos resulta patente tratándose de datos referidos a la esfera íntima de las personas, la informática también puede generar situaciones de indefensión a partir del registro y transmisión de datos personales que en un primer momento podrían calificarse como inocuos, pero que registrados, relacionados y transmitidos en conjunto con otros, revelan características esenciales de las personas y permiten delinear un perfil sobre su personalidad, afectando con ello su dignidad y diversos derechos fundamentales(5). Por ello, se suele afirmar que ningún dato personal es neutro o irrelevante por lo que la facultad de sus titulares de controlar su acopio y posterior uso debe garantizarse en todos los casos(6).

«EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SE CARACTERIZA POR SER UN DERECHO DE CONTENIDO COMPLEJO, PUES SE ENCUENTRA INTEGRADO POR DISTINTAS FACULTADES O DERECHOS ESPECÍFICOS».

Si se tienen en cuenta las ventajas que aporta la informática al desarrollo de la sociedad y se advierte que los fines a los que esta herramienta sirve resultan en muchos casos compatibles con la Constitución, es fácil concluir que es preciso encontrar un punto de equilibrio entre el respeto a los derechos fundamentales y la recolección y uso de datos personales(7). Desde esta perspectiva, se ha señalado que el derecho a la protección de datos personales constituye "una reacción de defensa, frente al avance de la informática"(8); un derecho destinado a solventar la tensión existente entre el uso generalizado -y necesario- de la informática y el riesgo que dicho uso supone en el disfrute de los derechos de las personas(9).

Si bien en sus inicios se concibió al derecho a la protección de datos personales como

(3) PÉREZ LUÑO, Enrique Antonio. *Informática y libertad. Comentario al artículo 18.4 de la Constitución Española*. En: *Revista de Estudios Políticos. Nueva época,* Número 24, noviembre-diciembre de 1981. p. 36.
(4) FROSINI, Vittorio. *Bancos de datos y tutela de la persona*. En: *Revista de Estudios Políticos (Nueva época)*, Número 30, noviembre-diciembre de 1982. pp. 23 y 24.
(5) MURILLO DE LA CUEVA, Pablo Lucas. *La construcción del derecho a la autodeterminación informativa*. En: *Revista de Estudios Políticos. Nueva época.* Número 104, abril-junio de 1999. p. 38.
(6) ORTI VALLEJO, Antonio. *El nuevo derecho fundamental (y de la personalidad) a la libertad informática. A propósito de la STC 254/1993, de 20 de julio.* En: *Derecho Privado y Constitución*. Número 2, enero-abril de 1994. pp. 319 y 320.
(7) SERRANO PÉREZ, María Mercedes. *Op. cit.*; pp. 18 y 19.
(8) EKMEKDJIAN, Miguel Ángel y PIZZOLO, Calogero. *Habeas data. El derecho a la intimidad frente a la revolución informática*. Buenos Aires: Depalma. p. 21.
(9) PIÑAR MAÑAS, José Luis. *Reflexiones sobre el derecho fundamental a la protección de datos personales*. En: *Actualidad Jurídica Uria Menéndez*. Número 12, 2005. p. 9.

una faceta positiva del derecho a la intimidad, a la cual se le adscribió la función tutelar a las personas ante la "agresión tecnológica de su intimidad"[10], cada vez existe mayor acuerdo en catalogarlo como un derecho autónomo[11]. A través de este derecho se reconoce a las personas la facultad de controlar el acopio, tratamiento y transmisión de sus datos personales; y para el ejercicio de dicho control se les reconoce un conjunto de facultades. Con ello, se busca garantizar que el tratamiento de la información personal no genere la afectación de derechos fundamentales. En esta línea, el Tribunal Constitucional Español lo ha definido en los siguientes términos:

"Consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, (...) se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular"[12].

Aunque en nuestro ordenamiento nacional el desarrollo integral de la protección de datos personales es todavía una tarea pendiente, su reconocimiento en la Constitución vigente -aunque sea de una forma insuficiente- y la existencia de un proceso constitucional destinado a su tutela, ameritan reflexionar en torno a su contenido y alcances. También es preciso advertir sobre la necesidad de compatibilizar su ejercicio con el de otros derechos fundamentales y bienes constitucionalmente protegidos.

En este trabajo presentamos algunos de los aspectos básicos que debiera contemplar la regulación en materia de protección de datos personales. Posteriormente, analizaremos el reconocimiento de este derecho fundamental en la Carta de 1993 y evaluaremos los aportes de la jurisprudencia del Tribunal Constitucional y del Código Procesal Constitucional en el desarrollo de este derecho. Finalmente, expresamos la necesidad de contar con una norma jurídica que desarrolle el contenido y alcances de este derecho y planteamos la necesidad de armonizar su ejercicio con el del derecho de acceso a la información pública.

2. La regla general del consentimiento previo e informado para el tratamiento de datos personales

El Consentimiento es un principio medular en materia de protección de datos. Supone, en líneas generales, la autorización previa e informada que debe brindar el titular de los datos personales que serán objeto de tratamiento al responsable de dicha actividad[13]. Esta manifestación de voluntad,

(10) PÉREZ LUÑO, Enrique Antonio. *Informática y libertad. Comentario al artículo 18.4 de la Constitución Española*. *Op. cit.*; p. 34.

(11) Esta evolución se puede apreciar en la jurisprudencia del Tribunal Constitucional español la cual inicialmente concibió al derecho reconocido en el artículo 18.4 de la Constitución española como un nuevo ámbito del derecho a la intimidad, para posteriormente, a partir de la expedición de la STC 292/2000, distinguir el contenido y objeto de cada uno de dichos atributos. De este modo "lo que antes era considerado un contenido "positivo", y no meramente negativo o excluyente, de un derecho a la intimidad ampliado a nuevos supuestos de infracción, por causa de la informática, es ahora un contenido diferenciado de un derecho autónomo": ROIG, Antoni. *La protección de las bases de datos personales. Análisis de la jurisprudencia del Tribunal Constitucional*. En: Revista Jurídica de Catalunya, Núm. 4, 2002, pp. 152 y 153. Ciertamente, en la actualidad encontramos autores que consideran al derecho a la protección de datos como una faceta del derecho fundamental a la intimidad. En esta dirección se ha señalado: "no podemos realizar otra aseveración mas que aquella que entiende al art. 18.4 CE como una indicación expresa del contenido esencial del derecho a la intimidad". REBOLLO DELGADO, Lucrecio. *El derecho fundamental a la intimidad*. Madrid: Dykinson, 2005. p. 306.

(12) Sentencia 292/2000, de 30 de noviembre.

(13) El tratamiento de datos personales incluye todas las operaciones de carácter técnico que recaen sobre los datos personales y que se dirigen a lograr su acopio o registro, su interrelación, su modificación, su comunicación a terceros y su cancelación o bloqueo.

que puede ser expresa o tácita según lo contemple cada ordenamiento jurídico, debe ser prestada atendiendo a las circunstancias concretas en las que se solicitan los datos personales. Así, el titular de la información personal debe conocer la finalidad para la cual sus datos son registrados, el uso que se pretende dar a los mismos y los derechos que lo asisten para vigilar que las condiciones bajo las cuales prestó su autorización sean respetadas(14).

Con esta exigencia se pretende que los titulares de la información personal puedan conocer y merituar los beneficios y eventuales desventajas que podría conllevar el tratamiento de sus datos. Por esta razón, el consentimiento debe ser específico. No cabría, entonces, un apoderamiento genérico pues ello desvirtuaría la finalidad del mismo(15). A su vez, una vez prestado éste puede ser revocado por el titular.

Ciertamente, la regla general del consentimiento previo e informado al tratamiento de datos personales admite excepciones. Aunque en este punto nuevamente es indispensable atender a la regulación específica de cada país, podemos mencionar, a título ilustrativo, algunos de los casos más comúnes en los que no se requiere la autorización previa del titular. Entre estos supuestos encontramos al tratamiento de la información personal que recogen las administraciones públicas para el desarrollo de las actividades que se enmarcan dentro del ámbito de sus competencias. Se considera que resultaría una excesiva carga para la Administración imponer la exigencia de recabar el consentimiento de los administrados y administradas en cada oportunidad en la que requiera tratar información personal(16).

También es frecuente que se excluya de la exigencia del consentimiento previo al tratamiento de datos personales que tenga su origen en una relación contractual, como puede ser la laboral o una de orden comercial. En estos casos operaría ante una suerte de consentimiento tácito(17). Así, por ejemplo, los datos que son recogidos por una empresa que vende seguros de salud son puestos en su conocimiento por sus usuarios de manera libre y voluntaria, con el objeto de que se concrete el vínculo contractual. Mencionaremos, finalmente, a la información personal que es recogida y procesada por los órganos policiales con la finalidad de resguardar la seguridad ciudadana y coadyuvar en la prevención del delito. Cabría precisar que el tratamiento de información en este ámbito suele sujetarse a un régimen especial.

3. Los datos personales y los datos sensibles

Podemos considerar como dato personal toda información sobre una persona física (o jurídica) que permita su identificación de manera directa o indirecta. Como ejemplos podemos mencionar: las huellas dactilares, la dirección domiciliaria, la pertenencia a un partido político, las creencias religiosas, entre otros. Las imágenes que son captadas por los sistemas de video vigilancia de las entidades públicas o privadas podrían constituir datos de carácter personal, si dichos registros visuales permiten identificar a las personas que aparecen en ellas. Bajo el mismo criterio, el registro auditivo de la voz de una persona podrá también ser considerado como un dato personal en la medida en que permita su identificación.

Dentro del género de datos personales existe una categoría cuya revisión es imprescindible en todo estudio que verse sobre protección de datos personales. Se trata de los datos sensibles. Si bien esbozar una definición de la información personal que puede ser catalogada como sensible no es una tarea sencilla, podemos señalar algunas de sus

(14) MURILLO DE LA CUEVA, Pablo Lucas. *Informática y protección de datos personales. Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal. Cuadernos y Debates*. Madrid: Centro de Estudios Constitucionales, 1993. pp. 61 y 62.
(15) SERRANO PÉREZ, María Mercedes. *Op. cit*.; pp. 195-243.
(16) *Ibid*.; p. 213.
(17) MURILLO DE LA CUEVA, Pablo Lucas. *Informática y protección de datos personales. Op. cit*.; p. 61.

principales características. Debemos empezar afirmando que la información sensible permite conocer características que forman parte del "núcleo de la personalidad y dignidad humanas"[18]. Entre estos datos destacan: el origen racial, los datos referidos a la ideología, religión o creencias, los datos relativos a la salud, la orientación sexual, entre otros.

Un rasgo esencial y a la vez determinante para calificar a un dato personal como sensible, es que alude a cuestiones cuya divulgación o comunicación a terceros puede dar lugar a prácticas discriminatorias. En este sentido, Peyrano considera que este concepto incluye "todos aquellos datos personales que por sus connotaciones en el medio social, tengan, en el caso concreto, la aptitud de generar (...) actitudes o conductas de carácter discriminatorio"[19].

Ahora bien, es importante destacar que la información sensible no se identifica, ni se agota en aquélla referida a la intimidad personal o familiar. Si bien la información de carácter íntimo puede considerarse sensible por su estrecha conexión con los aspectos básicos de la personalidad, existe información que sin ser necesariamente de naturaleza íntima, goza de carácter sensible. Así, por ejemplo, suele considerarse que la filiación sindical constituye un dato sensible, pese a que carece de carácter íntimo. Un comentario similar se puede formular en torno a la información referida a las condenas penales que ya han sido cumplidas. No se trata, en nuestra opinión, de información íntima, pero parece claro que el acceso ilimitado a dicho dato puede provocar discriminación.

El artículo 10 de la Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información, Ley 27489, dispone que dichas instituciones no podrán registrar, ni suministrar en sus reportes de crédito información sensible[20]. El artículo 2, literal c de dicha norma ofrece una definición al respecto:

"c) Información sensible. - Información referida a las características físicas, morales o emocionales de una persona natural, o a hechos o circunstancias de su vida afectiva o familiar, tales como los hábitos personales, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual u otras análogas que afecten su intimidad y todo lo referido en la Constitución Política del Perú en su Artículo 2º inciso 6)".

Asimismo, el proyecto de la Ley de protección de datos personales, aprobado mediante Resolución Ministerial 331-2004-JUS, contiene un listado de los datos considerados sensibles:

"2.4. Datos sensibles: datos personales relacionados con: el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, así como aquellos otros establecidos por el reglamento de la presente Ley".

La especial delicadeza de este tipo de información personal hace que merezcan una especial tutela. Esta protección reforzada se expresa en la prohibición de registrar información sensible, salvo que medie consentimiento expreso e inequívoco de su titular. Asimismo, como regla general, se encuentra proscrito la organización de archivos o registros que tengan como finalidad exclusiva el tratamiento de este tipo de datos.

(18) *Ibid.*; p. 69.

(19) PEYRANO, Guillermo. *Régimen Legal de los Datos Personales y Habeas Data*. Buenos Aires, LexisNexis-Depalma, 2002, p.38, citado por PUCINELLI, Oscar. *Los datos de afiliación partidaria son datos sensibles y no deben ser puestos a disposición del público general. A propósito de su inclusión en padrones electorales y en bases de datos disponibles en internet*. En: *Revista Jurídica del Peru*. Año LV, Número 64, setiembre-octubre de 2005. p.240.

(20) "Artículo 10º.- Información excluida
Las CEPIRS no podrán contener en sus bancos de datos ni difundir en sus reportes de crédito la siguiente información:
a) Información sensible (...)"

4. Los sujetos activos o titulares del derecho a la protección de datos personales

El sujeto activo o titular del derecho a la protección de datos personales es la persona a la que pertenecen los datos objeto de tratamiento, es decir, "aquella a quien conciernen las informaciones que, permitiendo directa o indirectamente su identificación, se registran, conservan, elaboran, modifican, cancelan o ceden"(21).

Las personas físicas resultan destinatarias naturales de este derecho, pues como hemos mencionado, su surgimiento tiene como fundamento inicial la protección del derecho a la intimidad personal. De hecho, las primeras normas que consagraron y desarrollaron este derecho limitaron su ámbito de protección a las personas físicas(22). Considerando que la Constitución vigente no ha reservado su titularidad de los derechos fundamentales a las personas físicas y que el Tribunal Constitucional peruano ha admitido que las personas jurídicas de derecho privado pueden ser titulares de derechos fundamentales de acuerdo a la naturaleza de estos(23), cabría preguntarse si este derecho puede ser reconocido también a favor de las personas jurídicas de derecho privado.

Somos partidarios de considerar que las personas jurídicas de derecho privado también son titulares del derecho a la protección de datos personales, aunque con un alcance distinto al que corresponde a las personas físicas. Ciertamente, no será posible sostener que respecto de las personas jurídicas de derecho privado pueda existir información íntima, en la medida que no los consideramos titulares del derecho a la intimidad personal. Tampoco podemos afirmar que cuenten con datos sensibles pues, como hemos indicado, estos datos traducen características intrínsecas de la personalidad humana, lo cual resulta ajeno a las personas jurídicas de derecho privado. Sin embargo, respecto de ellas se genera información cuyo eventual tratamiento debe ser tutelado. Así, por ejemplo, las personas jurídicas de derecho privado mantienen relaciones comerciales y contractuales cuyo incumplimiento puede dar lugar a la incorporación de dicha información en una central de riesgo crediticio, siendo necesario reconocerles la facultad de controlar el uso de dicha información.

Este criterio habría inspirado la Ley 27489, mediante la cual se regula la actividad de las Centrales Privadas de Información de Riesgos y de Protección al titular de la información. La norma en mención contempla expresamente como sujetos activos a las personas naturales y a las jurídicas, en el literal d de su artículo 2, en donde se define al titular de la información como: "La persona natural o jurídica a la que se refiere la información de riesgos". Por su parte, la legislación argentina contiene una disposición específica sobre el tema bajo comentario. El artículo 1 de la Ley 25326, Ley de protección de datos personales, dispone que: "Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a las personas de existencia ideal".

Por lo tanto, es posible afirmar que las personas jurídicas de derecho privado titularizan el derecho a la protección de datos de carácter personal, aunque con un contenido más limitado que el que se despliega tratándose de las personas físicas. Dicho alcance, deberá determinarse caso a caso.

5. Los sujetos pasivos u obligados por el derecho a la protección de datos personales

El sujeto pasivo u obligado es la persona o entidad, de carácter público o privado, que tiene a su cargo el registro, archivo o banco de datos personales. Sobre él recaen una serie de deberes y obligaciones en relación con los

(21) MURILLO DE LA CUEVA, Pablo Lucas. *Informática y protección de datos personales. Op. cit.*; p. 51.
(22) PÉREZ LUÑO, Enrique Antonio. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 1995. p. 375.
(23) Expediente 0905-2001-AA/TC, fojas 5.

datos personales objeto de tratamiento. Dicha actividad debe adecuarse a los principios de la protección de datos personales que serán objeto de desarrollo en el siguiente apartado.

Para efectos del presente estudio consideramos útil distinguirlos en tres categorías: i) los archivos o registros cuya función principal es suministrar información a terceros, ii) los bancos o archivos que sirven de apoyo a la función desempeñada por las entidades públicas o privadas a las que pertenecen, y, iii) los bancos de datos, archivos o registros de uso personal.

Los bancos de datos pertenecientes al primer grupo de sujetos pasivos están dedicados principalmente al tratamiento de información personal y su transmisión o suministro a terceros. Este sería el caso de las centrales de riesgo crediticio de carácter público o privado. En el segundo grupo encontramos a los archivos o registros utilizados por entidades públicas o privadas para apoyar las funciones que desempeñan. Si bien estas entidades no tienen por función principal el tratamiento de datos personales, el volúmen de información personal que requieren procesar demanda su organización mediante la creación y mantenimiento de registros o archivos. Como ejemplo, en el ámbito privado, encontramos a las bases de datos de los centros de salud que contienen las historias clínicas de sus pacientes, o los que pertenecen a las instituciones bancarias y financieras y conservan información sobre sus usuarios. En el sector público, encontraríamos a los bancos de datos de los distintos ministerios del Estado en donde constan los legajos del personal que labora en sus dependencias; o los archivos con los que cuentan los centros educativos estatales en donde se encuentra registrada información personal referida a sus alumnos y alumnas.

Dentro del tercer supuesto encontramos a los archivos o registros de uso personal o doméstico. Estos archivos son los que utilizan los particulares en cualquier ámbito de su vida personal o profesional. Su uso y acceso se encuentra restringido a su titular, pues no han sido creados ni son utilizados para suministrar información a terceras personas. Por ello, la transmisión de la información personal que almacenan, con los consiguientes riesgos que ello podría suponer para sus titulares resultaría -en principio- inexistente.

La legislación argentina en materia de protección de datos de carácter personal excluye de la condición de sujetos pasivos a los archivos o registros creados por particulares y que tengan un uso exclusivamente personal[24]. Pero, como anota Puccinelli, no siempre resultará sencillo determinar si, en efecto, la utilización de un registro o banco de datos no trasciende del ámbito personal. Por ello, propone como criterio determinante atender al uso que en la práctica se le viene dando. Así, la accesibilidad del archivo frente a terceros determinará su calidad de sujeto pasivo del derecho a la protección de datos personales. Según refiere el autor citado: "En la medida en que a la información contenida en el registro puedan acceder personas distintas de la persona física que es su propietario, aunque sea con fines estrictamente internos, el sistema de información cae en la órbita de la ley y se debe cumplir con todos sus principios y deberes"[25].

Dentro del grupo de archivos o bancos de información de uso personal un caso particularmente delicado es el referido a los archivos o bases de datos que elaboran y utilizan las personas como parte del ejercicio de su derecho a la libertad de información. En vista del potencial riesgo hacia el ejercicio de las libertades de expresión e información que podría representar su consideración como sujetos pasivos del derecho objeto de estudio[26], la Constitución argentina precisa que mediante el Habeas Data "no podrá afectarse el secreto de las fuentes de

(24) La Ley 25326 prevé en su artículo 24 lo siguiente: "Los particulares que formen archivos, registros o bancos de datos que no sean para uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21°".
(25) PUCCINELLI, Oscar R. *Protección de datos de carácter personal*. Buenos Aires: Astrea, 2004. pp. 372 y 373.
(26) SAGÜÉS, Néstor Pedro. *El Habeas Data argentino (orden nacional)*. En: *Derecho PUCP*, Número 51, diciembre de 1997. p. 183.

información periodística". Asimismo, en el caso chileno, la Ley 19628, Sobre protección de la vida privada o protección de datos de carácter personal, que tiene un amplio alcance en lo referido a los sujetos pasivos, pues incluye a todos los archivos o registros de datos de carácter personal, públicos o privados, contiene como excepción a los archivos que se elaboran para ejercitar las libertades de expresión e información. Veamos:

"Artículo 1: El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectué en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19º, N° 12 de la Constitución Política (...)"

6. Los principios en materia de protección de datos personales

La legislación comparada suele contemplar una serie de principios que orientan y guían el tratamiento de datos personales desde su fase inicial de acopio o recolección, hasta su etapa final de cancelación, supresión o eliminación. Estas pautas deben ser observadas por los sujetos responsables del tratamiento de datos personales. Consideramos que las más relevantes son las siguientes:

6.1. El principio de Pertinencia o Necesidad

Este principio demanda que los datos objeto de tratamiento sean idóneos o útiles para alcanzar la finalidad para la cual han sido registrados. Consecuentemente, impide el tratamiento de los datos que no coadyuven con el cumplimiento de la finalidad que justificó su incorporación al registro.

Para determinar si la inclusión de determinados datos personales en un registro o banco de datos es respetuosa de este principio, deberá analizarse si su registro resulta adecuado o idóneo en relación con la finalidad del banco de datos. Se trata, en suma, de "cotejar que los datos a tratar estén razonablemente conectados con las necesidades y finalidad del registro"[27]. Como es posible advertir, este principio despliega su eficacia, principalmente, en la fase de acopio o registro de los datos personales.

Así, por ejemplo, en una base datos destinada a brindar información de carácter comercial o central de riesgo crediticio, no tendría porque encontrarse registrada información distinta a la información de naturaleza patrimonial. Consecuentemente, la inclusión de la relación de instituciones donde ha laborado una persona resultaría contraria al principio de Pertinencia, toda vez que a partir de dicha información no es posible dar cuenta del cumplimiento de las obligaciones comerciales de su titular.

Puede suceder que un dato inicialmente pertinente deje de serlo con el transcurso del tiempo. En dicho caso, corresponde al sujeto pasivo cancelar el dato personal del archivo, o, en su defecto, al titular de dicha información exigir la cancelación o borrado del dato que ha devenido en inútil.

6.2. El Principio Finalista

De acuerdo al principio Finalista el uso de datos de carácter personal debe ser coherente con la finalidad que motivó su registro. De este modo, se pretende evitar el uso abusivo de la información personal. A diferencia del principio de la Pertinencia, el principio Finalista es de aplicación cuando los datos personales ya han sido incorporados en un archivo o banco de datos y despliega su eficacia, prioritariamente, frente a la transmisión y suministro de datos a terceros.

Como ejemplo, podemos citar el caso del archivo de una clínica privada, en donde se encuentran registrados diversos datos personales (nombres, apellidos, dirección domiciliaria, teléfono, etcétera) y las historias clínicas de sus pacientes. El principio Finalista se vería afectado si se suministra la dirección postal y/o electrónica de los pacientes a distintas farmacias con el fin de que éstas les hagan llegar propaganda publicitaria sobre los medicamentos que expenden.

Otro ejemplo de su aplicación se encuentra en

(27) PUCCINELLI, Oscar. *Op. cit*.;p. 195.

la decisión del director de la Agencia Española de Protección de Datos de Carácter Personal frente al uso de los datos personales de los vecinos inscritos en el Padrón Municipal de Habitantes de un ayuntamiento. Se cuestionó que las autoridades ediles, usando los datos del padrón de habitantes, hicieran llegar a los vecinos una tarjeta de felicitación por su cumpleaños. La decisión de la Agencia consideró que el uso de los datos personales que constaban en el referido padrón, resultaba incompatible con la finalidad prevista legalmente, por lo que resultaba violatoria del principio Finalista(28).

Como se aprecia, para que este principio resulte afectado no tiene que verificarse ningún daño o perjuicio adicional al uso no consentido e incoherente con la finalidad para la cual fueron recabados los datos personales.

6.3. El principio de Caducidad

Según el principio de Caducidad o de Temporalidad, el registro de la información personal adversa o socialmente reprobable se encuentra sometido a un término de caducidad por lo que resulta inadmisible su conservación indefinida(29). Consecuentemente, transcurrido un plazo razonable, el titular de dichos datos tiene el derecho a exigir la cancelación de la información del respectivo archivo.

A falta de previsión legal, la Corte Constitucional Colombiana ha desarrollado este principio en asuntos relativos al registro de datos negativos debido al incumplimiento de obligaciones financieras. En este sentido, ha señalado que: "La permanencia de los datos en (…) los sectores financiero y comercial debe ser razonable, y la existencia de un término de caducidad del dato -tal que permita la rehabilitación de quien incurrió en mora-, forma parte de esa razonabilidad"(30). Según considera la Corte, si bien resulta legítimo y útil el registro de datos referidos al incumplimiento de obligaciones crediticias, transcurrido un plazo razonable los titulares de dicha información ostentan una suerte de derecho al olvido. Así, ha sostenido: "el deudor tiene derecho a que la información se actualice, a que ella contenga los hechos nuevos que le beneficien (…) Y, por lo mismo, también hacia el pasado debe fijarse un límite razonable, pues no sería lógico ni justo que el buen comportamiento de los últimos años no borrara, por así decirlo, la mala conducta pasada"(31).

Las legislaciones en materia de protección de datos personales suelen incorporar previsiones inspiradas en este principio, sobretodo en lo atinente a los datos referidos a la solvencia patrimonial. Así, por ejemplo, la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de datos de carácter personal de España establece en el inciso 4 de su artículo 29 que: "Solo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a mas de seis años, siempre que respondan con veracidad a la situación actual de aquéllos".

Por su parte, el articulo 10 de la Ley 27489, Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información, dispone que las CEPIRS no podrán contener en sus bancos de datos, ni difundir en sus reportes de crédito la siguiente información:

"d) Información referida al incumplimiento de obligaciones de naturaleza civil, comercial o tributaria, cuando (i) la obligación se haya extinguido y hayan transcurrido 2 (dos) años desde su extinción; o (ii) 5 (cinco) años desde el vencimiento de la obligación. Estos plazos no rigen si el titular ejerce el derecho de cancelación de acuerdo a lo establecido en el inciso b) del artículo 13º de la presente Ley. (...)

(28) Agencia Española de Protección de Datos. Procedimiento AAPP/00002/2006. Resolución: R/00413/2006.
(29) MURILLO DE LA CUEVA, Pablo Lucas. *Op. cit.*; p. 68 y 69.
(30) Corte Constitucional colombiana, sentencia T-121/97, fojas. 2.2.
(31) Corte Constitucional colombiana, sentencia SU-082/95, fojas. 9.

e) Información referida a sanciones exigibles de naturaleza tributaria, administrativa u otras análogas de contenido económico, cuando (i) hayan transcurrido 2 (dos) años desde que se ejecutó la sanción impuesta al infractor o se extinguió por cualquier otro medio legal, y (ii) 5 (cinco) años desde que se impuso la sanción".

6.4. El principio de Veracidad

La veracidad supone la correspondencia del dato personal con la realidad. Según ha sostenido la Corte Constitucional Colombiana, este principio supone que la información registrada debe ser actual y completa. La actualidad exige que los datos registrados reflejen la situación presente de su titular. Al respecto, ha señalado: "Los datos que se consignan en las centrales informáticas no pueden tener el carácter de inmodificables. Son eminentemente variables, en la medida en que evolucionan los hechos en que se apoyan. Por lo tanto, pierden vigencia cuando discrepan de lo acontecido en la realidad y tal situación debe reflejarse necesariamente en su actualización"(32).

Adicionalmente, la información personal incorporada en un archivo o banco de datos debe ser completa. Ello supone que los datos personales registrados deben ser suficientes para describir adecuadamente la situación real del titular, sin generar confusión. Como ejemplo de su aplicación, podemos citar la decisión de la Corte Constitucional Colombiana en la que explica esta característica:

"En lo atinente a un crédito, por ejemplo, un banco no daría información completa, si se limitara a expresar que el deudor ya no debe nada y ocultara el hecho de que el pago se obtuvo merced a un proceso de ejecución, o que la obligación permaneció en mora por mucho tiempo. Igualmente, no seria completa si no se informara que el cliente esta a paz y salvo"(33).

6.5. El Principio de Exactitud

El principio de Exactitud se encuentra emparentado con el Principio de Veracidad anteriormente desarrollado. Este principio exige que la información personal se presente de forma tal que permita transmitir la realidad. Mientras que la exigencia de que la información registrada resulte completa demanda que los datos sobre determinada situación sean suficientes para transmitir la realidad descrita; la exactitud alude más bien al aspecto cualitativo, exigiendo precisión.

Es importante mencionar que el respeto a los principios de Veracidad y Exactitud conllevan por parte del sujeto pasivo un especial deber de diligencia. Ello exige la adopción de todas las medidas razonables para mantener la información personal registrada debidamente actualizada y en correspondencia con la realidad. Por ello, una vez producido un cambio, deben disponer la actualización de la información a la brevedad. En su defecto, corresponderá al titular de la información exigir su modificación.

6.6. El Principio de Lealtad y Licitud

La lealtad y licitud apuntan a resguardar que la recolección de datos de carácter personal se realice por medios legales y sin recurrir a prácticas fraudulentas o de mala fe. En aquellos ordenamientos en los que el derecho a la protección de datos ha sido objeto de desarrollo, la legislación suele prever requisitos que legitiman el tratamiento de datos personales cuyo incumplimiento supone la violación al principio de licitud.

Por su parte, el concepto de lealtad demanda que las acciones encaminadas a obtener información personal para su inclusión en un banco de datos, no recurran a formas encubiertas que impidan al titular de dichos datos aceptar o rechazar el tratamiento(34). De este modo, se entienden proscritas las prácticas tendentes a recoger información a través del engaño o el fraude(35).

(32) Corte Constitucional colombiana, sentencia T-303/98.
(33) Corte Constitucional colombiana, sentencia SU-082/95.
(34) PUCCINELLI, Oscar. *Op. cit*.; p. 196.
(35) GOZAÍNI, Osvaldo Alfredo. *Derecho Procesal Constitucional. Habeas Data. Protección de datos personales. Doctrina y jurisprudencia*. Buenos Aires: Rubinzal- Culzoni Editores. pp. 92-196.

Karin Castro Cruzatt

7. Las facultades del derecho a la protección de datos de carácter personal

El derecho a la protección de datos de carácter personal se caracteriza por ser un derecho de contenido complejo, pues se encuentra integrado por distintas facultades o derechos específicos. El ejercicio de estas facultades permite a su titular controlar el uso de la información referida a su persona. Como podrá intuirse, su número y alcance puede variar de un ordenamiento jurídico a otro. Por nuestra parte, estimamos que las más relevantes son las siguientes:

7. 1. El derecho de acceso al registro o archivo

El derecho de acceso permite al titular de los datos conocer la información registrada sobre su persona. Este derecho actúa como presupuesto para el ejercicio de las facultades que integran el derecho a la protección de datos de carácter personal: conociendo el contenido de la información personal registrada, se podrá detectar su carácter inexacto, desactualizado o erróneo, tras lo cual será exigible su rectificación, actualización o eventual exclusión.

Para efectivizar su ejercicio las legislaciones nacionales suelen establecer el acceso gratuito y periódico por parte de los titulares de los datos personales objeto de registro. En este sentido, el articulo 15 de la norma argentina sobre protección de datos personales, Ley 25326, reconoce el derecho del titular a obtener información sobre sus datos personales incluidos en los bancos de datos públicos o privados destinados a proveer informes. Se precisa que dicho derecho podrá ejercerse de forma gratuita, en intervalos de por lo menos seis meses. En el ámbito nacional, la Ley 27489 establece en su articulo 14 que los titulares podrán acceder anualmente o cuando la información contenida en los bancos de datos haya sido objeto de rectificación, a la información crediticia que les concierne de forma gratuita.

7.2. El derecho de actualizar los datos personales

Este derecho permite a su titular la puesta al día de aquella información que ha dejado de ser cierta por el cambio de circunstancias acaecido con el transcurso del tiempo. Esto se logra "completando la información que quedó temporalmente superada o sustituyéndola por una nueva"[36]. Ejercitando esta facultad una persona podría solicitar la actualización del registro en donde aparece calificado como deudor por el incumplimiento del pago de una obligación dineraria, si es que posteriormente ha procedido al pago de la misma.

7.3. El derecho a la rectificación de datos personales

El derecho a la rectificación permite al titular de los datos personales exigir la corrección o modificación de la información consignada de manera errónea. Consideramos que el derecho a la rectificación puede tener como finalidad corregir información consignada de forma errada, o la modificación de aquélla que es presentada de manera imprecisa o inexacta.

7.4. El derecho a impedir el suministro de información

No siempre el titular de la información personal se encontrará habilitado para impedir el registro de información de tipo personal, pues pueden existir causas que justifican la necesidad de su incorporación en un archivo o registro. Sin embargo, el titular de los datos puede impedir el suministro de dicha información a terceros cuando se trate de información de carácter íntimo o de tipo sensible. De este modo, aunque no sea posible exigir a los hospitales públicos que excluyan las historias clínicas de los asegurados que reciben tratamiento médico, si será viable controlar que dichos datos no sean facilitados a terceros.

Entendemos que también procedería ejercitar esta facultad cuando la información de carácter personal se transmita a terceros y dicha comunicación no tenga conexión con las finalidades que justificaron la inclusión de los datos personales en el registro.

(36) PUCCINELLI, Oscar. *Op. cit*.; p. 294.

7.5. El derecho de cancelación

A través de este derecho resulta factible exigir al archivo o registro la exclusión o cancelación de la información personal. Ello puede deberse al carácter íntimo o sensible de la misma, a que se encuentre almacenada sin consentimiento de su titular o sin que medie justificación legal para ello. Este será el caso de una central de riesgo crediticia que almacena indebidamente información referida a la pertenencia a un partido político de una persona. También procedería la cancelación cuando se conserve información personal que ha devenido en caduca; o cuando su registro resulte impertinente. Finalmente, es factible exigir la cancelación de los datos personales cuando su titular revoque el consentimiento que prestó para su incorporación en el banco de datos.

8. Reconocimiento constitucional del derecho a la protección de datos personales

En el Perú, el derecho a la protección de datos personales ha sido reconocido por primera vez en la Constitución de 1993. El inciso 6 de su artículo 2 lo concibe como la facultad de toda persona: "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". Además, el inciso 4 del artículo 200 de la Carta vigente prevé la existencia del proceso constitucional de Habeas Data para su tutela. Como ya ha sido advertido en nuestro medio, la fórmula constitucional consagra el derecho a la protección de datos personales de forma sesgada, guardando silencio respecto de los elementos básicos que configuran este derecho[37]. Estas insuficiencias se ponen de manifiesto en tres aspectos que pasaremos a comentar brevemente.

En primer término, la Constitución establece una relación de interdependencia entre el derecho a la protección de datos de carácter personal y el derecho a la intimidad personal. Como sostuvimos anteriormente, si bien este derecho surgió como parte del desarrollo del derecho a la intimidad, su evolución lo ha configurado como un derecho autónomo y con un ámbito de protección distinto al que corresponde al derecho a la intimidad personal[38]. En tal sentido, a través del ejercicio de las facultades que integran el derecho a la protección de datos personales, es posible controlar la recolección y uso de los datos personales, con o sin contenido íntimo.

La segunda crítica que se ha planteado es que el inciso 6 del artículo 2 de la Carta Política hace mención a solo una de las distintas facultades que integran el derecho a la protección de datos personales, a saber: el impedir el suministro de informaciones. Como es sabido, este derecho comprende un conjunto de poderes cuyo ejercicio resulta vital a efectos de controlar la información personal almacenada en cualquier tipo de archivo: el derecho de acceso, la actualización, rectificación y cancelación o exclusión de información personal[39].

Como último punto, el Texto Constitucional alude a los sujetos pasivos u obligados de este derecho denominándolos servicios informativos, lo cual podría sugerir que solo se encuentran comprendidas bajo los alcances de la norma constitucional las entidades (públicas o privadas) cuya actividad principal es el suministro de información a terceros. Desde esta perspectiva, se podría concluir que este derecho no es exigible frente a entidades que, sin tener como finalidad principal el suministro de información a terceros, cuentan con registros o bancos de datos personales

(37) EGUIGUREN PRAELI, Francisco. *El Habeas Data y su desarrollo en el Perú.* En: *Derecho PUCP.* Número 51, diciembre de 1997. pp. 291-310. También en: Estudios Constitucionales. Lima: Ara Editores, 2002. pp. 183-206. GARCÍA-COBIÁN CASTRO, Erika: *El derecho a la autodeterminación informativa: diez años después. Análisis y propuestas de reforma*. En: *Revista Jurídica del Perú*. Año LIV. Número 55, marzo-abril de 2004. pp. 95-105.

(38) Sobre la autonomía hoy casi generalmente aceptada entre el derecho a la protección de datos y el derecho a la intimidad se pronuncia en nuestro medio: GARCÍA-COBIÁN CASTRO, Erika: Op. Cit., pp. 98-102.

(39) EGUIGUREN PRAELI, Francisco. *Op. cit.*; p. 301.

que utilizan como apoyo a sus funciones. Este sería el caso, por ejemplo, de los archivos de datos que organizan diversos establecimientos de salud públicos o privados o de aquellos que mantienen las distintas dependencias de la administración pública(40).

9. Los aportes de la jurisprudencia del Tribunal Constitucional y del Código Procesal Constitucional

La jurisprudencia constitucional referida al derecho a la protección de datos personales resulta verdaderamente escasa. Pese a ello, y a propósito de demandas cuyo objetivo no siempre ha sido la protección del derecho objeto de estudio, el Tribunal Constitucional ha tenido oportunidad de precisar sus alcances. Merece especial atención la sentencia que puso fin al proceso de habeas data tramitado bajo el expediente 1797-2002-HD/TC, en la cual el Tribunal explicitó el contenido del derecho reconocido en el inciso 6 del articulo 2 de la Carta, al que denominó autodeterminación informativa. En dicha oportunidad, el Tribunal tomó distancia de la identificación entre el derecho a la intimidad y el derecho a la protección de datos personales que venía defendiendo hasta ese entonces(41):

"3. El derecho reconocido en el inciso 6) del artículo 2º de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar (…) Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen"(42). Resulta positivo que en la misma sentencia, siguiendo lo señalado en anteriores pronunciamientos y frente al contenido limitado que le reconoce la Constitución, el Tribunal haya precisado las facultades que integran este derecho. Es importante destacar que en esta decisión el Tribunal expresa una comprensión más integral de las facultades de impedir el suministro de datos personales y de exigir la cancelación de los mismos, pues no supedita su ejercicio a que los datos personales objeto de exclusión o reserva sean íntimos o sensibles:

"4. (…) la protección del derecho a la autodeterminación informativa (...) comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, (...) Asimismo, con el derecho en referencia (...), un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados".

Debemos puntualizar, sin embargo, que en decisiones posteriores el Tribunal ha retomado esta errónea identificación entre el derecho a la intimidad y la protección de datos personales o autodeterminación informativa. Así, se ha referido al derecho reconocido en el inciso 6) del articulo 2º de la Constitución sosteniendo que: "dicho atributo solo se circunscribe a

(40) *Ibid*.; p. 300.
(41) *Ibid*.; pp. 101 y 102.
(42) Expediente 1797-2002-HD/TC, sentencia expedida el 29 de enero de 2003, fojas.3.

garantizar que la información o los datos de la persona no puedan ser utilizados en detrimento de su intimidad"(43).

Siguiendo la misma línea, al sentenciar el proceso de habeas data tramitado bajo el Expediente 10614-2006-PHD/TC, el Tribunal hizo referencia a la autodeterminación informativa como "3. (...) el derecho a mantener en reserva la información que pueda afectar su intimidad personal y familiar". Cabe apuntar, sin embargo, que en esta misma decisión el Tribunal hizo referencia a las distintas facultades que integran este derecho y estimó la demanda que exigía la actualización y rectificación de la información referida a la persona del demandante. En el caso citado, el actor exigía la actualización de la información sobre el pago de una deuda que ya había cancelada a su acreedor; y la rectificación de la información registrada en una central de riesgo en la que se le calificaba como cliente pérdida, pese a que ya había cumplido con el pago total de la acreencia. Este ha sido uno de los pocos casos resueltos por el Tribunal en donde la controversia ha girado en torno a la afectación del derecho a la protección de datos personales o autodeterminación informativa.

Por su parte, el Código Procesal Constitucional, vigente desde el 01 de diciembre del año 2004, regula el proceso de Habeas Data, destinado a la protección del derecho a la protección de datos personales o autodeterminación informativa y al derecho a acceder a información en poder de las entidades del Estado. El inciso 2 de su artículo 61 dispone que toda persona puede promover un proceso de habeas data para obtener tutela del derecho a:

"2. Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades publicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

Según se puede advertir, el Código menciona las principales facultades del derecho a la protección de datos personales, con lo cual viene a complementar los aportes del Tribunal Constitucional en esta materia. Nos suscita cierta preocupación lo prescrito en el Código en torno a las facultades de supresión o cancelación y de impedir el suministro a terceros. En este aspecto, la norma establece una clara conexión entre el ejercicio de dichas facultades y la información a la que denomina sensible o de carácter privado que afecte derechos constitucionales. No cabe cuestionar la referencia expresa a la información sensible que ha realizado el Código, aunque el lugar idóneo para ello debiera ser una ley general de protección de datos personales en donde, entre otros aspectos, se establezca un régimen de protección reforzada para la información de naturaleza sensible. Empero, consideramos que la mención a la información de carácter privado podría asimilarse -erróneamente- con información de naturaleza íntima y, como ya hemos sostenido, las facultades de cancelación y de reserva se ejercen frente a todo tipo de datos personales, aunque no sean necesariamente íntimos ni sensibles. Por ello, hubiera sido preferible que el Código aluda más bien a información o datos personales y no introduzca una noción que puede generar confusión.

La revisión del Estudio Preliminar elaborado por los profesores que participaron en la elaboración del proyecto del Código Procesal Constitucional permite confirmar que el sentido de la norma apunta en la dirección que hemos cuestionado. En dicho documento se hace referencia las facultades de supresión y reserva señalando que su finalidad es: "lograr la exclusión o supresión de los datos "sensibles", que no deben ser objeto de registro ni de difusión, a fin de salvaguardar la intimidad personal o de impedir la eventual discriminación; así como poder oponerse a la transmisión y difusión de los mismos"(44).

(43) Expediente 4602-2005-PHD/TC, resolución expedida el 4 de agosto de 2005, fojas. 4 y Expediente 1052-2006-PHD/TC, sentencia expedida el 14 de marzo de 2006, fojas. 2.

(44) AUTORES VARIOS. *Código Procesal Constitucional. Estudio Introductorio, Exposición de Motivos, Dictámenes e Índice Analítico*. Tercera edición. Lima: Palestra, 2008. p. 77.

Adicionalmente, encontramos poco acertada la alusión a la afectación a derechos constitucionales que el Código parece exigir para el ejercicio de las facultades anteriormente señaladas. Y es que, si bien el derecho a la protección de datos personales goza de un carácter instrumental, en la medida que es frecuente que se muestre como un presupuesto para el ejercicio de otros derechos fundamentales, ello no supone que el ejercicio de las facultades que lo integran se encuentre condicionado a que se verifique la violación o amenaza de otro derecho. En tal sentido, consideramos que el Código podría facilitar una opción interpretativa que limite los alcances del derecho irrazonablemente.

Por otra parte, el Código indica con acierto que el derecho objeto de estudio supone la posibilidad de controlar la información personal registrada "en forma manual, mecánica o informática". En efecto, si bien la protección de datos personales surge como reacción ante el riesgo derivado del tratamiento informatizado de datos personales, ello no supone que el tratamiento de información personal almacenada de manera manual o mecánica no deba ser objeto de tutela.

Ahora bien, de acuerdo a lo previsto en el Código Procesal Constitucional el Habeas Data puede dirigirse contra "archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros". En tal sentido, serán sujetos pasivos de este derecho aquellos registros destinados a proveer información a terceros, es decir, los que "brinden servicio a terceros"; y los que "brinden acceso" a terceros. El primer supuesto planteado por el Código no ofrece dificultad. La norma hace referencia a los archivos o registros públicos o privados que se dedican al servicio de suministro de información. Sin embargo, es necesario esclarecer qué bases o archivos serían considerados como aquellos que "brindan acceso a terceros". Cabría preguntarse si con ello el Código ha querido aludir a las instituciones que, aunque no brinden el servicio de suministro de información, deben procesar un caudal considerable de información personal y organizarla en bancos de datos o archivos para facilitar las actividades que desarrollan.

10. Una tarea pendiente: el desarrollo normativo de la protección de datos en el Perú y su necesaria armonización con otros derechos fundamentales

Como es sabido, en la actualidad nuestro país no cuenta con una ley que desarrolle el derecho a la protección de datos personales, existiendo más bien regulación parcial y dispersa en algunos de los aspectos vinculados con este derecho. Ello supone que gran parte de las normas jurídicas que por la materia que regulan, tienen incidencia en el registro y uso de información personal, no incorporan una perspectiva que atienda a la facultad del titular de dichos datos de controlar su uso, lo que puede generar situaciones de desprotección.

La situación descrita se pone de manifiesto con especial intensidad en el contexto de la información personal que se encuentra en poder del Estado. Sobre el particular, merece especial atención la dificultad que comporta lograr armonizar el derecho a la protección de datos personales y el derecho de acceso a la información pública, reconocido en el inciso 5 del artículo 2 de la Constitución; y que tiene como excepciones la información relativa a la intimidad personal, a la seguridad nacional, al secreto bancario, la reserva tributaria y la información excluida a través de una ley[45]. Este derecho supone la facultad de toda persona de recibir de las entidades que

(45) Esta situación ha sido puesta de manifiesto en la la Conferencia Nacional sobre Acceso a la Información, realizada los días 29 y 30 de septiembre de 2008 en la ciudad de Lima. En dicha ocasión se llamó la atención sobre el eventual conflicto que se podría presentar entre el derecho de acceso a la información pública y el derecho a la autodeterminación informativa: "(...) en muchos casos, la entrega de información contenida en dichos registros, listados o bases de datos, en virtud del derecho de acceso a la información pública, podría afectar el derecho a la autodeterminación informativa de las personas. Más aún si se tiene en cuenta de que en el Perú no existe una ley de desarrollo del derecho a la autodeterminación informativa": PEREIRA CHUMBE, Roberto. Algunas cuestiones problemáticas en materia de transparencia y acceso a la información

desarrollan funciones públicas la información que tengan bajo su control, previa solicitud de la misma. Debemos precisar además que la obligación que la Constitución impone a las entidades públicas de facilitar o proporcionar información no se encuentra limitada a la documentación oficial, como por ejemplo, las actas, oficios o resoluciones. Tampoco se restringe a la información producida por las entidades públicas, sino que incluye a la que sin haber sido elaborada por éstas, se encuentra en su poder (Principio de Posesión)(46). Como vemos, la información a la que se puede acceder ejercitando el derecho consagrado en el inciso 5 del artículo 2 de la Carta incluye un abanico bastante amplio de datos y documentos.

«UN RASGO ESENCIAL Y A LA VEZ DETERMINANTE PARA CALIFICAR A UN DATO PERSONAL COMO SENSIBLE, ES QUE ALUDE A CUESTIONES CUYA DIVULGACIÓN O COMUNICACIÓN A TERCEROS PUEDE DAR LUGAR A PRÁCTICAS DISCRIMINATORIAS».

Pues bien, si consideramos que el derecho a la protección de datos personales no cuenta en estos momentos con un desarrollo normativo que permita delimitar su contenido y alcances, la tarea de armonizar este derecho con el acceso a la información pública puede complicarse. Asimismo, la excepción de acceder a la información en poder del Estado que se encuentre referida a la intimidad personal, establecida en el inciso 5 del artículo 2 de la Carta, es insuficiente para limitar el acceso de terceras personas a la información personal en poder de las entidades públicas. Esto se debe a que, como hemos visto, el derecho reconocido en el inciso 6 del artículo 2 de la Constitución no se limita a tutelar los datos de naturaleza íntima.

Consideramos que esta situación de indefinición puede perturbar el ejercicio de ambos derechos. Así, podría generar una interpretación excesivamente amplia de lo que debe entenderse por dato o información personal, impidiendo irrazonablemente el acceso a la información que debe ser de conocimiento público. Pero, por otra parte, podría fortalecer o incentivar la identificación entre información personal e información íntima, limitando el control sobre la información personal a la que tenga naturaleza íntima.

Para ilustrar lo señalado, podemos citar el proceso de habeas data iniciado por Luis Francisco Roggero Luna contra el Director de la Morgue de Lima. El demandate, amparándose en el derecho de acceso a la información pública, exigía conocer los nombres y apellidos de las personas fallecidas como consecuencia de accidentes de tránsito, su dirección domiciliaria, así como los nombres, apellidos, dirección y teléfonos de las personas que reclamaron sus cadáveres. Al sentenciar el caso el Tribunal Constitucional señaló lo siguiente:

"4. […] aunque el demandante invoca que ha sido vulnerado su derecho de acceso a la información pública por el hecho de no

pública. Documento de trabajo. pp.3 y 4. Asimismo, en la exposición de motivos del Proyecto de la Ley de Protección de Datos Personales, publicado en el diario oficial El Peruano el 23 de julio de 2004 se afirmaba: "(…) actualmente se viene dando mucha importancia a la regulación del acceso a la información que tiene o produce el Estado, la misma que se encuentra almacenada en las entidades públicas, situación que pone en riesgo, aún más, los datos personales de los ciudadanos y de las personas en general". p. 11.

(46) ABAD YUPANQUI, Samuel. *Transparencia y acceso a la información pública*. En: *Derecho de Acceso a la Información Pública*. Piura: Defensoría del Pueblo, 2005. p. 22. A ello habría que añadir la *presunción de publicidad* con la cuenta toda la información en poder del Estado, así como el carácter estricto con el que se deben interpretar las excepciones del derecho de acceso a la información pública; ambas pautas se encuentran recogidas en la Ley de transparencia y acceso a la información pública.

habérsele proporcionado información sobre determinados datos pertenecientes a las personas fallecidas en circunstancias de un accidente de tránsito, así como información concerniente a los familiares de los citados fallecidos, omite considerar que la misma, por sus alcances, podría repercutir en la esfera íntima y privada de estos últimos, cuyos datos no tienen por qué ser puestos en conocimiento de nadie sin su libre y voluntario consentimiento"(47).

En el caso citado, el demandante solicitaba el acceso a datos personales de terceras personas, pedido que acertadamente le fue denegado. La sentencia del Tribunal alude a la eventual afectación de la intimidad y privacidad de los involucrados, cuando en realidad el caso planteaba una solicitud de información personal formulada por una persona distinta al titular de la misma, lo cual no puede considerarse parte del contenido constitucionalmente garantizado del acceso a la información.

Como punto final, deseamos señalar que la legislación que desarrolle el derecho a la protección de datos personales deberá tener en cuenta también el respeto a otros principios y derechos cuya vigencia resulta fundamental en un estado democrático. En este sentido, el desarrollo normativo del derecho a la protección de datos personales supone un reto que exige la tarea de armonizar los principios de Transparencia y Publicidad en la gestión de la cosa pública, así como el derecho de acceso a la información pública, con el necesario respeto del derecho de toda persona de controlar la información que a ella concierne, para garantizar así su dignidad y libertad. En este sentido, si bien los aportes de ordenamientos foráneos son necesarios y útiles, es indispensable mirar hacia adentro y no perder de vista ambos objetivos.

(47) Expediente 5379-2006-PHD/TC, sentencia expedida el 23 de octubre de 2007.