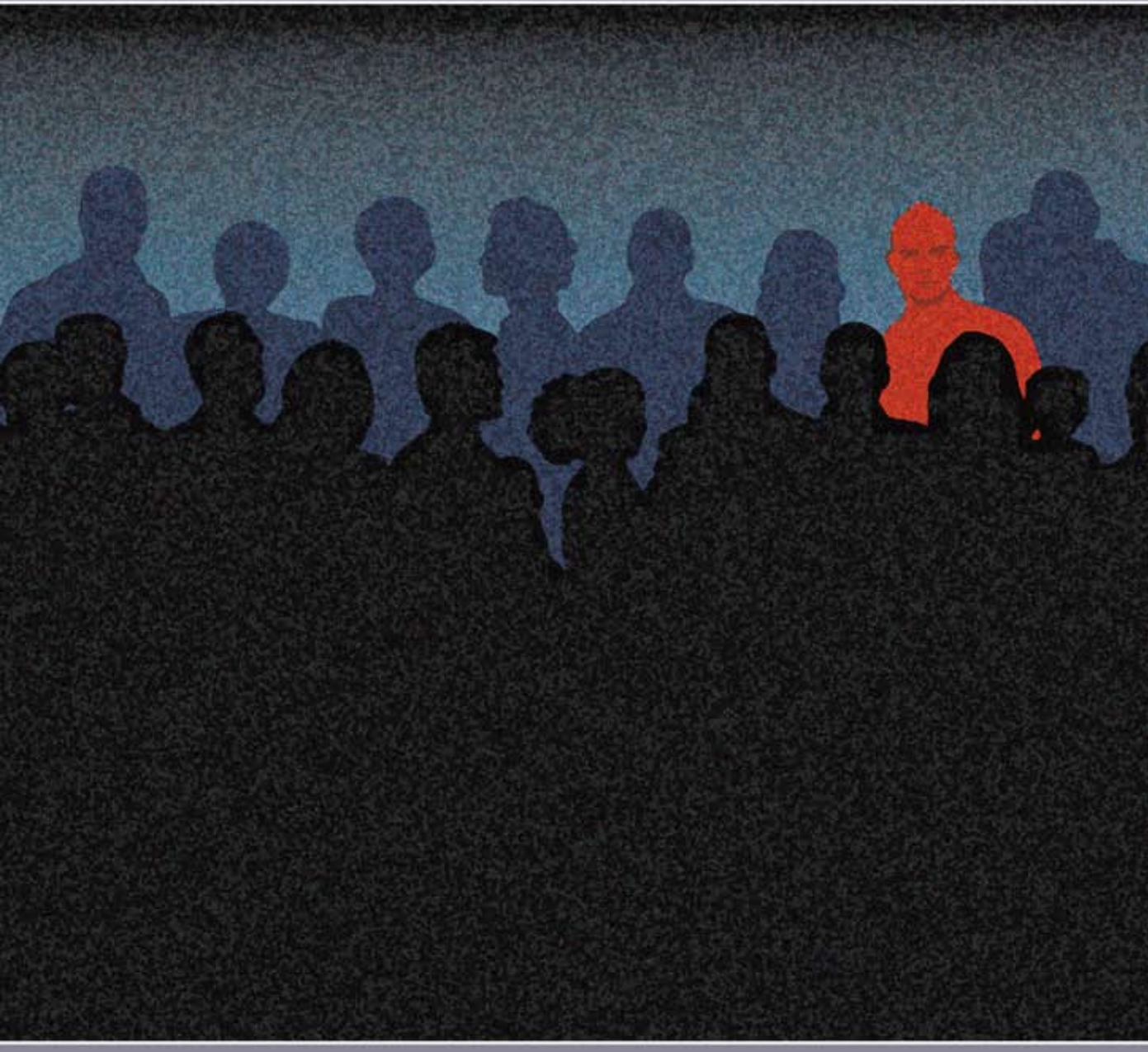
Reflexiones sobre el Uso y Abuso de los Datos Personales en Chile



expansiva

Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile

expansiva

Reflexiones Sobre el Uso y Abuso de los Datos Personales en Chile
I.S.B.N: 978-956-8678-04-3

Publicado en Santiago de Chile, marzo 2011

Impresión: Andros Impresores

Índice

I
Presentación

Raúl Arrieta Cortés
Coordinador

En la época en que vivimos las personas dejan huellas electrónicas, rastros de su identidad, comportamiento y preferencias en las bases de datos de los servicios que utilizan. Desde el momento en que se levantan van dejando marcas de su actuar cotidiano, al utilizar el teléfono, al circular por las autopistas urbanas, al pagar con una tarjeta de crédito, al registrarse en el ingreso a la oficina, al navegar por Internet, al comprar, etcétera. De este modo, a medida que las tecnologías se hacen más presentes en el quehacer diario, más huellas van quedando almacenadas, o lo que es igual, más rastros de las personas es posible encontrar. Junto a ello, hay muchas bases de datos y empresas que utilizan dicha información, sea capturándola, organizándola, vendiéndola y, en general, utilizándola.

En esta perspectiva es posible sostener que el desarrollo de las tecnologías de la información y comunicación van configurando una serie de cambios referidos a la forma en que las personas se relacionan con el entorno y, consecuentemente, con el modo en que las mismas se vinculan con la igualdad, libertad y dignidad, y en general con todos los derechos fundamentales.

En los últimos años mucho se ha discutido en nuestro país respecto a la necesidad de profundizar la regulación sobre la protección de datos personales, entendiendo que la finalidad de ésta es amparar a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos, con el fin de confeccionar información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad.

Con el presente trabajo colaborativo nos hemos propuesto abordar cómo en nuestro país se están tratando datos personales, básicamente buscando alimentar e ilustrar la discusión nacional sobre el tema, con la convicción de que la mejor forma de entender un derecho nuevo como la protección de datos

—que muchas veces aparece como difuso— es ilustrando situaciones en las cuales éste es o puede ser vulnerado. Asimismo, se pretende dotar al lector de propuestas de cambio o formas de abordar la problemática, de manera de poner coto, probablemente, a una de las principales fuentes de contaminación de las libertades de las personas.

Agradezco a cada uno de los autores con cuyos trabajos se encontrarán a continuación, así como también al Comité de Retail Financiero por su colaboración para que este libro fuera posible.

II
Autorregulación y protección de datos personales

Raúl Arrieta Cortés

I. Introducción

El aumento de la complejidad y la actual estructura corporativa de la sociedad, sumadas a la gran envergadura y diversidad de sus demandas, tienen excedida por completo la capacidad de respuesta del Estado frente al impacto de la tecnología sobre los derechos, de las personas. Ello origina que diariamente se vea sobrepasada la tutela de los derechos con lo que el sentimiento de infortunio ciudadano comienza a ser cada vez mayor.

Probablemente una de las áreas donde lo anterior tiene más significación en nuestro país es en lo que a tratamiento de datos personales se refiere, entendiendo por éste cualquier operación, complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos de cualquier otra forma.(1)

Basta con repasar un día cualquiera de un habitante de la ciudad de Santiago para tomar un mínimo de conciencia respecto de que prácticamente en todas las actividades que realizamos se pueden estar registrando nuestros datos, aunque la mayoría de las veces no tengamos ninguna conciencia de que ello está ocurriendo. Muchos de nosotros cotidianamente pagamos con algún medio electrónico, transitamos por las autopistas urbanas, empleamos tarjetas de identificación o registro magnético, encendemos nuestro computador e ingresamos a la red, nos autenticamos mediante un nombre de usuario y una clave en diferentes plataformas y para diferentes servicios, indicamos nuestro RUT al comprar en algún establecimiento, dando información acerca de nosotros mismos día a día y a cada minuto. Si bien estas acciones son en apariencia inocuas e indispensables para el quehacer cotidiano, no tenemos la menor idea respecto a qué se hace con toda la información que de ellas se recolecta y que, sin duda, permite obtener un sinfín de conclusiones en torno a nuestra persona.

(...) no tenemos la menor idea respecto a qué se hace con toda la información que de ellas se recolecta y que, sin duda, permite obtener un sinfín de conclusiones en torno a nuestra persona.

(1) Artículo 2° de la Ley 19.628, sobre protección de la vida privada.

De este modo, más allá de cualquier opinión o valoración subjetiva que tengamos sobre este punto, nos parece que sí es posible afirmar que el tratamiento de datos da espacio para construir perfiles de los individuos sobre la base de su quehacer, lo que indudablemente puede terminar produciendo estigmatizaciones, que junto con amenazar el legítimo ejercicio de los derechos individuales deterioran nuestra democracia al reconocer como normales condiciones de convivencia que erosionan los principios más elementales de una república democrática, fórmula utilizada por nuestra Carta Fundamental para establecer la forma jurídico-política del Estado.

(...) nos encontramos con que diariamente las personas están dejando rastros de su actuar y que lo que se hace con dicha información puede traer una serie de riesgos para ellas y la sociedad, a lo que se suma que el Estado se encuentra desbordado para hacer frente a estas situaciones.

En síntesis, nos encontramos con que diariamente las personas están dejando rastros de su actuar y que lo que se hace con dicha información puede traer una serie de riesgos para ellas y la sociedad, a lo que se suma que el Estado se encuentra desbordado para hacer frente a estas situaciones.

Ante esta situación han surgido diversas posiciones. Por una parte se encuentran un conjunto de corrientes doctrinales neoliberales que propugnan la innecesariedad del Estado. En contrapartida, están la Ciencia Política y el Derecho Administrativo que han propuesto encontrar soluciones alternativas, basadas en una modificación de las formas de actuación de los poderes públicos.

Lo anterior es especialmente relevante si consideramos que como resultado de la opacidad con que funcionan las tecnologías y que a consecuencia de ello el hombre medio no es capaz de conocer y entender la forma en que éstas operan, será sólo la acción del Estado, a través de su función de policía, la que posibilite una protección de los derechos frente a las consecuencias del desarrollo tecnológico, lo que obviamente habrá de tener lugar en una nueva forma de relación con la sociedad.

De este modo las siguientes páginas fueron escritas con la convicción de que más que plantearse la eliminación del Estado, resulta indispensable bosquejar formas diferentes de acción para hacer frente a la incapacidad de reacción que hoy éste posee. Así, consideramos que no es posible seguir aplicando las categorías jurídicas tradicionales para resolver problemas que tienen un origen, un impacto y una realidad tan diferente a las que se tuvieron

en consideración a la hora de configurar nuestro marco jurídico. A partir de estas premisas sentaremos las bases de lo que consideramos ha de ser una propuesta que nos permita recurrir a la autorregulación como técnica de ordenación, propugnando la instrumentalización de normas y controles privados al servicio de fines públicos definidos por el propio Estado.

Cabe destacar que en ningún caso el presente trabajo sugiere recurrir a la autorregulación como medio de eliminación o sustracción de competencias públicas, sino que, muy por el contrario, se vislumbra como un mecanismo que permite —valiéndose de todas las capacidades privadas— asegurar una intervención del Estado efectiva y eficiente en la tutela de los derechos de las personas, impactados por el desarrollo tecnológico.

II. Regular la autorregulación: Una técnica de intervención administrativa

Hasta hace no mucho tiempo la autorregulación había sido vista como una alternativa privatista para que el mercado encuentre por sí mismo su propio equilibrio, mientras la regulación era percibida como el instrumento de que dispone el Estado para garantizar los equilibrios del mercado. Claramente se trata de mecanismos diferentes para la optimización del funcionamiento de éstos, donde por un lado es la propia sociedad la que busca y define cómo hacerlo y, por otro, es el Estado el que lo hace como garante y promotor del bien común. Así, estas técnicas tenían un claro matiz económico, al ser formas de intervención en el mercado.

Hasta hace no mucho tiempo la autorregulación había sido vista como una alternativa privatista para que el mercado encuentre por sí mismo su propio equilibrio, mientras la regulación era percibida como el instrumento de que dispone el Estado para garantizar los equilibrios del mercado.

No obstante, hace ya unas décadas en nuestros entornos de referencia, fundamentalmente en la Unión Europea, es posible ir advirtiendo algunos cambios en el modo en que se relaciona la autorregulación y la regulación. Así, se ha ido dando paso a una forma en la cual la primera empieza a convertirse en un instrumento utilizado por los poderes públicos que —bajo una apariencia de ampliación de la autonomía de la sociedad en la definición de sus reglas de conducta— ha logrado ir escondiendo una nueva forma de intervención estatal. A través de esta mutación lo que se

persigue es poner al servicio de objetivos públicos toda la capacidad técnica, económica y social de los privados para la consecución de fines públicos. De este modo, la autorregulación deja de ser un fenómeno estrictamente privado y la regulación estatal, en parte, se despoja de su tradicional carácter coactivo y autoritario y, simultáneamente, renuncia a intervenir directamente en ciertas relaciones sociales, siempre y cuando la ordenación de éstas manifieste con absoluta nitidez la satisfacción de los bienes públicos en cuestión.

(...) sin duda representa un riesgo el hecho de que sea la propia profesión o sector industrial el que fije las normas que habrán de ser seguidas para brindar la tutela de las libertades que se han visto contaminadas como consecuencia del desarrollo tecnológico.

Ahora bien, sin duda representa un riesgo el hecho de que sea la propia profesión o sector industrial el que fije las normas que habrán de ser seguidas para brindar la tutela de las libertades que se han visto contaminadas como consecuencia del desarrollo tecnológico. No es posible dejar de considerar que bajo esta figura se dota de poder y autoridad a ciertos sectores para que, amparados en el principio de corresponsabilidad en la gestión de los riesgos,[(2)] desarrollen sus propias estructuras normativas como complemento o alternativa a la legislación. Así, quienes aparecen, en último término, como los principales responsables de poner en riesgo los derechos de las personas con el desarrollo de su actividad, son los que imponen las reglas que les servirán para mostrarse como los férreos defensores de los derechos de sus clientes ante la insuficiencia de las regulaciones aprobadas por el Estado, o bien, como los principales interesados en adecuar la normativa general a sus particularidades, de manera de generar estándares adaptados a las necesidades del referido sector, facilitando su cumplimiento y asegurando la tutela de los derechos en éste.

Es por ello que consideramos que la autorregulación orientada a establecer pautas de conducta comunes a una serie de sujetos no es suficiente para solventar las lesiones que se pueden producir en los derechos de las personas.

(2) Se trata de un principio que ha sido impulsado en la Unión Europea que se materializa en la actuación conjunta del Estado y la sociedad para garantizar ciertos fines, constitucionalmente asignados exclusivamente a los Estados, como lo son la protección de la vida, de la integridad de las personas, de la salud, de la seguridad, del medio ambiente, entre otros, como consecuencia de la responsabilidad que le cabe a la propia sociedad en la generación de los riesgos sobre dichos fines, básicamente como consecuencia del desarrollo tecnológico.

Para que la autorregulación realmente sea útil y confiable estimamos que resulta indispensable que sea el propio Estado el que regule el contexto de ésta, lo que supone, por un lado, el establecimiento de sistemas de control de la misma y, por otro, la fijación legal o reglamentaria de: los fines que ésta debe cumplir; las normas procedimentales aplicables a la adopción de sus instrumentos; la composición de los organismos vinculados a ella; y los requisitos de capacidad técnica y de imparcialidad exigibles a los sujetos que se autorregulan. Sólo así será posible garantizar la existencia de un sistema en que las actividades de un sector se encuentran sujetas a un conjunto de normas y controles privados, pero asegurando las garantías fundamentales implicadas. Adicionalmente, facilita el control que hace el Estado sobre dichas actividades, ya que deja de necesitar un *expertise* detallado en cada una de ellas para centrar su accionar en la supervisión del buen funcionamiento de los sistemas de autorregulación.

Para que la autorregulación realmente sea útil y confiable estimamos que resulta indispensable que sea el propio Estado el que regule el contexto de ésta, lo que supone, por un lado, el establecimiento de sistemas de control de la misma (...)

Así, se sugiere un sistema de regulación pública de la autorregulación, donde la expresión "regulación" es utilizada como un instrumento con el que cuenta el Estado para ordenar una profesión o sector industrial mediante leyes y/o actos administrativos. Claramente se tratará de una manera de ordenar la forma en que podrá operar la autorregulación para asegurar que se logren generar a través de ella los equilibrios económicos y sociales pretendidos. Junto a ello, es importante tener en consideración que se trata de una regulación de policía, donde lo que el Estado persigue no es el correcto funcionamiento del mercado, como ocurre en la regulación económica, sino proteger una serie de derechos y bienes socialmente relevantes.

Es en ese contexto que consideramos que la autorregulación es capaz de generar efectos públicos y con ello servir como técnica de intervención administrativa que —no obstante representar una forma mucho más tenue de los mecanismos tradicionales— encarna un significativo medio de intromisión del Estado en las relaciones entre éste y la sociedad, permitiendo aprovechar y optimizar los recursos que ofrece la propia sociedad para garantizar la consecución efectiva de fines públicos y, con ello, adicionalmente, ampliar el alcance efectivo de la tutela del Estado hacia una gran diversidad de materias,

con complejidades técnicas significativas, al deber éste únicamente volcar sus esfuerzos y recursos en la función administrativa de control y supervisión.

III. Autorregulación regulada y protección de datos personales

Es en materia de protección de datos personales donde quizás nos encontramos frente a uno de los espacios en los que resulta más fácil advertir cómo el Estado se ha pasado discutiendo cuál es la mejor forma de incrementar los niveles de protección de los derechos de las personas, por el impacto que sobre los mismos ha tenido la capacidad, aparentemente ilimitada, de las nuevas tecnologías y telecomunicaciones para tratar información de los individuos en tiempo real. Así, con una simple visita al sitio web de la Biblioteca del Congreso Nacional(3) es posible encontrar una veintena de proyectos de ley en trámite que responden a la búsqueda por el criterio "protección de datos" y más de una treintena que responde al criterio "vida privada", en lo referido a tratamiento de datos.

(...) en los últimos diez años no ha pasado nada respecto a este tema, evidenciando así la tolerancia del Estado ante una evidente, flagrante y diaria vulneración de los derechos de las personas, tanto por los organismos públicos como por los privados.

Ello permite imaginar una fecunda discusión nacional sobre el tema, pero ésta ha sido más bien aparente pues en los últimos diez años no ha pasado nada respecto a este tema, evidenciando así la tolerancia del Estado ante una evidente, flagrante y diaria vulneración de los derechos de las personas, tanto por los organismos públicos como por los privados.

En ese escenario es que consideramos necesario que la sociedad aborde la solución de un problema tan estructural para la convivencia democrática y no siga esperando que sea sólo el Estado el que ampare los derechos. Parece indispensable recurrir al principio de corresponsabilidad y apelar a una técnica de intervención, como la autorregulación regulada, para que tanto la sociedad como el Estado jueguen el rol que les corresponde en la protección de los derechos de las personas y, con ello, mejorar la capacidad de las instituciones de cumplir el cometido más elemental de una sociedad, esto es, concurrir en la satisfacción de las necesidades de los nacionales. Para ello resulta indis-

(3) www.bcn.cl sección "Tramitación de Proyectos", búsqueda por "Palabra o Frase".

pensable que todos los actores que intervengan no escatimen sus esfuerzos en la configuración de un mínimo ético.

Ahora bien, probablemente en este punto podamos convenir que se trata de una de las cuestiones que más trabajo podría significar, pues llegar a ese mínimo o máximo ético implica poner en orden el mundo de los laberintos que se genera a partir de la diversidad de sistemas morales, de la confusión respecto del concepto de libertad humana, de la maraña de los valores, del problema del fin y los medios, o del enredo que se deriva de la "obligación moral".(4)

Sin embargo, en materia de protección de datos personales la cuestión no debería ser tan compleja si consideramos que con ella lo que se busca es permitir la libre circulación de los datos. Lo que realmente se desea es que la información fluya sin más restricciones ni trabas que las necesarias para asegurar que ese intercambio de información no termine por amenazar o conculcar los derechos de las personas. Así, en nuestro caso para determinar un mínimo ético, o al menos proponerlo, resulta imprescindible recurrir a la génesis de la Carta Fundamental, para lo cual no es vano recordar que el anteproyecto constitucional y sus fundamentos nos recuerdan que la Constitución, al disponer en su artículo 1º que "los hombres nacen libres e iguales en dignidad", ha querido consagrar esta norma no sólo inspirada en los preceptos de la Declaración Universal de los Derechos Humanos, sino especialmente en la tradición libertaria de Chile, respetuosa de la persona humana como ser dotado de inteligencia y voluntad libre por su creador. El respeto a la dignidad del hombre es pues el principio fundamental que inspira la nueva constitución.(5)

Lo que realmente se desea es que la información fluya sin más restricciones ni trabas que las necesarias para asegurar que ese intercambio de información no termine por amenazar o conculcar los derechos de las personas.

De este modo, cualquier construcción de un mínimo ético en materia de protección de datos personales debe considerar la libertad y la dignidad de la persona como núcleo esencial y, en tal sentido, tener en cuenta que frente a

(4) Corcoba, Victor. ¿Hasta dónde llega el mínimo ético? Consulta [02.01.2011] En Línea: http://clasica.xornal.com/article.php?sid=20061211113216

(5) Anteproyecto Constitucional y sus Fundamentos p.11, citado en Sentencia del Tribunal Constitucional chileno, Rol N° 46, de 21 diciembre de 1987, considerando 17. [en línea] http://www.tribunalconstitucional.cl/index.php/sentencias/view/563 [consulta: 19 de octubre de 2009].

dichos valores constitucionales no importa el parecer del titular de los datos, siempre será obligación del Estado protegerlos. Como consecuencia de ello cualquier estructura de protección de los mismos necesariamente ha de configurarse como un sistema de derechos para los titulares de carácter indisponible.

Ahora bien, para aproximarse a lo que podría ser una intervención del Estado en esta materia a través de una autorregulación con efectos públicos, es que consideramos conveniente recurrir a un concepto de autorregulación con vocación en la protección de datos, dado por la Unión Europea en el año 1998,[6] en cuya virtud se la puede definir como el conjunto de normas que se aplican a la pluralidad de responsables del tratamiento de datos que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión. Tal vez a dicha conceptualización únicamente sería conveniente agregarle que el contexto de la misma, es decir, la forma en que se produce, el contenido mínimo que ha de tener y el modo en que se controla se encuentran determinados por el propio Estado.

Así, cualquier reconocimiento que haga el Estado de sistemas privados de protección de datos personales ha de considerar que el asunto debe ser abordado dualmente, por una parte para dar una adecuada protección a los principios o valores que han de inspirar la protección de datos y que brindan contenido sustancial a la misma y, por la otra, para establecer normas de ejecución que permitan garantizar el cumplimiento de las normas dadas en la implementación de los referidos principios. De este modo, cualquier sistema autorregulativo, junto con fijar las normas de conducta, ha de configurar una estructura compleja de protección de las personas que sea capaz de articular un nivel satisfactorio de cumplimiento de las normas, apoyo y asistencia a los interesados en el ejercicio de sus derechos, y vías adecuadas de recurso a quienes resulten perjudicados por la no observancia del cumplimiento de las normas que se ha fijado la profesión o sector industrial de que se trate.

(...) cualquier sistema autorregulativo junto con fijar las normas de conducta, ha de configurar una estructura compleja de protección de las personas que sea capaz de articular un nivel satisfactorio de cumplimiento de las normas (...)

(6) Comisión Europea. Grupo de Trabajo sobre la Protección de las Personas Física en lo que respecta al tratamiento de datos personales. Documento de Trabajo DG XV D/5057/97: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos de un tercer país? Adoptado el 14 de enero de 1998.

En síntesis, un sistema de autorregulación en materia de protección de datos deberá considerar un código deontológico, un mecanismo de resolución alternativa de conflictos y atribución de efectos públicos a la autorregulación.

Código Deontológico

(...) un sistema de autorregulación en materia de protección de datos deberá considerar un código deontológico, un mecanismo de resolución alternativa de conflictos y atribución de efectos públicos a la autorregulación.

Partiremos por señalar que se trata de un conjunto de normas y deberes dirigidos a un colectivo para guiar la forma en que se desarrolla una actividad o profesión desde una perspectiva ética. Es por ello que se trata de un documento que plasma el "deber ser" sin intentar emitir juicios de valor respecto a cómo los destinatarios del código desarrollan sus labores. Así, lo que verdaderamente se persigue con éstos es establecer lo que está bien y mal para con ello precisar cuál es el comportamiento deseable por el sector o profesión cuando trata datos personales.

En lo que se refiere a su contenido, estimamos que deberá recurrirse a los principios en que se sustenta la protección de datos personales, entendiendo que éstos son una serie de preceptos informadores, con pretensión de carácter universal, que han de inspirar la forma y la oportunidad en que se desarrolla el tratamiento de datos personales por parte de los responsables del mismo y de los bancos de datos.(7) Sólo con la finalidad de facilitar la comprensión del asunto, esbozaremos las características primarias de cada uno de ellos, haciendo presente que los principios básicos de la protección de datos son los siguientes, sin que la numeración sea en ningún caso taxativa ni que su importancia esté estimada en función del lugar que ocupan en la lista que sigue:

a. La recogida de datos debe realizarse de manera justa y legítima: El tratamiento de datos personales debe efectuarse, por una parte, con la debida proporción y, por la otra, de manera lícita. La debida proporción está determinada por el hecho de que la recogida se haga de manera pertinente a sus propósitos y en ningún caso de manera excesiva en consideración a los ámbitos y finalidades legítimos para los cuales fueron obtenidos los datos personales.

(7) ARRIETA, R. "Chile y la Protección de Datos Personales: Compromisos Internacionales", en Chile y la Protección de Datos Personales: ¿Están en Crisis Nuestros Derechos? Serie Políticas Públicas. Ediciones Universidad Diego Portales 2009, p. 16.

La licitud de la recogida tiene que ver básicamente con el hecho de que ésta debe realizase con el consentimiento del interesado, para lo cual será indispensable que no se recurra a procedimientos ilícitos o desleales, de manera que el titular de los datos tenga la capacidad de saber en todo momento que sus datos están siendo recogidos, sea a través de sistemas manuales y/o automatizados.

b. Exactitud: El tratamiento de datos personales deberá realizarse de manera de brindar certidumbre respecto a la verdadera situación de su titular. Para ello el responsable del tratamiento tendrá que desarrollar su actividad velando porque los datos sean exactos y adoptando todas las medidas razonables para que éstos sean actuales y completos.

Que los datos sean actuales apunta a que sean capaces de reflejar la verdadera situación temporal de su titular, sólo así el uso que se haga de la información de una persona será capaz de dar cuenta de la verdadera realidad de la misma.

Que los datos sean actuales apunta a que sean capaces de reflejar la verdadera situación temporal de su titular, sólo así el uso que se haga de la información de una persona será capaz de dar cuenta de la verdadera realidad de la misma. Por su parte, que sean completos apunta a que importa que los datos tengan la capacidad de reflejar íntegramente la situación de su titular de manera de evitar errores de omisión.

Sólo en la medida que concurran copulativamente dichos elementos del principio será posible asignarle a esos datos un real valor y la posibilidad de producir lesiones en los derechos de las personas se verá disminuida.

c. Finalidad: Al momento de realizarse la recogida de datos personales, junto con el deber de informar al titular respecto de ésta y de requerirle su autorización para que pueda tener lugar, es necesario que se especifique el uso que se dará a los datos.

Al respecto resulta necesario considerar que al momento de precisar la finalidad de la recogida se fija el alcance de lo que el responsable del tratamiento de datos podrá hacer con ellos.

En ningún caso la autorización que una persona otorga para que traten sus datos personales puede ser entendida o considerada como un "cheque en blanco" para que se haga con ellos cualquier cosa.

Así, es la autorización que otorga el titular de los datos la que determinará los usos justos y legítimos de los mismos, por lo que es especialmente importante que en la publicidad de la finalidad se haga una clara alusión respecto a los fines, si los datos serán o no revelados a terceras personas, si serán cedidos, el período de tiempo por el cual serán almacenados, el que no debe en ningún caso ser superior al necesario para la consecución de los fines para los cuales han sido recolectados.

(...) es la autorización que otorga el titular de los datos la que determinará los usos justos y legítimos de los mismos (...)

De este modo la finalidad declarada por el responsable del tratamiento de datos personales, ya sea con anterioridad o en el momento mismo de efectuarse la recogida de los mismos, será la que determinará el contenido máximo de la autorización dada por el titular para su tratamiento, pues la información jamás podrá utilizarse para las finalidades incompatibles a las que se tuvieron en consideración al momento de realizar el tratamiento. Ello es especialmente importante si tenemos presente que los objetivos de los tratamientos posteriores pueden ser incompatibles con los objetivos originariamente especificados.

Finalmente, resulta importante considerar que la finalidad incompatible deberá analizarse siempre a la luz de la autodeterminación informativa, de manera tal que baste que la declaración que haga el responsable del tratamiento de datos sea suficiente como para que con la diligencia del hombre medio el titular de los datos sepa si la información facilitada será empleada según los fines para los cuales él consintió.

d. Proporcionalidad: Este principio viene dado por el hecho de que los datos que se recolecten de las personas guarden relación con los objetivos perseguidos con el tratamiento. Así, se trata de un principio que se encuentra íntimamente ligado con el de la finalidad, toda vez que el análisis de la proporcionalidad deberá hacerse necesariamente teniendo en consideración si el fin perseguido con el tratamiento de datos puede ser suplido por la realización de una actividad distinta a la del citado tratamiento, sin que la finalidad sea alterada o perjudicada.

De este modo al enfrentarse a la cuestión de si un determinado tratamiento de datos es proporcional, se hará necesario determinar si se puede estar en presencia de medidas excesivas, para lo cual deberá examinarse la proporcionalidad sobre la base de la adecuación, necesidad y ponderación de éste.

Así, lo que éste ordena es que la actividad de tratamiento de datos se reduzca al mínimo necesario para alcanzar los fines perseguidos, ya que ningún objetivo ulterior puede justificar un uso extensivo de los datos personales tratados pues ello es justamente lo que puede posibilitar la lesión de derechos y la pérdida de capacidad de los titulares de datos para controlar las informaciones que sobre ellas circulan.

(...) ningún objetivo ulterior puede justificar un uso extensivo de los datos personales (...)

e. Transparencia: Al ser la protección de datos personales un sistema preventivo que justamente lo que persigue es que la libre circulación de los datos se realice con el conocimiento del titular de los mismos, resulta indispensable que el tratamiento se ponga oportunamente en conocimiento del titular de manera que pueda ejercer los derechos que la ley le otorga al titular de éstos. Adicionalmente, que las bases de datos en que estén se encuentren fácilmente en conocimiento de los titulares de manera que en todo momento puedan revisar si sus datos se encuentran o no incorporados en un registro en particular.

f. Participación individual: Este principio representa uno de los elementos más relevantes en la tutela dinámica de los derechos que trae consigo la protección de datos personales, de manera que el titular de éstos pueda seguirlos sin importar el lugar en que se encuentren, y con ello velar activamente por el adecuado tratamiento de los mismos.

Es posible advertir que en virtud de este principio es que las normativas han de consagrar una serie de derechos a favor del titular de datos que le permita conocer quien está tratándolos, por qué motivo y al mismo tiempo ejercer los derechos que permitan que el tratamiento de los mismos satisfaga los principios señalados precedentemente, posibilitando que se adecúe cualquier información que no permita representar cabalmente la situación de una persona a través de sus datos.

g. Seguridad: El tratamiento de datos personales supone la realización de un conjunto de operaciones, manuales o automatizadas, las que para evitar perder el control de la información requieren implementar medidas tecnológicas y de procesos orientadas a asegurar los datos y detectar oportunamente cualquier acceso no autorizado a los mismos.

Así, será indispensable que el código establezca la obligación de considerar estas medidas, tanto en la fase de diseño como de implementación de los sistemas de protección de datos, para lo cual deberá contemplarse, por una parte, el riesgo asociado al tratamiento de la información en función de la naturaleza de los datos que se tratan y, por la otra, el estado de la técnica y el costo de su aplicación.

De este modo, el código deberá importar la implementación de los principios señalados con miras a asegurar:

1. Que los responsables del tratamiento de datos personales conozcan clara y precisamente cuál es la conducta deseada por parte de la profesión o sector industrial de que se trata.

2. Que sean conocidos los derechos que se le reconocen a los titulares de los datos.

3. Que se brinde asesoría y apoyo a los titulares de datos para que conozcan sus derechos y las formas en los cuales pueden hacerlos exigibles en el marco del código.

4. Que se imponga un régimen sancionatorio efectivo que permita disuadir y reprimir las infracciones al código.

Mecanismo de resolución alternativa de conflictos

Partiremos señalando que los mecanismos de resolución alternativa de conflictos son aquellos métodos de prevención y solución de conflictos originados a propósito de la relación entre los responsables del tratamiento de datos personales y los titulares de los mismos, cuya resolución es encargada a órganos imparciales diversos de los tribunales de justicia.

(...) desarrollar en los titulares de datos la capacidad de hacer valer sus derechos con rapidez, eficacia y sin que los costos asociados aparezcan como un desincentivo para accionar.

La finalidad de implementar un mecanismo de esta clase se orienta a desarrollar en los titulares de datos la capacidad de hacer valer sus derechos con rapidez, eficacia y sin que los costos asociados aparezcan como un desincentivo para accionar. De este modo, lo que finalmente se persigue es reducir

los costos transaccionales del reclamo y de esta forma permitir que los titulares de datos se sientan más tranquilos y seguros al poder identificar con facilidad a quiénes tratan sus datos y saber que cuentan con un medio de restablecimiento de sus derechos en caso de vulneración, el que junto con ser expedito no ha de significar costos significativos.

Es por lo anterior que el mecanismo deberá estructurarse sobre la base de los siguientes principios:

a. Equidad: Por su intermedio se debe permitir que el titular de los datos pueda conocer inmediatamente la existencia del mecanismo de solución de controversias; que haya un tercero independiente con suficiente conocimiento y destrezas como para poder cumplir sus deberes responsablemente; que la puesta en movimiento del sistema sea gratuita o de muy bajo costo, considerando el valor de la disputa; que las barreras geográficas sean eliminadas o reducidas al mínimo; que los plazos de resolución de los conflictos permitan arribar expeditamente a solución y que siempre se mantenga resguardado el derecho de los titulares de datos de accionar judicialmente.

(...) se debe permitir que el titular de los datos pueda conocer inmediatamente la existencia del mecanismo de solución de controversias (...)

b. Visibilidad: La disponibilidad del mecanismo debe ser evidente para el titular de datos, por lo cual la información que el responsable del tratamiento de los mismos brinde al momento de solicitar el consentimiento deberá incluir esta información.

c. Accesibilidad: Cualquier titular de datos debe poder poner en movimiento el procedimiento y, en consecuencia, no deben existir barreras que lo dificulten. Con relación a los costos, se ha dicho que idealmente debe ser gratuito o de muy bajo costo, sin embargo, es necesario tener claro que ese punto está referido a la posibilidad de accionar y no a los costos que significa el proceso mismo, como pueden ser los valores asociados a la producción de la prueba.

d. Duración: El titular de datos que recurra a este mecanismo debe poder obtener rápidamente un pronunciamiento.

e. Finalidad: El mecanismo debe diseñarse e implementarse considerando que su objeto es resolver las disputas que se produzcan.

f. Cumplimiento: Atendiendo a que lo que se persigue con esta clase de mecanismos es que sean capaces de resolver las disputas que se produzcan, es que resulta indispensable definir los medios de solución como equivalentes jurisdiccionales.

Atribución de efectos públicos a la autorregulación

En este punto hacemos alusión a la necesidad de que el Estado sea el que reconozca y le otorgue consecuencias jurídicas a los códigos deontológicos y mecanismos alternativos de solución de controversias que cumplan con las condiciones que la propia ley o reglamentación le imponga a estos sistemas.

Al respecto, lo primero que parece necesario dilucidar es qué significa atribuir efectos públicos a la autorregulación y la respuesta, no obstante parecer bastante clara y directa, posee consecuencias jurídicas que son significativas. Así, estos efectos suponen una gradación donde es posible distinguir entre: efectos habilitantes, efectos probatorios, efectos vinculantes y efectos de cosa juzgada.

(...) lo primero que parece necesario dilucidar es qué significa atribuir efectos públicos a la autorregulación (...)

Finalmente, será necesario determinar la forma en que la autorregulación debe producirse para poder ser objeto de reconocimiento público, de manera que con ella se salvaguarden adecuadamente los fines públicos que se desea proteger con esta tenue, pero efectiva, forma de intervención del Estado.

IV. Recomendaciones finales

1. Desarrollar acciones de fomento para que los diferentes sectores industriales y profesionales elaboren sistemas de autorregulación que salvaguarden los derechos de las personas cuando se tratan sus datos personales.

2. Elaborar guías sectoriales de buenas prácticas que contribuyan al desarrollo de los códigos deontológicos y de los mecanismos alternativos de solución de controversias.

3. Reconocer legalmente que los sistemas de autorregulación que cumplan con ciertas características son capaces de producir efectos públicos.

4. Establecer un mecanismo de supervigilancia y fiscalización del cumplimiento de los sistemas de autorregulación.

5. Sancionar severamente el incumplimiento de los sistemas de autorregulación.

Autor

Raúl Arrieta Cortés

Abogado, Universidad Central de Chile, Magíster (c) en Derecho Público de la Universidad de Chile. Consejero del Instituto Chileno de Derecho y Tecnologías.

III
Protección de datos personales en la sociedad de redes

Paloma Baytelman

I. Introducción

La era de la información y el conocimiento trae consigo profundas transformaciones. Se trata de uno de los cambios socioculturales más importantes que ha experimentado la humanidad desde la invención de la imprenta. Hoy la tecnología afecta la vida diaria en muchos sentidos, desde el cómo trabajamos, aprendemos, consumimos y nos relacionamos con marcas, instituciones, gobiernos, e incluso con nuestros pares. Gracias a ella, la participación, colaboración y creación de contenidos se vuelven prácticas cada vez más comunes, hasta cotidianas, generando nuevos contextos y formatos de construcción social.

Como bien señala Douglas Rushkoff en su libro "Renacimiento 2.0", Internet no es un fenómeno tecnológico, ni siquiera mediático, es un fenómeno social. Si esto aún resulta difícil de entender para algunos es porque todavía se cree que la tecnología y los medios de comunicación son herramientas que sirven para controlar a las personas, cuando en realidad lo que hacen es entregarles más poder, parte del cual está dado por la capacidad de construir, reconfigurar y compartir contenidos o datos, a través de los que también se construye, reconfigura y comparte nuestra identidad. De este modo, la gran cantidad de información disponible a través de medios y plataformas digitales, sumada a los crecientes cambios culturales producto de los avances tecnológicos, generan escenarios más complejos, al mismo tiempo que trastocan paradigmas.

Internet no es un fenómeno tecnológico, ni siquiera mediático, es un fenómeno social. Si esto aún resulta difícil de entender para algunos es porque todavía se cree que la tecnología y los medios de comunicación son herramientas que sirven para controlar a las personas.

Uno de los cambios más profundos que se plantean a partir de estas nuevas dinámicas, sin duda, dice relación con la privacidad de las personas. Esto no es un tema que esté en discusión, ni algo a lo cual podamos oponernos: los cambios en torno a lo privado y los datos personales son una realidad. "La era de la privacidad ha terminado", así lo expresó en enero de 2010 Mark Zuckerberg al referirse a la controversia generada por los cambios en las normas de privacidad de Facebook, la red social que él mismo fundó en 2006 y que hoy cuenta con más de 500 millones de personas registradas en todo el mundo.

Más que estar de acuerdo con la idea de que se trate del fin de la privacidad, parece interesante ver el tema desde otros dos puntos de vista, esto es, como *cambio* y como *desafío*. El primer enfoque —el *cambio*— dice relación con un acelerado proceso de transformación en los paradigmas que hasta ahora han establecido los límites entre lo público y lo privado. El *desafío*, en tanto, apunta al reto que significa educar a las personas y a las sociedades sobre la responsabilidad que les concierne en relación a la protección de los datos, en contextos donde la posibilidad de control está lejos de ser absoluta.

Más que estar de acuerdo con la idea de que se trate del fin de la privacidad, parece interesante ver el tema desde otros dos puntos de vista, esto es, como cambio y como desafío.

Tanto el *cambio* como el *desafío* traen consigo múltiples interrogantes sobre la responsabilidad de los individuos, los gobiernos, las instituciones, las empresas, las plataformas de redes sociales y muchos otros y variados estamentos sociales y tecnológicos.

Si bien estos fenómenos suelen ser sorprendentes y abrumadores para quienes hemos sido testigos de la aparición y evolución de nuevos instrumentos tecnológicos, son hechos absolutamente naturales para los que han nacido en el transcurso de esta historia: los llamados nativos digitales. De hecho, los cuestionamientos más complejos respecto de la construcción de la identidad, la privacidad, la protección de los datos personales y la libre circulación de la información aparecen cuando se analiza la situación de los niños y adolescentes, cuyos comportamientos, oportunidades y riesgos son temas que recién se están comenzando a analizar en algunos ámbitos académicos y se encuentran todavía muy lejos de movilizar la creación de políticas públicas o marcos regulatorios que se condigan con los actuales contextos, los cuales están caracterizados por escenarios en permanente cambio.

II. De inmigrantes y nativos

Cada vez con más fuerza la información se transforma en una moneda de cambio. Cómo accedemos a ella, la manejamos, la filtramos o compartimos, son parámetros que dan cuenta de nuestras destrezas para comprender el mundo actual y gestionar nuestra existencia dentro de él.

En esta era del conocimiento las fronteras están marcadas no sólo por cuánto sabemos o cómo aprendemos, sino también por cuán naturales nos resultan los nuevos entornos.

En esta era del conocimiento las fronteras están marcadas no sólo por cuánto sabemos o cómo aprendemos, sino también por cuán naturales nos resultan los nuevos entornos.

Mientras los nativos digitales han crecido con controles remotos, videojuegos, computadores, teléfonos celulares, Internet y la interactividad como elementos naturales de su medio, los demás nos desplazamos a tientas, incluso a ciegas, como inmigrantes en las tierras de la participación. Por mucho que adoptemos la tecnología, usemos las plataformas y entendamos de nuevos lenguajes, el acento del Viejo Mundo de una u otra forma se hace presente.

Son muchos los inmigrantes digitales que, educados en los viejos modelos, son más cautos respecto de lo que comparten, de su reputación y de su vida privada. Tienen más miedo del "qué dirán" y más conciencia sobre las consecuencias de sus actos. Los nativos, en cambio, poseen otros entendimientos de "lo privado" y parecerían dar menor importancia a las consecuencias de su comportamiento en la red.

Según la investigadora estadounidense Danah Boyd los nativos digitales sienten que ni siquiera sus propias habitaciones les pertenecen y, por lo tanto, no las perciben como espacios de privacidad. Éstas vendrían a ser para ellos sólo una parte más de las casas de sus padres, donde el resto de la familia circula a su antojo. En cambio, paradójicamente respecto a Internet sienten que les otorga un lugar más privado a la hora de construir su mundo e identidad, o sus mundos e identidades, pues la diversidad de elección en los espacios de pertenencia es para ellos un valor.

De esta forma se sienten protegidos en los contextos virtuales, por lo que comparten sus vidas allí, algunas veces sin pensar demasiado sobre el hecho de que sus datos, reflexiones, información y contenidos quedan en las redes y podrían ser conocidos casi por cualquier persona, tanto ahora como en muchos años más.

Sin embargo, al parecer esto comienza a cambiar, pues pese a que sienten la necesidad de compartir sus sentimientos y experiencias en las redes, los jóvenes cada vez más con mayor frecuencia utilizan mensajes en clave para contarles a sus amigos sus vivencias.

Más allá de las diferencias generacionales y los resquemores, con más o menos precaución, en la actualidad tanto nativos como inmigrantes comparten grandes volúmenes de información personal en plataformas de redes sociales, ya sea para comunicarse, entretenerse o, simplemente, para compartir contenidos. También, con más o menos precaución, se protege la privacidad. No obstante, lo que muchas veces se pasa por alto es que la información es una moneda de cambio, es decir, que las herramientas tecnológicas que parecieran ser gratuitas son al fin y al cabo un negocio que debe sustentarse, cuyo bien transable, precisamente, son los datos y contenidos que las personas generan e intercambian.

(...) lo que muchas veces se pasa por alto es que la información es una moneda de cambio, es decir, que las herramientas tecnológicas que parecieran ser gratuitas son al fin y al cabo un negocio que debe sustentarse cuyo bien transable, precisamente, son los datos y contenidos (...)

En este contexto surgen múltiples cuestionamientos. ¿Hasta dónde estamos dispuestos a entregar nuestra información a cambio de tener los espacios para compartirla? ¿Los niños y adolescentes cuentan con el discernimiento suficiente sobre los límites y alcances de los datos que comparten y los filtros sobre la información referente a su identidad? Éstas son sólo algunas de las interrogantes sobre las cuales urge reflexionar y actuar.

III. Internet como tatuaje

De acuerdo a la legislación la información que ingresemos en Internet será considerada "dato personal" en la medida que a partir de ella seamos identificados o "identificables". Entonces ¿son datos personales aquellos datos falsos que son ingresados para la identificación de una persona en una red social? ¿Qué es lo que sucede con nuestros datos personales una vez que los ponemos en la red? Estas preguntas generan una creciente preocupación, en especial entre los inmigrantes digitales, quienes miran con desconfianza cómo los jóvenes comparten una cantidad abrumadora de información a través de las plataformas colaborativas.

Desde nuestra perspectiva, incluso los datos falsos deben ser considerados datos personales, por cuanto el concepto legal no se limita a aquellos datos de fácil vinculación a una persona, sino que también comprende a aquellos que requieren de operaciones más complejas para identificar la persona a la cual se refieren.

Respecto de la segunda pregunta, del análisis de las redes sociales y su forma de funcionamiento, queda claro que cuando realizamos intercambios de datos personales a través de dichas plataformas sociales —ya sean textos, fotos, videos o datos de identificación— debemos estar preparados para que tarde o temprano esta información sea pública. Por mucho que hayamos ajustado los filtros de privacidad, basta que uno solo de nuestros amigos o contactos tome alguno de esos elementos para que su difusión salga de nuestra esfera de control. En este contexto, podríamos sostener que la red social no se puede comprometer a una protección irrestricta de la privacidad de la persona. Lo que sí creemos que contraviene los principios de protección de datos personales es que los administradores de una determinada plataforma de redes sociales comuniquen los datos personales a terceros gratuita u onerosamente.

Volviendo al hecho de que debemos estar conscientes de que la información compartida en plataformas sociales puede tornarse pública en cualquier momento, es posible hacer un paralelo con la práctica de tatuarse el cuerpo.

Tal y como sucede con los tatuajes, si a los 30 años una persona se arrepiente del dibujo que se hizo en la piel a los 20, puede intentar que se lo borren con tecnología láser, pero la marca siempre quedará. Con la información que ponemos en Internet ocurre algo similar; sin embargo, el asunto es aún más complejo. Interactuar a través de las redes pareciera ser algo mucho más natural y menos doloroso que tatuarse el cuerpo, no obstante, es bastante más duradero y visible.

Interactuar a través de las redes pareciera ser algo mucho más natural y menos doloroso que tatuarse el cuerpo, no obstante, es bastante más duradero y visible.

En el caso de los nativos digitales estos nuevos tatuajes plantean situaciones más complejas, precisamente por sus prácticas de comportamiento digital y por su entendimiento sobre lo público y lo privado. Así, una imagen o un video que en un principio puede resultarles divertido, años después, en un entorno laboral o familiar diferente, corre el riesgo de transformarse en un material comprometedor.

Tengamos o no conciencia de ello, los elementos que configuran la identidad que las personas van construyendo de sí mismas en la red exponen a los individuos tanto a recibir mensajes indeseados como a correr diversos tipos de peligros, que van desde ver afectada su reputación, la suplantación de identi-

El desafío está en reflexionar y articular modelos de enseñanza que permitan a las personas relacionarse en las nuevas plataformas, al mismo tiempo que cuidan su integridad.

dad, hasta sufrir situaciones de acoso. Asimismo, es importante considerar que un individuo puede verse afectado por decisiones arbitrarias, tomadas a partir del análisis de la información que le concierne y que la misma persona y/o terceros han publicado en estas redes.

En todo caso, frente a esta realidad no se saca nada con negar, criticar y oponerse a las herramientas digitales, pues como ya hemos dicho estamos frente a un fenómeno social ya instalado que trasciende por mucho a lo meramente tecnológico.

El desafío está en reflexionar y articular modelos de enseñanza que permitan a las personas relacionarse en las nuevas plataformas, al mismo tiempo que cuidan su integridad.

IV. Identidad virtual

Según un estudio realizado en 2010 por la compañía de investigación de marketing en Internet Comscore, en América Latina el 81% de las personas que usan Internet tiene cuenta en redes sociales. Se estima que ese porcentaje se concentra principalmente en perfiles de Facebook, plataforma que en Chile registra más de 7 millones de cuentas creadas. Dado el vasto uso que ha alcanzado y tomando en cuenta que en teoría no permite el anonimato, esta herramienta plantea uno de los mejores escenarios para reflexionar sobre las formas en que las personas están configurando su identidad en el mundo digital.

El capital de Facebook se centra en las relaciones interpersonales, fuertemente ancladas en el mundo real, según explican los investigadores Ignacio Uman, Carolina Venesio y Nataly Medina, de la Universidad de Buenos Aires (UBA), quienes junto al profesor Alejandro Piscitelli han venido estudiando los alcances sociales de esta plataforma de redes sociales y su repercusión en la construcción de identidad virtual.

"Facebook integra la vida *offline* con la vida *online*, el perfil público con la identidad real. Toma huellas de lo real que hace presentes en lo virtual y viceversa, disolviendo aquellos entornos que permitían jugar con la identidad y la posibilidad de reinventarse, que parecían característicos de mediados de

los 90. Sin embargo, lo virtual y lo real no son mundos opuestos sino capas de una misma realidad. Ya no es posible oponerlos, los entornos virtuales forman parte de nuestra vida real. Ante este escenario, pareciera ser que Facebook está haciendo mucho hincapié en la identidad real (más que en la virtual) de las personas, al contrario de lo que sucedía con el auge del chat, los foros y juegos de rol, donde cada persona inventaba su avatar", señalan.

Así, nos encontramos con entornos no anónimos, donde la identidad parece implicar una aceptación de los otros, dejando poco espacio para la transgresión y lo oculto.

V. Anonimato y olvido

Internet acumula hoy cantidades de información inimaginables, cifra que crece de forma exponencial cada día, siendo alimentada por millones de personas para quienes la web y en especial las plataformas de redes sociales se han convertido en herramientas de comunicación casi imprescindibles.

Pese a ello, mucha gente no quiere que las cosas que dice en la web sean relacionadas con su verdadera identidad o desean borrar cualquier registro de su paso por dichas plataformas. Esto puede deberse al temor por posibles represalias políticas, laborales o económicas, miedo al acoso o incluso a situaciones que amenazan sus vidas.

(...) mucha gente no quiere que las cosas que dice en la web sean relacionadas con su verdadera identidad o desean borrar cualquier registro de su paso por dichas plataformas.

Personas que denuncian verdades incómodas para gobiernos o empresas, activistas de los derechos humanos en su lucha contra regímenes represivos, padres que tratan de crear una forma segura para que sus niños puedan explorar contenidos de la web, víctimas de violencia intrafamiliar que quieren reconstruir sus vidas sin que sus abusadores las puedan rastrear. Todos ellos prefieren usar seudónimos para comunicarse.

Según indica la Electronic Frontier Foundation, tanto para estas personas como para las organizaciones que las apoyan, el anonimato es un asunto crítico de seguridad pues, literalmente, les puede salvar la vida.

De este modo, el anonimato se yergue como parte importante del derecho a la libertad de expresión, pues permite a los disidentes proteger sus identidades mientras expresan sus puntos de vista.

Dado que Internet ofrece un importante espacio en la lucha por la democracia y la injusticia social, el derecho al anonimato es central en el mundo de las redes.

Cabe recordar entonces que si bien existen algunas plataformas de redes sociales que permiten mantener una identidad oculta, otras de vasto alcance como Facebook solicitan a las personas entregar información acabada sobre su nombre, sexo y ubicación geográfica. Sin embargo, qué sucede si más allá de ser anónimos lo que queremos es desaparecer de la web y borrar voluntariamente el rastro que hemos dejado durante el tiempo que hemos utilizado Internet o, específicamente, las redes sociales.

Si bien existe una normativa orientada a proteger la reputación de los individuos y, en teoría, uno podría pedir la eliminación de toda la información relacionada con su persona que no sea de gravitante interés público, en la práctica el derecho al olvido se torna algo prácticamente imposible en Internet: el derecho al olvido es inviable en un contexto de redes interconectadas casi hasta el infinito. Es por ello que surge la imperiosa necesidad de ser extremadamente cuidadosos con las informaciones, los datos y las imágenes que se suministran, con el fin de proteger al máximo la privacidad de dicha información y de evitar su uso con fines para los que no ha sido autorizada.

(...) en la práctica el derecho al olvido se torna algo prácticamente imposible en Internet: el derecho al olvido es inviable en un contexto de redes interconectadas casi hasta el infinito.

VI. El fin del secreto

Las nuevas tecnologías de la información y la comunicación permiten e impulsan prácticas positivas y escenarios de mayor participación y transparencia. Sin embargo, para muchas personas que no tienen pleno conocimiento de las implicancias que revierte el hecho de compartir sus datos se abren entornos complejos y, potencialmente, peligrosos.

Conscientes de lo anterior, satanizar a las plataformas no es el mejor camino para evitar dichas amenazas.

Si bien las redes sociales son entornos especialmente creados para compartir información, es importante recordar que las prácticas de entrega e intercambio de datos personales no se remiten únicamente a los ámbitos

digitales. Decidir con quiénes y dónde compartimos nuestros datos son parámetros sobre los cuales tenemos que tomar decisiones no sólo en la red, sino también a diario en nuestra vida *offline*.

Debemos entender que el mundo cambió y recordar que no estamos hablando de tecnología, sino de lo que la gente hace con ella. Hoy prácticamente cualquier persona puede tomar una foto o un video y subirlo a Internet. No es realista entonces pretender que un gobierno o los administradores de las redes sociales puedan controlar de forma absoluta qué información propia o de otras personas comparte una persona en la red.

Asimismo, como hemos señalado anteriormente, es necesario saber que todo lo que pongamos en la web podría ser potencialmente encontrado e indexado por los buscadores. Nadie está libre de esto, ni siquiera los gobiernos o las grandes corporaciones. Basta con detenerse a mirar el caso de WikiLeaks, organización que desde 2006 ha publicado en su sitio web informes y documentos filtrados con contenido sensible en materia de interés público, principalmente relacionados con denunciar comportamientos no éticos por parte de gobiernos y empresas de todo el mundo.

(...) es necesario saber que todo lo que pongamos en la web podría ser potencialmente encontrado e indexado por los buscadores.

Si bien nuestros correos electrónicos u otros datos que compartimos en la web seguramente están lejos de tener la importancia global que han mostrado algunas de las filtraciones de WikiLeaks, estos hechos ponen de manifiesto lo fácil que resulta descifrar hasta las publicaciones más confidenciales, y lo debatible que pueden llegar a ser los límites del derecho a la información y a la intimidad.

Es por esto que resulta tan importante que las personas se detengan a pensar en el tipo de datos que están entregando o compartiendo y las consecuencias futuras que podría tener el hecho de hacer disponible este material. Esto dice relación con el principio de control de los datos personales, pues si la información que un individuo comparte en estas redes se hace pública, cualquier persona podría utilizarla sin su consentimiento.

Si bien el gobierno y la institucionalidad jurídica juegan un importante papel en la protección de la privacidad de las personas, no forma parte del rol de las instituciones velar por el tipo de información que cada individuo decide compartir por voluntad propia en la red, por cuanto esto queda entregado a

la autonomía de la voluntad de la persona que ingresa datos en plataformas digitales. Por ello es fundamental ser capaz de monitorear por uno mismo qué es lo que se hace en la web, qué datos se comparten con agentes públicos, privados e, incluso, con nuestros círculos más cercanos.

(...) es fundamental ser capaz de monitorear por uno mismo qué es lo que se hace en la web, qué datos se comparten con agentes públicos, privados e, incluso, con nuestros círculos más cercanos.

Todo esto sucede porque lo que hacemos en Internet no es un fenómeno aislado, es una práctica social que se articula en lo colectivo. Si bien existen riesgos, cambios, cuestionamientos y desafíos, también, como nunca antes en la historia de la humanidad, aparecen oportunidades de generar valor a través de la libre circulación de los datos y de la construcción conjunta de conocimiento. Lo importante es que nos eduquemos para ello.

Referencias

- Agencia Española de Protección de Datos; Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. León (España), 2009.
- Boyd, Danah. *Taken Out of Context: American Teen Sociality in Networked Publics*. Universidad de Berkeley, California (Estados Unidos), 2008.
- ComScore. *Estado de Internet en Latinoamérica*. www.comscore.com, 2010.
- Electronic Frontier Foundation. Anonymithy. https://www.eff.org/issues/anonymity.
- Piscitelli, Alejandro. *Nativos Digitales. Dieta cognitiva, inteligencia colectiva y arquitecturas de la participación*. Santillana. Buenos Aires (Argentina), 2009.
- Rushkoff, Douglas. *Renacimiento 2.0. Empresa e Innovación en la Nueva Economía*. Urano, Barcelona (España), 2007.
- Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. Penguin Books, Londres (Inglaterra), 2008.
- Tapscott, Don. *Era Digital. Cómo la generación Net está cambiando el mundo*. McGraw-Hill Interamericana, Ciudad de México (México), 2009.

Autora

Paloma Baytelman

Periodista de la Universidad Diego Portales, creadora de uno de los primeros Blogs de Chile. Especializada en comunicación digital, ha participado en decenas de seminarios y dado múltiples charlas sobre comunicación digital, tanto en Chile como en el extranjero. Actualmente, es encargada de Web y Nuevos Medios de Corfo.

IV
Protección de datos y servicios globales: ¿Regulación o incentivo?

Francisco J. Cruz Fuenzalida

I. Introducción

Los servicios globales, también conocidos como *offshoring*, significan un modelo de negocios por el cual una empresa decide trasladar una de sus funciones o procesos internos hacia el exterior, ya sea mediante su traspaso a una subsidiaria en otro país o bien a través de la subcontratación de un tercero que ejecutará dicho proceso o función en una locación geográfica distinta. Este modelo de negocios permite reducir costos, liberar flujos e incrementar la eficiencia operativa, privilegiando enfoques basados en la innovación empresarial, al aprovechar ventajas laborales, tributarias y tecnológicas de plazas diversas.

Este modelo de negocios permite reducir costos, liberar flujos e incrementar la eficiencia operativa, privilegiando enfoques basados en la innovación empresarial, al aprovechar ventajas laborales, tributarias y tecnológicas de plazas diversas.

Los procesos más comunes que pueden identificarse en la industria del *offshoring* se vinculan a las tecnologías de la información (ITO), los procesos empresariales (BPO) y los procesos de conocimiento (KPO).(1) Los primeros cubren funciones asociadas a tecnologías en infraestructura o aplicación, como puede ser el soporte técnico de negocios, desarrollo de software, captura y procesamiento de bases de datos y mantención de redes. Los BPO se identifican con procesos administrativos (*back office*), procesamiento de *telemarketing*, *callcenters* y, en general, administración de recursos humanos y compras corporativas. A su vez, los KPO se vinculan con flujos de alto valor agregado en investigación, ingeniería, biotecnología y, frecuentemente, con sectores profesionales específicos como medicina o derecho.

La operación del negocio descansa, mayoritariamente, sobre centros de producción y despacho de conocimiento o procesos (*delivery centers*), preferentemente ubicados en Europa y Asia, siendo deslocalizados desde la matriz al país extranjero en donde se ejecuta la función.

En la actualidad la tasa de crecimiento de esta industria bordea el 15% anual y moviliza más de US$ 192.000 millones. En el caso de Chile existe un grupo aproximado de 60 firmas extranjeras cuyos flujos de exportación representan cerca de US$ 1.000, generando 20.000 plazas de empleo.(2)

(1) ITO: Information Technology Outsourcing. BPO: Business Process Outsourcing. KPO: Knowledge Process Outsourcing.

(2) Cifras de la Corporación de Fomento de la Producción (CORFO) dadas a conocer por El Mercurio, Economía y Negocios; Crónica del 27 de septiembre de 2010.

A nivel mundial los márgenes de crecimiento del *offshoring* están en plena expansión, considerando el progresivo proceso de globalización económica, la creciente aplicación de tecnologías de la información en la industria y el surgimiento de nuevos modelos de negocios.

India e Irlanda son algunos de los principales proveedores que deslocalizan operaciones en América Latina, aprovechando ventajas de huso horario, proximidad geográfica y bajos costos de operación para prestar servicios hacia Estados Unidos, uno de los consumidores más importantes del sector.

Es en este escenario que las economías emergentes, dotadas de buen ambiente institucional, tienen una oportunidad privilegiada para capturar esta industria, la que desafía a competir en costos y también en el desarrollo de segmentos que generen un valor agregado en aspectos como: Capital Humano, Investigación y Desarrollo (I+D), Nuevas Tecnologías y Protección de Datos. Cabe destacar que esta última es clave para todos los segmentos en los que se desarrolla el *offshoring*, ya que mientras en ITO y BPO la protección de la información permite que los procesos se desenvuelvan dentro de marcos jurídicos y estándares de seguridad que habiliten un tratamiento de datos responsable, en KPO la información personal constituye la *"materia prima"* para el desarrollo del rubro, muy especialmente cuando se trata de servicios que transitan varios destinos (como lugar de origen, plaza de procesamiento y locación final en donde se entrega el servicio).

(...) en lo que respecta a los procesos de conocimiento, los servicios globales demandan marcos regulatorios sofisticados y definidos, que brinden protección al "corazón" del negocio y que se sumen al incentivo permanente que mueve la industria (...)

En síntesis, en lo que respecta a los procesos de conocimiento, los servicios globales demandan marcos regulatorios sofisticados y definidos, que brinden protección al "*corazón*" del negocio y que se sumen al incentivo permanente que mueve la industria, el de relocalizarse en lugares con costos de operación bajos y altas oportunidades de proyección.

II. Tutela de la protección de datos a propósito de los servicios globales

La justificación de la protección jurídica en la industria de los servicios globales surge de la ineficiente regulación que existe en materia de transferencias internacionales y de la necesidad de armonizar marcos normativos regidos

por estándares desiguales. Lo anterior genera una insuficiencia o asimetría que puede encontrarse en el origen del dato, el lugar de su tratamiento o el destino final del mismo.(3)

La literatura comparada identifica dos sistemas principales para entender el soporte de estándares que deben tener las legislaciones que interactúan en las transferencias de información. Estos sistemas son conocidos como Nivel Adecuado de Protección y Puerto Seguro.

La literatura comparada identifica dos sistemas principales para entender el soporte de estándares que deben tener las legislaciones que interactúan en las transferencias de información. Estos sistemas son conocidos como Nivel Adecuado de Protección y Puerto Seguro.

El Nivel Adecuado de Protección, vigente en la Unión Europea (UE), descansa sobre un complejo conjunto de normas y principios que definen y orientan la decisión de la autoridad(4) llamada a evaluar si el país receptor de la transferencia califica con un escenario institucional que dé garantías a los datos que serán objeto de flujo. Este complejo sistema de normas está compuesto, preeminentemente, por el Convenio 108 del Consejo de Europa; la Directiva 95/46 de la CE;(5) el Grupo de Trabajo del Artículo 29 de dicho instrumento (GT29)(6) y las directrices de la OCDE(7) en la

(3) Cuando se transfieran datos de una agencia (exportador de los datos) a la entidad matriz de un grupo (importador de los datos), ubicada en un tercer país, con la finalidad de centralizar una gestión, se entenderá que el importador de los datos es responsable de su posterior tratamiento, es decir, decidirá sobre la finalidad, contenido y uso del tratamiento de la información. A su vez, cuando una entidad (exportador de los datos) transfiere información a otra entidad (importador de los datos), ubicada en un tercer país, cuya finalidad es la prestación de un servicio, el importador de los datos será el encargado del tratamiento que recibirán los datos para su posterior uso en nombre del exportador de los datos, de conformidad con sus instrucciones.

(4) Respecto de la agencia llamada a efectuar esta evaluación, la UE exhibe fórmulas con arreglos diversos. De esta forma en países como Reino Unido la primera evaluación es efectuada por el propio responsable de exportar los datos, mientras que en España y los Países Bajos dicha decisión radica directamente en la autoridad de control, que podría ser el propio órgano regulador (caso español) o bien en el órgano del Ejecutivo vinculado al rubro, como el Ministerio de Justicia en el caso de los Países Bajos.

(5) El considerando quinto de dicha directiva, atingente en esta materia, señala: "La integración económica y social resultante del establecimiento y funcionamiento del mercado interior (…), va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados Miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior".

(6) Vid http://ec.europa.eu/justice/policies/privacy/index_en.htm

(7) Vid OECD's "Guidelines governing the Protection of Privacy and Transborder Data Flow of Personal Data" en www.oecd.org

materia, que en su conjunto permiten inferir un núcleo de principios con contenido,[8] que fija las pautas de cumplimiento mínimo para el Nivel Adecuado.[9]

Por cierto, bajo determinados contextos en los que se consideren elementos como las empresas involucradas en la transferencia, el volumen y nivel de seguridad de los datos sujetos a la operación, y otras circunstancias que incidan en la evaluación de riesgos, esta línea de partida podría ampliarse o bien tener ciertas indulgencias restrictivas para su aplicación. En definitiva, deben evaluarse todas las circunstancias que concurran en una transferencia.

(...) el sistema de Puerto Seguro es aún más complejo ya que significa una serie de regulaciones parciales, estructuradas sobre normas específicas y conductas sectoriales, con un fuerte énfasis en la autoregulación (...)

Por su parte, el sistema de Puerto Seguro es aún más complejo ya que significa una serie de regulaciones parciales, estructuradas sobre normas específicas y conductas sectoriales, con un fuerte énfasis en la autoregulación, pero sin un contenido de estándares básicos de aplicación general. Este es el sistema vigente en Estados Unidos y que para algunos genera vacíos y riesgos al depender excesivamente del autocumplimiento.

(8) En este contexto es posible destacar como principios de contenido centrales los siguientes:
- Principio de Finalidad: Los datos deben tratarse con un objetivo específico, debiendo haber armonía entre dicho objetivo y el que motiva la transferencia.
- Principio de Proporcionalidad y Calidad: Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren.
- Principio de Transparencia: Debe informarse en todo momento a los titulares acerca del objetivo del tratamiento y la identidad del responsable en el tercer país.
- Principio de Seguridad: El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento.
- Principio de Acceso, Rectificación y Oposición: El titular o interesado debe tener derecho a obtener una copia de todos los datos relativos a su persona, rectificar datos inexactos y a oponerse a su tratamiento.
- Principio de restricción respecto a transferencias sucesivas a terceros países: Las transferencias sucesivas de datos personales del tercer país de destino a otro tercer país deben considerar, en el caso de este último, un nivel de protección adecuado.

(9) Existen otros marcos atendibles que no detallamos en el eje central de este trabajo, pero que es importante considerar si se desea profundizar en el tema, como es el caso Foro de Cooperación Económica Asia Pacífico (APEC) con su Marco de Privacidad (2004) que vigoriza la protección de la privacidad y los flujos de información, y con el Privacy Pathfinder (2007) que impulsa la aprobación de normativas que establezcan responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reduce costes de cumplimiento con la normativa y facilita a los consumidores instrumentos efectivos de protección de sus derechos, fortaleciendo la acción de reguladores y minimizando cargas administrativas. Para acometer estos fines el Privacy Pathfinder desarrolla un sistema que permite al sector privado crear sus propias reglas transfronterizas para la protección de la privacidad y los datos personales, apoyándose en el uso de sellos de confianza para el consumidor y de una plataforma tecnológica multilingüe que facilita la interacción de los consumidores de cualquier economía de la APEC con las distintas instancias nacionales que se encuentren a cargo de la instrumentación de mecanismos alternativos de resolución de conflictos.

En este contexto, puede considerarse que la complejidad de dicho sistema radica en que produce soluciones aisladas y con un enfoque casuístico, las que, sin embargo, podrían generar los incentivos correctos respecto de ir avanzando en crear respuestas universales a partir de los casos específicos que se vayan resolviendo. Esto no sólo permitiría acrecentar buenas prácticas sectoriales, sino que además entregaría soluciones regulatorias flexibles y dinámicas.

(...) la complejidad de dicho sistema radica en que produce soluciones aisladas y con un enfoque casuístico, las que, sin embargo, podrían generar los incentivos correctos respecto de ir avanzando en crear respuestas universales a partir de los casos específicos que se vayan resolviendo.

En síntesis, existen aproximaciones diversas a un mismo tema, en donde el Puerto Seguro presenta más las cualidades de un buen sistema registral y certificatorio que de control y normativo.

III. Protección de datos y servicios globales

Tras haber realizado una descripción general de los servicios globales, habiendo justificado la necesidad de su tutela jurídica y evidenciado cómo en ella se identifica la protección de datos, volvemos a nuestra interrogante original, la que refiere a si la protección de datos constituye una regulación indispensable para el desarrollo de la industria de los servicios globales o es más bien un incentivo para la misma; si es una carga necesaria o si constituye una oportunidad aprovechable, en otras palabras, ¿las normas de protección requeridas son para justificar el negocio o para potenciarlo?

Para responder a lo anterior no son precisas explicaciones muy elaboradas, pues basta apreciar la experiencia internacional que permite entender la protección de datos como un activo corporativo y no sólo como una carga regulatoria.

A continuación se desarrollan algunas razones que permiten justificar esta posición:

1. **Al ser una industria altamente expuesta al flujo transfronterizo de datos, la protección de éstos se convierte en un "ancla de certezas" para los servicios globales, que permite fijar reglas claras y estándares, añadiendo predictibilidad a las decisiones en los negocios.**

En efecto, las empresas que operan en la industria de servicios globales, particularmente las que hemos denominado como BPO, transfieren grandes volúmenes de información, deslocalizando centros de operación de dimensiones acotadas hacia plazas de negocios que exhiban garantías institucionales para el tratamiento de datos. En síntesis, buscan países en donde los costos de instalación y operación sean bajos, pero que posean un sólido marco legal que les garantice el "*corazón del negocio*", es decir, el tratamiento de la información y el procesamiento de los datos.

2. Las medidas tendientes al resguardo de los datos ayudan a uniformar las políticas de *Privacy by Design*[(10)] (PbD), denominación que apunta a la protección de la información desde el origen de las operaciones y no sólo cuando éstas puedan constituir un riesgo, promoviendo también la autorregulación.

Las empresas internacionales consolidadas están dotadas en su gran mayoría de políticas internas que protegen sus flujos corporativos entre las filiales y entre éstas y su matriz. En la literatura especializada esto es conocido como *Privacy by Design,* adelantando mapas de riesgo y levantando procesos que den confianza a los consumidores, socios, accionistas y, en general, a los titulares de datos.[(11)]

Las empresas internacionales consolidadas están dotadas en su gran mayoría de políticas internas que protegen sus flujos corporativos entre las filiales y entre éstas y su matriz.

Un segundo elemento destacable es que fomentan el surgimiento de códigos tipo o normas de autorregulación, como ocurre en el caso de las denominadas BCR (*Binding Corporate Rules*).[(12)] Las BCR´s son reglas de conducta vinculantes, que fijan estándares para transferencias inter-

(10) "El término *"Privacy by Design"* (PbD) refiere en general a la incorporación de la privacidad y la protección de datos dentro del ciclo de vida del sistema de tecnología de la información, desde sus inicios hasta el cese de su actividad". (AEPD y Fundación CEDDET; "El Derecho a la Protección de Datos"; Módulo 3º: Seguridad, Confidencialidad, Transferencias Internacionales y Autorregulación, Primera Edición; página 69.

(11) "PbD puede suponer diferentes acciones, dependiendo del caso concreto donde se implante, ya sea eliminando o reduciendo datos de carácter personal, previniendo o eliminando tratamientos no deseados. También puede suponer el empleo de herramientas que mejoren el control del interesado sobre sus datos personales. Además pueden ser incorporadas dentro de la arquitectura de los sistemas de información y las comunicaciones y/o en la estructura de las organizaciones que traten datos de carácter personal". Ibídem página 67.

(12) Reglas Corporativas Vinculantes.

nacionales dentro de grupos multinacionales de empresas y que gozan de mayor flexibilidad para la exportación e importación de datos. Cabe entonces preguntarse cuál debiera ser el incentivo que tienen las grandes multinacionales para contar con escenarios que contemplen un nivel adecuado de protección, si ellas mismas ya han internalizado el costo de este estándar.

(...) mientras más sofisticadas y precisas sean las regulaciones para el tratamiento de datos mayores externalidades positivas reportará ese contexto al negocio (...)

La respuesta tiene al menos dos expresiones elocuentes. La primera se relaciona precisamente con los costos de operación, mientras más sofisticadas y precisas sean las regulaciones para el tratamiento de datos mayores externalidades positivas reportará ese contexto al negocio, sin tener que asumir las brechas de la legislación como desafíos propios.

En segundo lugar, el hecho de que dos empresas de volúmenes y rubro similares cuenten con estándares distintos —en una misma plaza y al mismo tiempo— nos arroja al menos la duda razonable de que alguna falla de mercado podría originarse por la vía de que no existirían las mismas reglas de juego para que la competencia despliegue su negocio.

3. La protección de datos comparte similares gratitudes de mercado como las políticas de responsabilidad social empresarial, impactando en este caso directamente en los titulares de datos (la mayoría de las veces el cliente), que siempre esperan información adecuada y proporcional a la entregada.

No se debe perder de vista que la protección de datos es un derecho fundamental, aquel definido como de "autodeterminación informativa" y que en esa virtud permite al titular del dato controlar su información de manera que ésta sea genuina y circule respetando estándares como calidad y adecuación. Es importante hacer énfasis en este punto ya que por lustros la protección de datos —quizás por una tradición "*americanista*"— ha estado a ratos fuertemente influenciada por la libertad de expresión, siendo vista como contradictoria de esta última. Se trata de un sesgo errado ya que la protección de datos busca precisamente llenar una dimensión de la libertad de expresión que apunta a la entrega de información referida a personas individuales.

Así, el respeto por la circulación de datos responsables no puede sino contribuir a que el mercado de la información, pública y privada, encuentre su centro de equilibrio y no arriesgue distorsiones que vayan en desmedro del interés general o lesionen derechos fundamentales.

(...) el respeto por la circulación de datos responsables no puede sino contribuir a que el mercado de la información, pública y privada, encuentre su centro de equilibrio y no arriesgue distorsiones que vayan en desmedro del interés general o lesionen derechos fundamentales.

Quizás hay aquí un punto de convergencia que vale la pena resaltar en el sentido de que en la protección de datos *"todos ganan"* por igual: los consumidores al controlar su información, las empresas al prevenir los riesgos de que la información de sus clientes sea vulnerada y los países al vigorizar sus políticas públicas de atracción de inversiones, mejorando su posición comparativa y cumpliendo con los niveles internacionales en esta materia.

4. La protección de datos no es sólo un requisito del negocio de los servicios globales, sino que es un activo agregado del mismo, por lo cual estamos convencidos de que ésta es a la vez regulación e incentivo, apostando a que en este ámbito el costo de contar con marcos regulatorios adecuados[13] sólo puede generar retornos al país que invierte en ellos, convirtiéndolos en verdaderas plataformas de servicios.

Como se ha sostenido, la deslocalización de funciones o procesos, propia de la industria de servicios globales, conlleva la lógica de instalarse en países en donde el ambiente público, institucional y legal otorgue garantías a sus operaciones, a través de regulaciones certeras y recogidas en los instrumentos internacionales descritos. Estas regulaciones no constituyen un mayor costo de transacción para sus operaciones sino que, por el contrario, son una ventaja comparativa para desenvolverse en los mercados.

En el caso de Chile esto adquiere una importancia creciente por el impacto de los servicios globales en el mercado nacional, y el crecimiento evidenciado en países como Colombia, Perú, Uruguay y Argentina (este último con nivel adecuado de protección), los que han avanzado hacia

(13) Es evidente que para aproximarnos al concepto de marcos regulatorios adecuados es necesario revisar lo que apuntamos con ocasión de "Nivel Adecuado de Protección" y "Puerto Seguro", en la sección anterior.

políticas de protección de datos más audaces, transformándose en plazas altamente atractivas para el desarrollo de servicios globales.(14)

Importante es destacar que el sector privado comparte esta necesidad y la ha manifestado en instancias como el Consejo Estratégico de la Industria de Servicios Globales, alianza público-privada que lidera la Corporación de Fomento de la Producción (CORFO), lo cual demuestra que esta preocupación no es un monopolio estatal de posibles regulaciones emergentes, sino una necesidad de competitividad de los propios destinatarios de la regulación.

IV. Conclusiones y desafíos futuros

La protección de datos implica no sólo avanzar en la tutela de las garantías fundamentales —transitando de un modelo binario de resguardo de la intimidad a uno de autodeterminación informativa—, sino que además trae consigo una serie de impactos positivos en áreas extrajurídicas, como ocurre en los servicios globales.

Esto refuerza nuestra tesis de aunar alianzas institucionales bien constituidas, en donde consumidores, empresas, agencias públicas y ciudadanos titulares de datos personales entiendan lo importante de una normativa informada y en la cual todos los intereses en juego se develen con organización y transparencia en el mercado, contribuyendo así a concentrar costos de regulación.

Esto refuerza nuestra tesis de aunar alianzas institucionales bien constituidas, en donde consumidores, empresas, agencias públicas y ciudadanos titulares de datos personales entiendan lo importante de una normativa informada (...)

Para lograrlo es indispensable promover liderazgos responsables y diversos que procedan de todos los sectores involucrados, de manera de no polarizar el debate en grupos específicos.

En el caso de la industria de servicios globales resulta crítico tener una discusión sensible al interés privado y que incluya a todos los rubros y

(14) Cifras de la Agencia Española de Protección de Datos (AEPD) exhiben que, entre enero y septiembre de 2010, México ha recibido 18 autorizaciones de transferencia de datos, Perú 11, Uruguay 9, Colombia 9 y Chile 4. Esto evidencia el impacto de las políticas a favor de la protección de datos en el estímulo comercial. Por cierto que Argentina no figura en este listado, ya que al tener "nivel adecuado de protección" no requiere de autorización para estas transacciones.

empresas potencialmente involucradas, más allá de su tamaño. En esta lógica es perfectamente posible pensar en los nuevos mercados que van surgiendo, por ejemplo, en las empresas emergentes que se abren a la oferta de tratamiento de información por encargo.

Un segundo orden de materias que consideramos importante, más allá del arreglo institucional por el cual se opte para albergar una regulación de protección de datos, es la provisión de una normativa que promueva "*externalidades posicionales*". Éstas deberán ser entendidas como aquellas recompensas colectivas que el comportamiento individual de los obligados es capaz de entregar al sistema. En términos simples: que todos, en alguna medida, ganen con la protección de datos.(15)

¿Cómo avanzar en esa dirección? Creemos que a partir de la generación de un *accountability* sustantivo(16) que priorice la aplicación de políticas transparentes, justificadas desde el interés público y desde el punto de vista económico (eficiencia y redistribución).

¿Cómo avanzar en esa dirección? Creemos que a partir de la generación de un* accountability *sustantivo que priorice la aplicación de políticas transparentes, justificadas desde el interés público y desde el punto de vista económico (...)

Esto último no es una novedad cuando se entra en mercados regulados y de fuerte competencia, pero es especialmente relevante considerarlo si en esos mercados habrá en juego actores muy diversos, por su identidad, tamaño, interés y ubicación geográfica. Es así que cabe sostener que la rendición de cuentas es un concepto relacional, que cobra particular vigencia en la protección de datos y en su vinculación con la industria de servicios globales, en donde las bondades o defectos de una buena política cruzarán fronteras**.**

En tercer lugar la protección de datos debiera ser un terreno fértil para la autoregulación y las políticas de normalización en materia de flujos de información. Esto no significa promover alternativas sustitutivas a ciertos parámetros normativos básicos que hemos venido revisando, pero sí alentar una cultura responsable de tratamiento de la información que pueda colaborar con disminuir costes regulatorios y vigorizar el *enforcement* de la legislación.

(15) En materia regulatoria esto podría simplificarse a través de un "Pareto Superior", en virtud del cual al menos un individuo gana y ninguno pierde.

(16) Vid "Accountability y Transparencia en el Estado Regulador"; Juan José Romero Guzmán, Apuntes Inéditos.

En esta línea los sellos de calidad o confianza en comercio electrónico y mecanismos de resolución de conflicto alternativos, en soporte *online*, son un ejemplo de buenas prácticas que permiten avanzar en la dirección correcta y sobre la cual el énfasis del estándar de APEC en el Proyecto Pathfinder (al cual aludimos anteriormente) ha puesto especial atención.

Por último, un llamado a mirar las cosas desde una perspectiva diferente: la protección de datos no debe ser asumida como una exquisitez jurídica que interese a sesudos estudiosos de un área del Derecho o beneficie a mercados elitistas y desconectados de la necesidad económica local. La protección de datos es, al mismo tiempo, tutela ciudadana, garantía de consumidor y un muy buen negocio, ya que sólo puede proveer bienes públicos al mercado de la información, corrigiendo asimetrías, mejorando la calidad y adecuación de los datos que circulan y sincerando la responsabilidad de quienes intervienen en su tratamiento. Significa entonces un esfuerzo de Estado, colectivo y democrático, que redundará en iguales beneficios para todo el país.

La protección de datos es, al mismo tiempo, tutela ciudadana, garantía de consumidor y un muy buen negocio, ya que sólo puede proveer bienes públicos al mercado de la información, corrigiendo asimetrías, mejorando la calidad y adecuación de los datos que circulan y sincerando la responsabilidad de quienes intervienen en su tratamiento.

Autor

Francisco J. Cruz Fuenzalida

Abogado de la Pontificia Universidad Católica de Chile, postitulado en Derecho Constitucional y egresado del Programa de Magíster en Derecho Público de esa misma Universidad. Miembro de la Red Iberoamericana de Protección de Datos (RIPD).

V
La institucionalización de la protección de datos de carácter personal*

María Nieves de la Serna Bilbao

* El presente trabajo se desarrolla dentro del proyecto DER2009-09819 "De los servicios públicos y los servicios de interés general: El futuro de intervención pública en un contexto de crisis económica", dirigido por el prof. T. Quadra Salcedo.

I. Introducción

Como es sabido, la recopilación y organización de los datos pertenecientes a las personas físicas o jurídicas es una actividad tradicionalmente enfocada tanto al desarrollo del tráfico público como de la actividad privada. Es fácil recordar la existencia de grandes ficheros de distinta naturaleza destinados a acumular datos de las personas, entre los que cabe citar, por ser los más conocidos, a los ficheros de datos fiscales, bancarios, médicos, de solvencia o, incluso, penales. No es posible ignorar, sin embargo, que aquella recopilación y organización de datos personales experimentó un cambio importante tras la aparición de los computadores y la generalización de su uso en toda la población. En efecto, los ordenadores han permitido aumentar de manera exponencial, de forma prácticamente ilimitada, el almacenamiento de datos en los distintos soportes. Este gran adelanto tecnológico —en constante evolución—, sumado a la aparición de Internet, que permite intercomunicar, obtener, difundir y/o apropiarse de los datos personales —sean verídicos o no— por cualquier sujeto, llevó a un replanteamiento total de la regulación jurídica existente, dado que era evidente el peligro que para la intimidad de las personas —en sentido amplio— implicaban tales elementos. En efecto, no cabe duda de que los ordenadores con su gran velocidad de cálculo y los relevantes avances en las telecomunicaciones son herramientas muy importantes para obtener datos personales, recopilarlos, compararlos y contrastar los mismos en un instante.

(...) los ordenadores han permitido aumentar de manera exponencial, de forma prácticamente ilimitada, el almacenamiento de datos en los distintos soportes.

Hoy son indiscutibles las posibilidades ilimitadas que proporcionan estas herramientas tecnológicas para —insistimos— captar, almacenar, relacionar y trasmitir todo tipo de datos personales que, enlazados y unidos entre sí, pueden revelar múltiples facetas de la vida de las personas y que, utilizadas por terceros bien intencionados o no, pueden llegar a transformar aquellos datos en una fuente de información muy poderosa, a tal punto de llegar a controlar y presionar a la sociedad causando perjuicios importantes. Muchos han sido los estudios dedicados a esta cuestión,

y en ellos se solicita el amparo del derecho para controlar y decidir sobre los datos de cada persona, de tal forma que podamos controlar nuestra intimidad, asegurando, por ejemplo, una calidad mínima de vida de tal suerte que los demás sólo conozcan aquello que cada persona desea compartir y revelar a los otros, sin que por ello se pierda tampoco el control sobre los datos personales. No creemos que el avance tecnológico sea peligroso *"per se"* para la sociedad. Por el contrario, ciñéndonos a la materia de estudio, la existencia de ficheros de datos personales resulta necesaria e importante para el funcionamiento de la misma al permitir que informaciones relevantes y de gran trascendencia para ésta puedan estar disponibles en momentos cruciales —por ejemplo, los datos de salud cuando se trata de salvar la vida de las personas—. No obstante esta finalidad quedaría limitada o podría ser perjudicial para las personas si aquellos datos no fuesen exactos, no se encontrasen puestos al día, o si el acceso a los mismos no tuviera unos límites bien definidos. De ahí que el derecho relativo a la protección de datos deba proteger ese ámbito de intimidad, libertad y dignidad, y regular medidas de control sobre los datos —sea de acceso, uso, disposición, modificación, cancelación, como de veracidad, proporcionalidad, finalidad, etcétera—, los usos y destinos de los mismos para evitar poner en peligro la dignidad de las personas. Recordemos que los datos aisladamente considerados pueden carecer de significación intrínseca, pero que, coherentemente enlazados entre sí, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Recordemos que los datos aisladamente considerados pueden carecer de significación intrínseca, pero que, coherentemente enlazados entre sí, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Finalmente, no se puede dejar de mencionar que en la actualidad el derecho a la protección de datos, tal como lo concebimos, no sólo contempla los datos incluidos en los ficheros informatizados —denominados automatizados— sino que también se hace extensivo a los ficheros manuales o en papel —ficheros no automatizados—, en cuanto a que éstos pueden también poner en peligro la libertad, la dignidad o la intimidad en el sentido amplio del término.

II. Un derecho nuevo y en constante evolución

Las inquietudes planteadas en el apartado anterior han dado lugar a la aparición de un nuevo derecho —llamado de tercera generación o de cuarta—[1] que ha ido adquiriendo cuerpo bajo distintas formas tanto en los ordenamientos de los estados democráticos como en las instituciones internacionales.[2] Su denominación no es unívoca; en ocasiones se identifica con los conceptos de *"privacy"* en el ámbito norteamericano,[3] *"derecho a la autodeterminación informativa"*, en Alemania,[4] o *"derecho a la protección de datos"*, en el ámbito de la Unión Europea y en la Carta de los Derechos Fundamentales de la Unión Europea aprobada en el año 2000 en su artículo 8.[5] Además, si bien este nuevo derecho se identifica con una concepción amplia del derecho a la intimidad, se distingue desde

Las inquietudes planteadas en el apartado anterior han dado lugar a la aparición de un nuevo derecho —llamado de tercera generación o de cuarta— que ha ido adquiriendo cuerpo bajo distintas formas tanto en los ordenamientos de los estados democráticos como en las instituciones internacionales.

(1) De acuerdo con el profesor Murillo de la Cueva, P.L en "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, en *El Derecho a la Autodeterminación informativa*, edit. Fundación Coloquio Jurídico Europeo, Madrid, 2009 págs11 y ss., se denominan así porque "responden a los retos y dificultades de la sociedad de nuestros días. Principalmente, a los derivados del avance tecnológico, del impacto sobre el medio y de las nuevas formas de desigualdad".

(2) Así, por ejemplo, cabe citar el Convenio 108, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, en 1981, o las numerosas Recomendaciones de la OCDE sobre circulación internacional de datos personales para la protección de la intimidad y la recomendación relativa a la seguridad de los sistemas informáticos de 1980. Sobre los antecedentes del derecho a la protección de datos véase Téllez Aguilera A; *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, edit. Edisofer, Madrid, 2002.

(3) El uso del término *privacy* —que se suele situar hacia 1873, recogido en el artículo "The Right to Privacy" de Warren y Brandeis— proviene de las pretensiones jurídicas de protección de la vida privada para preservar el entorno personal de posibles injerencias no consentidas. Su evolución llevó a que adquiriera en Estados Unidos el rango de Derecho Constitucional en 1965, si bien en sentido amplio del término dentro del derecho a la intimidad. Finalmente, destacar que en Estados Unidos en 1975 se aprueba la Privay Act donde se recogen los aspectos principales de este derecho. Véase Piñar Mañas, J.L., "La protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

(4) Término utilizado en la Sentencia del Tribunal Constitucional Federal de Alemania de 15 de diciembre de 1983 relativa a la Ley del Censo. Es preciso destacar al respecto que en Alemania ya se había aprobado la Ley Federal alemana en 1977.

(5) En el año 1992 se inicia la tramitación del proyecto de Directiva de protección de datos que finalmente es aprobada como Directiva 95/46/CEEE. Pero también se encuentran antecedentes anteriores como la Resolución del Parlamento Europeo sobre "La tutela de los Derechos del individuo frente al creciente progreso técnico en el sector de la informática", adoptada 1979. El Tribunal Constitucional Español también hace eco de este término en su célebre sentencia 292/2000, de 30 de noviembre, en donde reconoce y distingue el derecho a la protección de datos del derecho a la intimidad.

una perspectiva más estricta en tanto que si, ciertamente, el derecho a la intimidad protege la vida privada de las personas —dentro de la que se comprende la familiar, de amistad y de relaciones personales— de cualquier invasión por parte de terceros no autorizados y en defensa de la dignidad, el derecho a la intimidad en sentido estricto tiene como objeto excluir del conocimiento ajeno las intromisiones de terceros en la vida privada de las personas en contra de su voluntad, para lo cual reconoce a su titular una facultad de preservar del conocimiento ajeno nuestra faceta privada.

De esta forma, aquel nuevo derecho se preocupa por fijar reglas objetivas sobre el tratamiento de estos datos, prevé deberes jurídicos para los terceros que se apropien de los datos y establece procedimientos específicos de garantía.

Por el contrario, el denominado derecho a la protección de datos se diferencia del supuesto anterior —derecho a la intimidad en sentido estricto—, en tanto que el bien jurídico subyacente es la libertad informática, valor que persigue, sencillamente, garantizar a cada una de las personas un poder de control y disposición sobre los datos que les afectan, sean íntimos o no, públicos o privados, para preservar de este modo y, en último extremo, la propia identidad, nuestra dignidad y libertad. De esta forma, aquel nuevo derecho se preocupa por fijar reglas objetivas sobre el tratamiento de estos datos, prevé deberes jurídicos para los terceros que se apropien de los datos y establece procedimientos específicos de garantía. Este derecho también requiere la existencia de una institución pública independiente cuya finalidad es velar por el cumplimiento de las normas que integran este nuevo derecho.(6) Reconoce así unos derechos y deberes que se erigen en límites impuestos por el legislador al tratamiento de datos por parte de terceros y determina la existencia de normas sancionadoras, penales y administrativas que deben dirigirse a asegurar su plena vigencia. Como destaca Murillo de la Cueva, "los deberes que pesan sobre quienes pretenden tratar información personal, contrapartida de los derechos y de las exigencias de los principios, comportan, junto a su estricto respeto, la observación de formas y procedimientos imprescindibles para hacer efectivas las garantías del derecho de protección de datos". De esta forma, se puede afir-

(6) Normalmente, se suele considerar la aparición de este derecho a los años sesenta del siglo pasado, cuando se reúne, en el seno del Consejo de Europa, la Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, de donde surge la Resolución 509 de la Asamblea del Consejo de Europa sobre "Los derechos humanos y los nuevos logros científicos y técnicos".

mar que la protección de datos adquiere una sustantividad propia y se define bajo un rótulo nuevo, con una denominación singular que lo identifica, distinta del derecho a la intimidad, en sentido estricto.

Finalmente, corresponde destacar que se trata de un derecho que se encuentra en constante evolución y que, como destaca el profesor Piñar Mañas,(7) aún continúa perfilándose. Su fundamento radica en la Sentencia de 27 de febrero de 2008 del Tribunal Constitucional alemán, que considera como integrante del derecho a la protección de datos la confidencialidad e integridad de los sistemas tecnológicos de información —dentro de los que se comprenden los ordenadores personales, PDAs, teléfonos móviles—. Esta nueva consideración es debido a que, a través de ellos —solos o interconectados con otros—, se puede acceder a datos personales que expresan la personalidad o aspectos relevantes del comportamiento de las personas, como los correos electrónicos. Por ello, para el citado tribunal, sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro *online*, prohibiendo en consecuencia la utilización de aquellas técnicas en investigaciones de delitos "normales" o en la actividad genérica de servicios de inteligencia.

(...) sólo en casos de evidencia de un peligro concreto para la vida, la integridad física o la libertad de las personas, así como para los fundamentos del Estado, los poderes públicos pueden hacer uso de técnicas de registro online (...)

III. El objeto de protección de este derecho "el dato"

Como hemos expresado, el derecho a la protección de datos tiene como objeto de protección el "dato" de una persona física identificada o identificable, aunque algunas legislaciones hayan extendido también su protección a los datos de las personas jurídicas. Por ello, la delimitación de qué se entiende por dato es muy importante, dado que equivale a definir el ámbito de aplicación de las normas sobre protección de datos, es decir, lo que entra o queda fuera de él.(8)

(7) Ob. cit.; pág. 98 y ss.

(8) Véase el artículo de Fonseca Ferrandis, F; "Comentario al artículo 2 de la LOPD", en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson Civitas, 2010, Madrid, págs. 156 y ss.

Con carácter general, la comprensión del concepto de dato contenida en las distintas normativas vigentes es bastante amplia, definiéndolo como «toda información sobre una persona física identificada o identificable (el "interesado"). A estos efectos se considera identificable a 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».(9) Dentro de esta definición se comprenden distintos tipos de datos como los numéricos, alfabéticos, gráficos, fotográficos, acústicos o de cualquier otro tipo concernientes a personas físicas identificadas o identificables, independiente de que el dato sea íntimo o no, privado o público. Lo importante es que éste, cualquiera que sea, pertenece a una persona concreta, identificada o identificable y es a ésta a quien el Derecho reconoce un poder de control sobre el mismo y, paralelamente, impone al tercero que se apropia de los datos ciertos deberes jurídicos para que no afecten a los derechos de los titulares, sean éstos fundamentales o no. La amplitud con la que se define el concepto de "datos" determina que dentro del mismo se incluyan todos aquellos que identifiquen o permitan la identificación de la persona, y que puedan servir para la confección de un perfil ideológico, racial, sexual, económico o de cualquier otra índole, o para cualquier otra utilidad y que en determinadas circunstancias constituyan una amenaza para el individuo. Sólo se pueden considerar excluidos del concepto aquellos datos que expresamente la normativa disponga, así como los datos disociados, es decir, aquellos que no permiten la identificación de un afectado o interesado.

(...) la comprensión del concepto de dato contenida en las distintas normativas vigentes, es bastante amplia, definiéndolo como «toda información sobre una persona física identificada o identificable (...)

(9) Definición contenida en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, aplicada por todos los países miembros de la Unión Europea. En parecidos términos se pronunció la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad*, *en relación con el Tratamiento de Datos de carácter personal*, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, donde se define a los "Datos de carácter personal" como *cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados*. La mención a la citada conferencia es importante dado que tuvo como finalidad definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal así como facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado. También la normativa española, contenida en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Por otra parte, no se puede ignorar que, si bien la amplitud del concepto de "dato" es beneficiosa para los titulares de los mismos —en tanto que "todos" sus datos encuentran protección—, ha supuesto también la existencia —tanto a nivel internacional como dentro de la propia Unión Europea— de cierta incertidumbre. En efecto, aquella amplitud ha determinado la presencia de diversos criterios a la hora de definir el concepto de dato, diversidad que también se ha complicado por la existencia de regulaciones especiales para datos peculiares, como por ejemplo, los datos relativos a salud, telecomunicaciones, laborales, imagen, videovigilancia u otros.

(...) no se puede ignorar que, si bien la amplitud del concepto de "dato" es beneficiosa para los titulares de los mismos —en tanto que "todos" sus datos encuentran protección—, ha supuesto también la existencia —tanto a nivel internacional como dentro de la propia Unión Europea— de cierta incertidumbre.

IV. Características del régimen jurídico de protección de datos

Denominamos características principales del derecho a la protección de datos personales a aquellos elementos que hacen reconocible el derecho y, sin los cuales, el mismo no existe o es violentado. Dentro de estas características son esenciales los principios aplicables a todo tratamiento de datos, los derechos de los titulares de datos, los deberes jurídicos de las personas responsables de ficheros, los terceros que accedan a los mismos, la seguridad de los datos y la existencia de un poder público habilitado para controlar la correcta aplicación de la normativa sobre protección de datos. Veamos todos ellos.

1. Los principios aplicables en todo tratamiento de datos

Existen varios principios reconocidos en el ámbito del derecho a la protección de datos. Todos ellos se encuentran relacionados y ninguno es superior o ejerce una función más importante que los demás. Las clasificaciones sobre los mismos suelen variar de un lugar a otro pero, en definitiva, su contenido suele ser muy similar. En este trabajo reflejaré los más importantes y que nunca pueden dejar de reconocerse para que exista plenamente el derecho a la protección de datos.

En primer lugar, con carácter general, se suele exigir que todo tratamiento de datos de carácter personal se realice de manera "leal" en tanto

que no se produzcan discriminaciones injustas o arbitrarias para el titular del dato. Para ello es necesario que todo tratamiento se desarrolle con plena sujeción y cumplimiento de los principios y fines contenidos en las normativas internacionales existentes, de los derechos y libertades de las personas, y de la normativa vigente de cada país.(10)

El principio de finalidad es otro principio esencial en el ámbito de protección de datos e implica que todo tratamiento se debe limitar al cumplimiento de las finalidades determinadas, explícitas y legítimas para las que se ha obtenido el dato. Esto quiere decir que la persona responsable sólo se encuentra habilitada para realizar aquellos tratamientos compatibles con las finalidades para las que obtuvo el dato, a menos, claro está, que obtenga el consentimiento inequívoco del interesado para otras finalidades. El citado principio de finalidad, como ya se apuntó, presenta una especial importancia en la medida que sirve para valorar la validez de otros principios que rigen en el ámbito de protección de datos como tendremos ocasión de estudiar.

El principio de finalidad es otro principio esencial en el ámbito de protección de datos e implica que todo tratamiento de datos se debe limitar al cumplimiento de las finalidades determinadas, explícitas y legítimas para las que se ha obtenido el dato.

Otro principio intrínseco a la institución analizada es el principio de proporcionalidad que supone que todo tratamiento de datos se debe circunscribir a aquellos datos que resulten adecuados, relevantes y no excesivos en relación con las finalidades del tratamiento. En virtud de este principio la persona responsable debe verificar que los datos obtenidos y tratados en el fichero sólo sean los necesarios y adecuados al fin con el que fueron obtenidos. En consecuencia, le corresponde minimizar la cantidad de datos de acuerdo con la finalidad perseguida.

El principio de calidad es también esencial en esta materia. Él implica que le corresponde a la persona responsable asegurar que, en todo momento, los datos de carácter personal recogidos y tratados en los ficheros sean exactos, completos, se pongan al día y sean los necesarios para el cumplimiento de las finalidades para las que son tratados. Para lograr cumplir con este principio el responsable

(10) Entre las que cabe citar la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos de 1966 y la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad*, *en relación con el Tratamiento de Datos de carácter personal*, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009.

debe establecer un período de conservación de los datos así como modificar o cancelar de oficio aquellos datos inexactos o que hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento.

Por su relación con el contenido esencial del derecho a la protección de datos es preciso mencionar el denominado principio de transparencia o de información. En efecto, como hemos visto, el derecho a la protección de datos reconoce al titular del dato un poder de disposición sobre los mismos, lo que supone el derecho a conocer quién y para qué obtiene sus datos. Este conocimiento da transparencia al procedimiento de obtención y sólo se cumple si se proporciona antes de obtener el dato, de tal forma que permita conocer todos aquellos extremos necesarios para su control. El principio se cumple si se facilita información sobre determinados extremos tales como la identidad del responsable, la finalidad del tratamiento, los destinatarios a los que prevé ceder los datos de carácter personal, así como la forma en la que los interesados pueden ejercer los derechos reconocidos y cualquier otra información necesaria. Toda la información proporcionada a los interesados debe ser clara, sencilla, entendible y adecuada a la edad del titular del dato —no es lo mismo un menor que un adulto— y, como regla general, se debe facilitar con carácter previo a la recogida o en el mismo momento el que se produce la obtención del dato. El principio se cumple también si los datos no se han obtenido del propio interesado —cuando la norma lo autorice— y la información se facilite a posteriori, dentro de un tiempo prudencial, salvo que resulte imposible o exija un esfuerzo desproporcionado a la persona responsable. Finalmente, es importante destacar —dada la peculiaridad que presenta— que cuando los datos sean obtenidos a través de redes de comunicaciones electrónicas, el principio de transparencia se considera satisfecho si se procede a la publicación de políticas de privacidad, fácilmente accesibles e identificables, que incluyan todos los extremos antes señalados.

(...) el derecho a la protección de datos reconoce al titular del dato un poder de disposición sobre los mismos, lo que supone el derecho a conocer quién y para qué obtiene sus datos.

Aunque no se trate de un principio propiamente dicho sino más bien de un deber, es necesario mencionar el denominado "deber de secreto" o "deber de confidencialidad" que tiene que regir para todas las personas que conozcan los datos. Se trata de un aspecto muy importante para el correcto funcionamiento de la institución de protección de datos, ya que implica la

imposición de la carga de todas las personas —responsables o no— que intervengan en cualquier fase del tratamiento de los datos de carácter personal de respetar la confidencialidad de los mismos. Esta obligación no se agota con la relación laboral o de otro tipo que se haya tenido y haya permitido acceder al dato sino que, por el contrario, continuará vigente aun después de finalizadas aquellas. Téngase en cuenta que no cumplir este mandato puede suponer la vulneración de todo el sistema de protección de datos, por cuanto las personas que acceden a los datos, por la relación existente, son infinitas. Piénsese, por ejemplo, en los datos personales que tiene una empresa y su tratamiento y, aún más, si esa empresa externaliza parte de su actuación. Por ello es un deber que debe respetarse y hacerse cumplir para que la institución de protección de datos pueda ser efectiva.

2. Elementos esenciales del régimen jurídico de la protección de datos

a. Alcance

Como hemos visto, el derecho a la protección de datos supone el reconocimiento a los titulares de los datos correspondientes de un control y un poder de disposición sobre los mismos que se materializa a través de derechos y garantías que, en definitiva, permiten hacer efectivo este derecho. Correlativamente se impone a las personas responsables que obtienen, conservan, tratan, transmiten o ceden datos personales —extensivo a todos los terceros que acceden a los datos, tales como encargados de tratamiento, cesionarios, trabajadores, etcétera—, ciertos deberes jurídicos u obligaciones. Como cierre de aquellos reconocimientos y, para lograr la efectividad de los mismos, las distintas regulaciones exigen la existencia de uno o varios poderes públicos independientes —cuyo número depende de la configuración territorial de cada Estado— que tutelen la correcta aplicación de este derecho.

(...) el derecho a la protección de datos supone el reconocimiento a los titulares de los datos correspondientes de un control y un poder de disposición sobre los mismos que se materializa a través de derechos y garantías que, en definitiva, permiten hacer efectivo este derecho.

Ahora bien, como todo derecho, su reconocimiento no es absoluto y, por tanto, admite un grado de flexibilidad en algunos ámbitos con el fin de lograr

un equilibrio adecuado entre la protección de los derechos del interesado, los posibles intereses legítimos de las terceras personas y el interés público. De ahí la existencia de algunas excepciones al régimen general, excepciones que en todo caso deben encontrar una correcta justificación, adoptada por el legislador y fundamentada en el interés mayor. Con carácter general, en todos los ordenamientos jurídicos se suelen fundamentar dichos límites en la defensa y la seguridad del Estado y en la averiguación de los delitos.

b. Los titulares de los datos

A los titulares de los datos —denominados también afectados— el derecho a la protección de datos, como hemos visto, les reconoce un control y disposición sobre el uso y el destino de los mismos a fin de impedir el tráfico ilícito y lesivo para su dignidad y sus derechos —sean estos derechos fundamentales o no—.[(11)] Así, a los titulares se les reconoce una facultad de decisión de consentir sobre cuál o cuáles de los datos personales quieren proporcionar a un tercero —poder público o privado— y para qué fin, poder de disposición que también les permite oponerse a la apropiación o uso de los datos por terceros.

A los titulares de los datos —denominados también afectados— el derecho a la protección de datos, como hemos visto, les reconoce un control y disposición sobre el uso y el destino de los mismos a fin de impedir el tráfico ilícito y lesivo para su dignidad y sus derechos (...)

Ahora bien, esta regla no es absoluta y puede ser exceptuada siempre que una norma con rango de ley así lo contemple por considerar que prevalece el interés general. En otras palabras, corresponde a los representantes de la soberanía popular permitir excepcionar el control del titular del dato y sustituir su consentimiento. Así, por ejemplo, en el caso de la seguridad o la defensa del Estado o, en otro orden de cosas, cuando se permite a las

(11) Existen numerosos estudios que explican la división y, consecuentemente, la diferenciación de estos derechos. Sin ánimo de exhaustividad se pueden consultar los distintos trabajos del profesor Pérez Luño, a "Los Derechos Humanos en la sociedad tecnológica" en vol. *Cuadernos y Debates*, Centro de Estudios Constitucionales, Madrid, 1989, o *La tercera generación de derechos humanos*, Aranzadi, Pamplona, 2006, del Magistrado Pablo Lucas Murillo de la Cueva, en *El derecho a la autodeterminación informativa,* edt. Tecnos, Madrid, 1990; *Informática y protección de datos*, en Centro de Estudios Constitucionales, Madrid, 1993, y del citado autor, conjuntamente con el profesor José Luis Piñar Mañas, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, y toda la bibliografía que allí se menciona.

autoridades públicas acceder a datos médicos en casos de epidemias con la finalidad de adoptar medidas inmediatas y preventivas. En estos supuestos prima el interés mayor antes que el particular.(12)

Como regla general, el derecho a controlar los datos implica, pues, para el titular de los mismos la facultad de consentir su obtención o tratamiento, consentimiento que sólo es válido si previamente se le facilita información por parte del tercero que obtiene los datos. Esta información, como hemos visto, debe tener un contenido mínimo que permita al titular conocer para qué y a quién autoriza su uso. Se trata, en este caso, de cumplir con el principio de información.

El derecho a la protección de datos reconoce también a sus titulares derechos que se configuran, todos ellos, como parte del contenido esencial del mismo. Se trata de los derechos de acceso, rectificación, cancelación y oposición, derechos que permiten al titular del dato controlar los datos y verificar en todo momento que cumplen con los principios antes mencionados (...)

El derecho a la protección de datos reconoce también a sus titulares derechos que se configuran, todos ellos, como parte del contenido esencial del mismo. Se trata de los derechos de acceso, rectificación, cancelación y oposición, derechos que permiten al titular del dato controlar los datos y verificar en todo momento que cumplen con los principios antes mencionados, en especial con el de calidad. Cada uno de ellos le permite controlar el dato, ya sea conociendo los que están en poder de terceros y sus fuentes de obtención, corrigiendo los mismos a través del derecho de solicitud de rectificación y modificación, solicitando la desaparición del fichero por medio de su cancelación o impidiendo que se lleve a cabo el tratamiento de sus datos de carácter personal o su cese. De esta forma adquiere relevancia, como destaca Murillo de la Cueva, la existencia del *"habeas data"*, institución cualificada activamente por los derechos o facultades que aseguran tal dominio

(12) En el ámbito español, la Ley Orgánica, 15/1999, de Protección de Datos de Carácter personal concreta que no es preciso el consentimiento cuando se recojan para el ejercicio de las funciones propias de las **Administraciones públicas** en el ámbito de sus competencias; se refieran a las **partes de un contrato o precontrato** de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; tengan por finalidad proteger un **interés vital del interesado** —salud; o cuando los datos figuren en **fuentes accesibles al público** y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero. Sobre el concepto de fuentes accesibles al público, véase de la Serna Bilbao, M.N. "Comentario al artículo 3.j) de la LOPD", en en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson Civitas, 2010.

y, pasivamente, por los límites opuestos a quienes desde los poderes públicos o desde la sociedad utilizan información de carácter personal.(13)

c. La persona responsable del fichero

Las personas responsables de los ficheros que obtienen, conservan, tratan, transmiten o ceden datos ajenos se encuentran sujetas, de acuerdo con el derecho a la protección de datos, a unas exigencias formales y procedimentales necesarias para garantizar el cumplimiento de los principios. Dentro de aquellas exigencias y a efectos de que se consideren lícitos los tratamientos, corresponden, básicamente, a las personas responsables los siguientes requisitos:

Las personas responsables de los ficheros que obtienen, conservan, tratan, transmiten o ceden datos ajenos se encuentran sujetas, de acuerdo con el derecho a la protección de datos, a unas exigencias formales y procedimentales necesarias para garantizar el cumplimiento de los principios.

- Utilizar los datos para las finalidades legítimas para las que fueron recabados y con respeto a todos los principios vigentes en materia de protección de datos. En este sentido, debe velar porque el fichero donde se vayan a introducir los datos se haya creado con una finalidad lícita, concreta y determinada y que los datos que allí se introduzcan sean proporcionados a la finalidad, exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Es su responsabilidad adoptar estas medidas.

- En general, antes de tratar un dato debe obtener el consentimiento del titular del mismo, consentimiento que debe ser libre, inequívoco, específico e informado, salvo que se exceptúe su obtención por ley —caso de los datos contenidos en las denominadas fuentes accesibles al público—.

- Finalmente, corresponde a la persona responsable la adopción de medidas de seguridad de forma que impida la manipulación o acceso de los datos por terceros no autorizados o la pérdida de los datos contenidos en los ficheros.

(13) Ob. cit, pág 18.

- En relación con el primer requisito, es preciso indicar que toda persona responsable, que trata datos ajenos, debe realizar tal tarea con pleno respeto a la dignidad de la persona. Por ello y, dado que la verificación de esta vulneración a posteriori no evitaría el daño causado, se exige con carácter previo a la creación de un fichero y antes de introducir datos en el mismo, verificar un control sobre la adecuación y proporcionalidad de los datos y fines por parte de una autoridad independiente, la cual debe llevar un registro público de los mismos. Se persigue de esta manera, por un lado, evitar la proliferación de ficheros y, por otro, controlar el cumplimiento de los principios de protección de datos en el fichero por parte de la autoridad pública habilitada al efecto. Todo ello, insisto, con carácter previo a la recopilación de datos. En consecuencia, corresponde a las personas responsables someter el proyecto de fichero a un control por un poder público independiente —llámese agencia, autoridad o supervisor de protección de datos, u otro— que es el que verifica la relación entre el fin explícito y legítimo perseguido y los datos que se pretende recopilar. Así, se garantiza el cumplimiento *"ex ante"* de todos los principios que rigen en materia de protección de datos, como el de finalidad, de calidad, de proporcionalidad, etcétera.

Por otra parte, cuando los datos de carácter personal objeto del tratamiento deban ser comunicados a un tercero ajeno a la persona responsable para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, el responsable debe velar porque se cuente siempre con el previo consentimiento del interesado, salvo que una ley prevea otra cosa —supuesto típico de la cesión de datos al poder público recaudador de impuestos por parte de todos los sujetos—. Se trata de la institución de la cesión de datos. También puede ser preciso comunicar los datos a terceros con los que el responsable contrate servicios —denominado encargados— en cuyo caso se

(...) cuando los datos de carácter personal objeto del tratamiento deban ser comunicados a un tercero ajeno a la persona responsable para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, el responsable debe velar porque se cuente siempre con el previo consentimiento del interesado, salvo que una ley prevea otra cosa (...)

suele exigir la firma de un contrato donde se especifiquen obligaciones para el encargado en aras de respetar el derecho a la protección de datos.

Es preciso indicar que son responsabilidad de la persona a cargo tanto los daños morales como los daños materiales ocasionados a los interesados. Por tal motivo, está obligado a adoptar las medidas necesarias para satisfacer los principios y las obligaciones establecidas por el derecho a la protección de datos. Recordemos en este caso el deber de confidencialidad que pesa sobre todas las personas que accedan a los datos. Es importante que los estados promuevan medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos, judiciales o administrativos, que les permitan obtener la reparación de los daños y/o perjuicios causados, sin desmedro de las sanciones penales, civiles o administrativas previstas, en su caso, por violación de la legislación nacional aplicable en materia de protección de datos.

En cuanto al consentimiento del titular del dato es preciso indicar que la persona responsable debe obtenerlo del titular con carácter previo a la introducción del dato en el fichero. Dicho consentimiento se debe producir por una manifestación de voluntad del titular del dato y no puede existir vicio alguno del consentimiento en los términos regulados por las normas vigentes.

En cuanto al consentimiento del titular del dato es preciso indicar que la persona responsable debe obtenerlo del titular con carácter previo a la introducción del dato en el fichero. Dicho consentimiento se debe producir por una manifestación de voluntad del titular del dato y no puede existir vicio alguno del consentimiento en los términos regulados por las normas vigentes, es decir, debe ser libre. Por tanto, está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos y los citados datos sólo se pueden recoger para el cumplimiento de finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Igualmente, se debe señalar que el consentimiento del afectado se debe producir para una concreta operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, no caben, por tanto, los consentimientos genéricos. El permiso debe ser también específico y corresponde al responsable del fichero informar al afectado sobre la existencia del tratamiento y las finalidades que se persiguen con el mismo, así como demostrar que ha informado correctamente al interesado y obtenido legalmente la aprobación. La persona responsable no

puede deducir el consentimiento por meros actos realizados por el titular de los datos —no cabe el consentimiento presunto—, siendo preciso que siempre exista expresamente una acción u omisión que implique la existencia del consentimiento, siendo en este caso un consentimiento inequívoco.

(...) independientemente de la obligación que pesa sobre la persona responsable, el titular del dato tiene reconocidos los derechos de acceso, rectificación, cancelación y oposición que le permiten controlar todos aquellos extremos.

Cuando el fichero esté creado, corresponde al responsable garantizar el cumplimiento de los principios y, en especial, que los datos contenidos sean exactos y puestos al día de tal forma que respondan con veracidad a la situación real del afectado, sean estos ficheros públicos o privados y cualquiera sea la finalidad perseguida. Recordemos que, en todo caso, independientemente de la obligación que pesa sobre la persona responsable, el titular del dato tiene reconocidos los derechos de acceso, rectificación, cancelación y oposición que le permiten controlar todos aquellos extremos.

En relación con las medidas de seguridad que el responsable debe establecer y aplicar comprenden las siguientes dimensiones:

i) Confidencialidad, por medio de la cual se persigue que el sistema sea seguro y concreta el mayor o menor secreto con el que se van a guardar.

ii) Integridad, que persigue que los datos contenidos en el fichero no puedan ser objeto de alteraciones indebidas, erróneas o no autorizadas.

iii) Fidelidad, en cuanto que los datos sean reales, exactos y puestos al día de acuerdo con la situación real del afectado.

iv) Disponibilidad, en virtud de la cual sólo pueden acceder a los datos a aquellas personas autorizadas para ello.

d. Los poderes públicos garantes de la aplicación del derecho a la protección de datos

Con carácter general, las distintas normativas han exigido la creación de entes públicos dotados de una posición de independencia.[14] Algunos autores, como Piñar

(14) Véase, por ejemplo, la Resolución 45/1990, de 14 de diciembre de la Asamblea General de Naciones Unidas.

Mañas se refieren a esta característica como un "principio de control independiente", principio que considera inherente a la institución de protección de datos en tanto que persigue garantizar la efectividad de dicho derecho. La falta o ausencia de aquel principio en alguna legislación impediría de lleno el cumplimiento del derecho a la protección de datos y, por tanto, lo desnaturalizaría.

A las citadas entidades, para el desarrollo de su función, se les debe reconocer distintas potestades, de control y vigilancia, de tutela de los derechos de las personas, de cooperación o de inspección y sanción, entre otras. Todas ellas persiguen velar por el respeto de todos los principios y derechos que son inherentes al derecho a la protección de datos así como el cumplimiento de todo el conjunto normativo que regula la institución de la protección de datos.

Una función de estos organismos que normalmente se suele olvidar es la relativa a la información y la formación. En efecto, esta actividad es, desde mi punto de vista, esencial dado que permite difundir y dar a conocer el derecho a la protección de datos, inculcando buenas prácticas, solventando dudas o problemas que se presentan, formando personal y a los distintos sujetos que intervienen o manipulan datos, elaborando recomendaciones, guías, informes, entre otras, todo ello para la correcta aplicación del derecho.

A las citadas entidades, para el desarrollo de su función, se les debe reconocer distintas potestades, de control y vigilancia, de tutela de los derechos de las personas, de cooperación o de inspección y sanción, entre otras.

Estos organismos, denominados agencias, supervisor, direcciones, etcétera, cuentan con una organización propia y en la que no pueden faltar:

- Los registros de ficheros públicos, cuya función es dar publicidad y conocimiento de los ficheros y tratamientos de datos personales existentes a efectos del ejercicio de los derechos reconocidos.

- Una sección dedicada a proporcionar información y atención de consultas, a efectos de divulgar y solventar las dudas que pueda ocasionar el respeto a la protección de datos.

- Otra dedicada a la inspección, para verificar ante denuncias o sospechas la aplicación correcta de la normativa de protección de datos, actuación que debería ir acompañada de medidas sancionadoras.

V. Conclusión

El derecho a la protección de datos es un nuevo derecho que pretende impedir que los grandes adelantos tecnológicos vulneren nuestra dignidad, libertad e intimidad en sentido amplio. No persigue "prohibir" los avances tecnológicos sino poner "límites" a los usos que dichas tecnologías nos ofrecen. Las tecnologías —ordenadores y telecomunicaciones— permiten el desarrollo de muchas posibilidades para poder obtener infinidad de datos personales y reunirlos de tal forma que no queden aspectos de la vida de las personas al margen del conocimiento ajeno. De ahí que el derecho a la protección de datos aparezca para proteger facetas de la personalidad de los sujetos al reconocer a las personas el derecho control y disposición sobre sus datos, como el derecho de acceso, rectificación, cancelación y oposición. Este derecho impone también deberes y concreta aspectos sobre la creación de los ficheros que deben en todo caso estar justificados en una finalidad legítima del titular, así como su uso y utilización y la exigencia de obtener el consentimiento del titular del dato proporcionando información. El no cumplimiento de estos presupuestos es una vulneración importante de los derechos de las personas, sean o no fundamentales. Esta protección se ha extendido también a los ficheros en papel —no automatizados—, en cuanto que éstos pueden también suponer una vulneración a la dignidad de la persona.

El derecho a la protección de datos es un nuevo derecho que pretende impedir que los grandes adelantos tecnológicos vulneren nuestra dignidad, libertad e intimidad en sentido amplio.

Todas las sociedades deben contar con una regulación clara y precisa que reconozca los derechos de los titulares de datos, establezca los principios e imponga deberes jurídicos a los terceros que accedan a dichos datos y les imponga obligaciones y responsabilidades. A estas exigencias se debe sumar la existencia de una institución independiente que garantice el cumplimiento de aquel derecho y su defensa, así como la articulación por parte de los estados de vías administrativas, sancionadoras y judiciales para poder hacer efectivas las reclamaciones que su incumplimiento conlleve.

Como destaca Murillo de la Cueva,[15] todas estas pretensiones se deben justificar a partir de la misma dignidad de la persona y guardan una estrecha

(15) Ob. cit., pág 16.

relación con la libertad que le caracteriza. Libertad individual en su más amplio sentido, concebida como identidad, dado que el uso incontrolado de los datos personales por terceros conlleva riesgos e inconvenientes y lleva a aquellos que se sienten observados y controlados a comportarse de una forma concreta sin poder manifestarse con su propia forma de ser.

Finalmente, no podemos olvidar que se trata de un derecho en constante evolución. Tiene que hacer frente y adecuarse a los nuevos adelantos tecnológicos. De ahí que continuarán apareciendo importantes retos legales y que se presenten ámbitos nuevos por tratar y regular. En este momento es posible citar el "derecho al olvido" que está planteando una verdadera discusión en relación con los buscadores de información en Internet.(16)

(16) Véase la Resolución de la Agencia Española de Protección de Datos sobre Google.

Referencias

Resulta imposible citar en este lugar toda la bibliografía existente sobre esta materia

-DAVARA RODRIGUEZ, M.A. *La protección de datos en Europa*, Madrid, 1998.
-De la SERNA BILBAO, M.N. "Comentario al artículo 3.j) de la LOPD", en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson/Civitas, Madrid, 2010.
-De la SERNA BILBAO, M.N. "La agencia de protección de datos española: con especial referencia a su característica de independiente", en *Actualidad Informática Aranzadi*, núm. 22, 1997, págs. 1 y ss.
-FONSECA FERRANDIS, F. "Comentario al artículo 2 de la LOPD", en *Comentario a la Ley Orgánica de protección de datos de carácter personal*, edit. Thomson/Civitas, Madrid, 2010.
-MARTINEZ MARTINEZ, R. *Una aproximación crítica a la autodeterminación informativa*, Thomson/Civitas, Madrid, 2004.
-MURILLO DE LA CUEVA, P.L. "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, en *El derecho a la autodeterminación informativa*, edit. Fundación Coloquio Jurídico Europeo, Madrid, 2009.
-PEREZ LUÑO, A. "Los Derechos Humanos en la sociedad tecnológica", en *Cuadernos y Debates*, Centro de Estudios Constitucionales, Madrid, 1989.
-PIÑAR MAÑAS, J.L. "La protección de datos: origen, situación actual y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio jurídico Europeo, Madrid, 2009.
-RALLO LOMBARTE, A. *Derecho y redes sociales;* edit Civitas/Thomson; 2010.
-TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, edit. Edisofer, Madrid, 2002.
-TRONCOSO REIGADA, A. "Introducción y presentación", en *Protección de datos personales para Servicios Sanitarios Públicos*, edit. Thomson, Cívitas, Madrid, 2008.
-TRONCOSO REIGADA, A. "Introduction And presentation", en An aproach to data protection in Europe. APDCM/Thomson-Civitas, Madrid, 2007, pp. 9-58.

-VIZCAINO CALDERON, M. *Comentarios a la Ley Orgánica de Protección de Datos de carácter personal*, edit Civitas, Madrid, 2001.
-VVAA. *Comentario a la Ley Orgánica de protección de datos de carácter personal*, Director TRONCOSO REIGADA, edit. Thomson/Civitas, Madrid, 2010.
-VVAA, Comentarios al reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Directores PALOMAR OLMEDA y GONZALEZ ESPEJO, Thomson/Civitas, Madrid, 2009.

Autora

María Nieves de la Serna

Profesora titular de Derecho Administrativo, Universidad Carlos III de Madrid.

VI
El problema del tratamiento abusivo de los datos personales en salud

Lorena Donoso Abarca

I. Introducción

El tratamiento de datos personales es uno de los motores de la sociedad actual. Las decisiones en todos los ámbitos requieren de información para ser tomadas y el sector de la salud no es una excepción. En efecto, las instituciones públicas y organismos privados de atención como de aseguramiento de la salud precisan información veraz y oportuna tanto para la adopción de políticas públicas como para la toma de decisiones económicas, asociadas, por ejemplo, al otorgamiento de beneficios, prestaciones pecuniarias, definición de primas, etcétera. Además de la natural necesidad de contar con esta información para efectos de diagnóstico o tratamiento.

(...) la industria farmacéutica necesita información relativa a la efectividad de los fármacos que produce, para lo que busca datos sobre los efectos de su aplicación en pacientes concretos. Adicionalmente, los laboratorios capturan información en los puestos de venta (principalmente farmacias) para analizar los comportamientos de mercado.

Asimismo, la industria farmacéutica necesita información relativa a la efectividad de los fármacos que produce, para lo que busca datos sobre los efectos de su aplicación en pacientes concretos. Adicionalmente, los laboratorios capturan información en los puestos de venta (principalmente farmacias) para analizar los comportamientos de mercado de sus productos respecto de sus equivalentes de otros laboratorios. En nuestro trabajo nos referiremos a estas dos situaciones. Ahora bien, no obstante hemos sido testigos de conductas reprochables de parte de los laboratorios, relativas a la captura de información de prescripciones de remedios por los facultativos, no nos referiremos aquí a este aspecto del tratamiento de datos personales.

Un tercer tema que nos interesa dice relación con la implementación de la licencia médica electrónica.(1) Entendemos que esta experiencia es un avance hacia la ficha médica electrónica y la receta médica electrónica, pero es necesario reflexionar sobre la protección de los datos personales contenidos en estos documentos y los sistemas asociados a su administración por parte del sistema de salud.

(1) Al respecto véase el D.S. N°3, de 1984, del Ministerio de Salud, Resolución Exenta Nº 608, de 2006, del Ministerio de Salud.

En cuarto lugar, queremos llamar la atención respecto del tratamiento de datos personales obtenidos a partir de la toma de muestras médicas, ya sea para la realización de análisis clínicos dentro de un procedimiento de diagnóstico o tratamiento, o en el marco de una investigación *in vivo* o *in vitro*, asociado a una investigación científica o farmacéutica.

En sede de Salud se han realizado algunos ajustes normativos, a través del artículo 127 del Código Sanitario, modificado por la Ley 19.628, del DFL 1 de 2005 del Ministerio de Salud,(2) que fija el texto refundido de la Ley 18.933 sobre instituciones de salud previsional, que señalan expresamente las atribuciones del Ministerio de Salud(3) y del Fondo Nacional de Salud(4) en materia de tratamiento de datos personales, y las normas relativas a la licencia médica electrónica; sin embargo, la aplicación práctica de estas normas requiere de una reflexión desde la óptica de los principios del tratamiento de datos personales, que es lo que realizaremos en estas páginas.

II. El problema del tratamiento abusivo de los datos de salud

Los medios de comunicación han difundido una serie de hechos noticiosos que levantan alarma respecto de las condiciones de legitimidad con que se están desarrollando las operaciones de tratamiento de datos personales por parte de los operadores del sistema de salud, entendiendo por tales los establecimientos de salud, las farmacias y en general expendios de medicamentos, las instituciones de salud previsional, los laboratorios farmacéuticos, los laboratorios de análisis clínico, por mencionar los más representativos.

Un caso emblemático fue conocido gracias a que la afectada es una abogada, quien advirtió que una farmacia podía acceder a través del computador

(2) Este DFL, fija el texto refundido, sistematizado y concordado del decreto Ley 2.763, de 1979 y de las leyes N° 18.933 y N° 18.469, de acuerdo al mandato del artículo 4 transitorio de la Ley 20.015.

(3) En su artículo 4 dispone que serán atribuciones del Ministerio: "5.- Tratar datos con fines estadísticos y mantener registros o bancos de datos respecto de las materias de su competencia. Tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud. Para los efectos previstos en este número, podrá requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria. Todo ello conforme a las normas de la Ley 19.628 y sobre secreto profesional."

(4) El artículo 50 del DFL 1 dispone que serán funciones del Fondo: "f) Tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud. Para los efectos previstos en este número, podrá requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuera necesaria. Todo ello conforme a las normas de la Ley 19.628".

a la información sobre las patologías AUGE que padecía. Si bien este hecho copó las pantallas e involucró un pronunciamiento de la autoridad sanitaria, hay otras situaciones menos evidentes como el intercambio de datos entre las instituciones financieras y las compañías de seguro, respecto de los datos de salud que la persona declara o a la que tienen acceso con ocasión de los préstamos de largo plazo que requieren seguro de desgravamen, las que no por ello son menos graves.

Otro ejemplo se da en el ámbito laboral, en el que los empleadores acceden a la información sobre el estado de salud de una persona. Aun cuando las normas legales se han encargado de limitarles el acceso al diagnóstico, al menos hacen tratamiento de datos respecto de la condición de enfermo o sano de una persona, a través de los registros de asistencia al trabajo. Lo mismo sucede con los establecimientos de educación en relación con sus estudiantes.

Por ser muy variadas las hipótesis en que los datos personales de salud pueden ser objeto de tráfico en el mercado de los datos, en este artículo trataremos acerca de los lineamientos y principios que rigen y/o deben regir en materia de tratamiento de datos personales relativos a la salud.

Por ser muy variadas las hipótesis en que los datos personales de salud pueden ser objeto de tráfico en el mercado de los datos, en este artículo trataremos acerca de los lineamientos y principios que rigen y/o deben regir en materia de tratamiento de datos personales relativos a la salud, con sus principales consecuencias en el ámbito de procesos de tratamiento de datos. Esperamos con ello contribuir a los operadores y a quienes deben elaborar políticas públicas y/o elaboración normativa.

III. Concepto de datos de salud

Los datos personales han sido definidos en Chile en el artículo 2 letra f) de la Ley 19.628 de 1999[5] a partir de los siguientes elementos, los cuales procuraremos adaptar al tema que nos ocupa:

a. **Toda información:** Se trata de un concepto amplio, que abarca imágenes, sonidos o muestras físicas que proporcionen antecedentes de una

(5) "*Los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*".

persona. En el ámbito de la salud, la información puede referirse a resultados de exámenes, imágenes radiográficas, información genética y/o de identidad soportada en muestras médicas, etcétera. Registro de citas médicas, remedios prescritos, diagnósticos médicos, información de licencias, registros de ausencia por enfermedad en el ámbito laboral o estudiantil, entre otros.

b. **Sobre una persona natural:** Por tratarse de un atributo de la personalidad, derivado directamente de la dignidad humana, sólo la persona física es sujeto de protección de datos personales, excluyéndose en Chile a las personas jurídicas.(6) Tratándose de los datos de salud la información no sólo afecta a la persona sujeto de tratamiento o diagnóstico sino que también a su grupo familiar, con el cual comparte su patrimonio genómico. Asimismo, puede involucrar a un tercero que aún no es reconocido por el derecho como sujeto de derechos, es decir, la vida embrionaria. Incluso puede afectar a los donantes de órganos que pudieren haber sido implantados en un sujeto.

c. **Identificada o identificable:** Será dato personal aquel susceptible de ser vinculado a una persona determinada o determinable a través de procedimientos de identificación (los que pueden revestir diversos grados de complejidad). En el caso de los datos que revelan información de salud, sólo hablaremos de datos personales cuando esa información sea atribuible a una persona y no serán datos personales si han sido absoluta e irreversiblemente disociados.(7)

IV. Naturaleza jurídica de los datos de salud

En cuanto a la naturaleza jurídica específica de los datos de salud, la Ley 19.628 los considera en el artículo 2, letra g), en tanto define datos sensibles como "aquellos datos personales que se refieren a las características físicas

(6) Aun cuando en algunos proyectos de ley que se han presentado en el Parlamento se abre la posibilidad a que los datos de personas jurídicas, lo cual estimamos va contra la naturaleza de la normativa de protección de datos personales. Este es el caso de los boletines: 2422-07, de 1999, desde esa fecha en primer trámite constitucional, 2477-07, de 2000, archivado, entre otros.

(7) De acuerdo a la Ley 19.628, el procedimiento de disociación de datos consiste en "todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o indeterminada" (art. 2 letra l).

o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

Siendo así, nos surge la duda respecto de si aquella información relativa a la salud, pero que no es susceptible de ser calificada como *estados de salud físicos o psíquicos*, ¿debe ser considerada dato sensible o queda sujeta al régimen general de tratamiento de los datos personales que no son de este carácter? De nuestra parte, entendemos que la enumeración de datos sensibles no es taxativa y, por tanto, esta información podría ser calificada como tal por el juez, en la medida que se cumplan las condiciones tenidas en vistas por el legislador, esto es, que su tratamiento pueda afectar garantías fundamentales y traer aparejadas decisiones arbitrarias respecto de la persona.

(...) surge la duda respecto de aquella información relativa a la salud pero que no es susceptible de ser calificada como estados de salud físicos o psíquicos, ¿debe ser considerada dato sensible o queda sujeta al régimen general de tratamiento de los datos personales que no son de este carácter?

Así por ejemplo, la información sobre el ADN, que no revela estados de salud sino predisposiciones de una persona a ciertas afecciones, podrá ser calificada como sensible por parte de la jurisprudencia, no obstante, no responder exactamente al calificativo "estado de salud" al que alude la norma que comentamos, salvándose por esta vía las zonas no cubiertas por el texto legal.

Si bien la ley vigente permite entonces salvar estas situaciones, consideramos que no es adecuado que la calificación de los datos de salud como datos sensibles quede sujeta a los avatares de las decisiones jurisprudenciales. Creemos que lo más adecuado es corregir la norma con el fin de calificar en general esta información como sensible, dando aplicación del principio de precaución que rige en materia de derechos fundamentales.

De hecho, si analizamos el texto legal de la Ley 19.628, nos queda claro que los datos contenidos en una receta médica, en un examen médico y en la ficha médica son claramente datos sensibles, y por esto la ley modifica el artículo 127 del Código Sanitario. Lo mismo sucederá con las solicitudes de reserva de horas y licencias médicas emitidas respecto de cada persona. Estas evidencias son las que nos llevan a pensar que estamos frente a un caso de oscuridad legal, que debe ser enmendado por la vía de una modificación a la Ley 19.628.

Ahora bien, respecto de los datos relativos al "plan de salud", entendemos que cuando el legislador dispone que "la Institución de Salud Previsional deberá mantener la información recibida en reserva, de acuerdo a lo dispuesto en la ley Nº19.628" (art.33), alude a lo dispuesto en el artículo 7 de la ley, cuando regula el deber de secreto. De su parte, debe ser considerada dato sensible la información sobre enfermedades preexistentes, entregada por el afiliado en el contrato de salud. Lo mismo sucede con la información sobre los planes y seguros de salud que ha contratado y/o mantiene una persona, ya sea como suscriptor o beneficiario y las prestaciones a que éste tenga derecho con ocasión de dichos contratos, tal y como se establece en la Ley 18.933.

Como se adelantó en la introducción, otro aspecto importante en esta materia dice relación con el tratamiento de datos de la información contenida en muestras biológicas obtenidas a partir del diagnóstico médico o de la donación de tejidos, por mencionar algunas hipótesis. Al respecto, rige la Ley 20.120, sobre investigación científica en seres humanos, su genoma, y prohíbe la clonación humana de 22 de septiembre de 2006 y su normativa complementaria, además de los múltiples decretos que rigen la actividad de los profesionales de la salud en general y de los laboratorios en particular. Al respecto, y contemplando además la normativa internacional que rige esta materia, debemos considerar que no sólo la información de obtenida a partir de la muestra es sensible, sino que además debe aplicarse el tratamiento de "dato sensible" a la muestra biológica en que esta información se soporta. (8)

(...) debemos considerar que no sólo la información de obtenida a partir de la muestra es sensible, sino que además debe aplicarse el tratamiento de "dato sensible" a la muestra biológica en que esta información se soporta.

V. Condiciones de legitimidad del tratamiento de datos de salud

Continuando con nuestro análisis, aquellos datos personales de salud que son calificados como datos sensibles quedan sujetos a las normas previstas en el artículo 10 de esta ley, el cual dispone que: "No pueden ser objeto de tratamiento

(8) Uno de los temas más apasionantes en el área de tratamiento de datos personales en el ámbito de la investigación científica dice relación con las posibilidades de disociación de los datos personales respecto de la demás información proveniente de las muestras humanas.

los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

De esta manera corresponderá en cada caso buscar la autorización legal, o contar con el consentimiento (informado) del titular de los datos personales, o bien acreditar que las mismas son necesarias para la determinación u otorgamiento de beneficios de salud que les corresponden a estas personas. Por ejemplo, serían finalidades legítimas aquellas que dicen relación con la posibilidad del individuo de acceder a los medicamentos prescritos por un médico tratante, o los contenidos en los resultados de exámenes que permitirán diagnosticar y los que se refieran a la historia clínica del paciente cuando sea necesario para los efectos de aplicar procedimientos destinados al restablecimiento de su salud. Ello además del tratamiento de datos necesario para el otorgamiento de prestaciones pecuniarias, asociadas, por ejemplo, a los planes de salud de la persona.

(...) corresponderá en cada caso buscar la autorización legal, o contar con el consentimiento (informado) del titular de los datos personales, o bien, acreditar que las mismas son necesarias para la determinación u otorgamiento de beneficios de salud (...)

De nuestra parte, estimamos que la frase "beneficios de salud que correspondan a sus titulares", además de las prestaciones pecuniarias, comprende los beneficios propios del sistema de salud, asociados a la concreción de la garantía fundamental consagrada en el artículo 19 N° 9 de la Constitución Política de la República, en tanto garantiza a todas las personas el derecho a la protección de la salud, en los siguientes términos:

"El Estado protege el libre e igualitario acceso a las acciones de promoción, protección y recuperación de la salud y de rehabilitación del individuo.

Le corresponderá, asimismo, la coordinación y control de las acciones relacionadas con la salud.

Es deber preferente del Estado garantizar la ejecución de las acciones de salud, sea que se presten a través de instituciones públicas o privadas, en la forma y condiciones que determine la ley, la que podrá establecer cotizaciones obligatorias.

Cada persona tendrá el derecho a elegir el sistema de salud al que desee acogerse, sea éste estatal o privado".

Siendo así, habremos de analizar de qué manera se aplican los principios de la Ley 19.628 al tratamiento de datos de salud. A estos efectos, hemos considerado que los aspectos más relevantes a considerar son los siguientes:

a. Calidad de los datos personales y calidad del tratamiento de datos

i. Sujeción a la finalidad del tratamiento de datos personales: La información relativa a la salud no puede ser considerada como proveniente de una fuente accesible al público. Siendo así, los datos personales deben utilizarse sólo para los fines a partir de los cuales fueron recolectados, los que en todo caso deben estar asociados a la salud, entendida como acciones de promoción, protección y recuperación de ésta por parte de las personas.

ii. Veracidad de la información (artículos 6, incisos 2, 3 y 4 y 9 de la Ley 19.628): La información relativa a la salud, contenida en las bases de datos de los prestadores y terceros que tienen injerencia en el sector debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos. Asimismo, los datos deben ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

La información relativa a la salud, contenida en las bases de datos de los prestadores y terceros que tienen injerencia en el sector debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

En tercer lugar se deben bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales debe proceder a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

Es así como debiera eliminarse la información sobre diagnósticos erróneos que han sido modificados por diagnósticos posteriores. Asimismo, debiera impedirse la elaboración de datos apreciativos a partir de los contenidos en los sistemas de salud. Este es el caso de los sistemas que elaboran pronósticos de infertilidad a partir de, por ejemplo, información sobre abortos espontáneos. Lo mismo ocurre con los sistemas de alerta de automedicación cuando una persona compra un remedio sin receta,

los que actúan sin cuestionarse si ésta los compra para sí o para un tercero. Estas situaciones, por sólo mencionar algunas, son fuente de abuso permanente por parte de los actores del mercado de datos personales.

iii. Deber de custodia de los datos personales (artículo 11 de la Ley 19.628): La autorización de los organismos ligados a la salud, tanto a nivel de prestaciones como los administradores, de efectuar operaciones de tratamiento de datos personales para los efectos de dar cumplimiento a la finalidad específica de protección y administración de la salud de los titulares de estos datos. Adicionalmente, hay finalidades que autorizan el tratamiento de datos personales que dicen relación con las necesidades públicas asociadas al deber de garantizar la salud pública, además de aquellas derivadas del cumplimiento de las normas de control de ciertas substancias calificadas especialmente por el regulador y demás finalidades previstas en el ordenamiento jurídico.

(...) hay finalidades que autorizan el tratamiento de datos personales que dicen relación con las necesidades públicas asociadas al deber de garantizar la salud pública, además de aquellas derivadas del cumplimiento de las normas de control de ciertas substancias calificadas especialmente por el regulador y demás finalidades previstas en el ordenamiento jurídico.

Esto ocurre con las recetas médicas, las cuales son una fuente importante de datos personales a las que luego se refiere la norma. Los tipos de receta médica reguladas en los decretos supremos 404 y 405, de 2 de noviembre de 1983, del Ministerio de Salud, se distinguen entre: a) **Receta magistral**: "Aquella en que un profesional legalmente habilitado para ello prescribe una fórmula especial para un enfermo determinado, la que debe elaborarse en el momento de su presentación"; b) **Receta Médica Retenida**: "Aquella en la que se prescriba productos sujetos a esta condición de venta, y ella deberá archivarse en el establecimiento, conforme a lo dispuesto en el artículo 21° del presente reglamento". Cuando se trate de la prescripción de estupefacientes y productos psicotrópicos cuya condición de venta es receta retenida ésta deberá ser impresa con los datos que señalan los respectivos reglamentos; c) **Receta Cheque:** "Los formularios oficiales que formen parte de talonarios que los Servicios de Salud proporcionan a los médicos cirujanos y a las farmacias para la prescripción de estupefacientes y productos psicotrópicos".

Es de público conocimiento que las recetas médicas han sido una fuente de abusos en materia de tratamiento de datos personales, por lo que no ahondaremos en ese tema sino que llamaremos la atención respecto de la necesidad de que los actores sociales que entran en contacto con estos documentos resguarden el debido secreto y/o reserva de la información que en ellas se refleja tanto respecto de los datos que conciernen al médico tratante como a los pacientes. Evidentemente esto es sin perjuicio de la obligación de informar y remitir a la autoridad en el caso de las recetas retenidas y recetas cheque.

Es de público conocimiento que las recetas médicas han sido una fuente de abusos en materia de tratamiento de datos personales (...)

En el marco de este deber se deben establecer sistemas de control de sesión y gestión de operaciones y comunicaciones. Esto queda claro tratándose de los organismos públicos, conforme lo establecido en el art. 31, art. 32 dto. 83 del Ministerio Secretaría General de la Presidencia, de 2004, y en el capítulo 8 Norma Chilena 2777 de seguridad informática.

iv. Seguridad en el tratamiento de datos personales (artículo 5 Ley 19.628):

Los requerimientos de seguridad en el ámbito sanitario son muy elevados y precisan una infraestructura de manejo de privilegios para la gestión de roles, además de una infraestructura de clave pública que permita una política de reconocimiento transfronteriza, a la vez de garantizar la confidencialidad de la información.

En nuestra opinión, los sistemas de apoyo a la gestión del sector de la salud en Chile deben implementarse medidas de seguridad del más alto nivel, en lo que respecta al resguardo de los datos personales, sobre todo en lo que se refiere a la transferencia electrónica de datos. Esto impacta, por ejemplo, en la necesidad de resguardar la privacidad del paciente a través de sistemas de acceso personalizado a los datos personales, sin que sean adecuados aquellos sistemas en los cuales los miembros de un grupo familiar pueden revisar recíprocamente la información de salud que consta en dichos sistemas.

Asimismo, tratándose de información crítica para las acciones de salud, tales como reacciones alérgicas a ciertos principios activos o afecciones

crónicas que puedan sufrir las personas, los sistemas de tratamiento de datos personales relativos a la salud deben tener medidas de aseguramiento de continuidad del servicio, que en el caso de los organismos públicos han sido establecidas en los artículos 35 y 37 dto. 83 antes citado y en el capítulo 11 Norma Chilena 2777.

(...) tratándose de información crítica para las acciones de salud, tales como reacciones alérgicas a ciertos principios activos o afecciones crónicas que puedan sufrir las personas, los sistemas de tratamiento de datos personales relativos a la salud deben tener medidas de aseguramiento de continuidad del servicio (...)

Además, en materia de seguridad, respecto de los organismos públicos ligados a la salud, debe darse cumplimiento a lo dispuesto en el decreto 77, de 2004, del Ministerio de Economía, relativo a la eficiencia de las comunicaciones electrónicas entre órganos de la administración del Estado y entre éstos y los ciudadanos. Estas normas son relevantes para el caso de los datos personales que constan en los servicios públicos, pero también en las entidades privadas, en tanto que pueden ser requeridos, por ejemplo, para atenciones de urgencia en centros públicos. Este Decreto contiene las siguientes exigencias: art. 3 dto. 77: a) Autenticación; b) Disponibilidad y acceso para uso posterior, en los términos del art. 6, debiendo conservar los registros por un período que no podrá ser inferior a 6 años; c) Compatibilidad técnica de los sistemas, que permita la visualización correcta de los documentos; d) Medidas de seguridad que impidan la intercepción, alteración, obtención y otras formas no autorizadas de acceso a las comunicaciones electrónicas. A dichos efectos, este mismo decreto determina las siguientes medidas de seguridad:

i. El registro deberá ser cerrado diariamente por medio de un mecanismo manual o automatizado que garantice el no repudio e integridad, bajo la responsabilidad del encargado del repositorio.

ii. El Ministro de Fe del respectivo servicio deberá concurrir con su firma electrónica avanzada al menos una vez al mes al cierre de todos los registros diarios acumulados documentalmente durante el período comprendido entre el último cierre y el que se realiza.

iii. Publicidad de las direcciones electrónicas en las cuales pueden hacerse las consultas y solicitar comunicaciones.

v. Temporalidad del tratamiento de datos personales (artículos 2 letra d) y 6 inciso 1 Ley 19.628): En el caso de los datos de salud, entendemos que si bien la ficha médica es de autoría del médico tratante, la información es de titularidad del "paciente". Siendo así, la persona debiera controlar la información de salud que le concierne, de hecho esta es una de las medidas que se han adoptado en otros países, en los cuales la persona es la que porta un dispositivo o controla los mecanismos de acceso al sistema en el cual se almacenan sus datos de salud, otorgando accesos temporales a los facultativos que le asisten. Es el caso de las llamadas LaserCards® que en tarjetas de aspecto similar a las tarjetas bancarias, almacenan altos volúmenes de información con altos niveles de seguridad.

En el caso de los datos de salud, entendemos que si bien la ficha médica es de autoría del médico tratante, la información es de titularidad del "paciente". Siendo así, la persona debiera controlar la información de salud que le concierne (...)

De su parte, las instituciones de salud previsional debieran tener esta información durante la época en que la persona está afiliada y/o mientras sea necesario para el otorgamiento de los beneficios de salud que emanan del contrato.

En tercer lugar, tratándose del Ministerio de Salud y sus organismos dependientes, deberían mantener esta información mientras se necesite para la realización de las actividades que emanan de sus respectivas competencias.

vi. Deber de secreto /reserva de los datos personales (artículo 7, Ley 19.628 y 127 incisos 2 y 3 del Código Sanitario): Cuando la ley dispone que las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos cuando hayan sido recolectados de fuentes no accesibles al público (que es el caso que nos ocupa), la obligación no sólo alcanza a los datos personales sino que también a los demás antecedentes relativos al banco de datos, actividad que no cesa por dejar de trabajar en ese ámbito.

Ello sin perjuicio de las condiciones especiales previstas en el artículo 127 del Código Sanitario, modificado por la misma Ley 19.628, del siguiente tenor: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".

En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.

Conforme esta norma estimamos que las recetas médicas deben considerarse como reservadas, por cuanto la mención *"servicios relacionados con la salud"* es suficientemente genérica para estimarlo así. Esto más aún si consideramos que las recetas médicas han sido objeto de malos usos por parte de las empresas del sector, conforme se ha revelado en diversas denuncias y estudios.

b. Control del tratamiento de datos personales por parte del titular de los datos

i. Consentimiento del afectado y en su caso deber de información (artículos 10 y 20 Ley 19.628): Tratándose de los datos de salud, para su tratamiento las instituciones privadas requieren del consentimiento del afectado y/o de sus representantes legales, tratándose de menores, incapaces o personas incapacitadas temporalmente.

En este punto surge una duda razonable respecto de los adolescentes, y/o jóvenes adultos que son carga familiar de sus padres, en cuanto si

deben consentir ellos respecto del tratamiento de sus datos personales y si se debe dar acceso a los mismos a sus padres. Al respecto, si bien los padres tienen la patria potestad, la convención de los niños y adolescentes protege la privacidad de éstos.

Así por ejemplo, si un menor adulto consulta a un médico respecto de sistemas anticonceptivos o de contracepción, debiera ser consultado respecto de si desea que sus padres puedan acceder a esta información y en la negativa no debiera permitirse el acceso a estos datos personales, en la medida que la salud de los menores no se encuentre en riesgo.

(...) si un menor adulto consulta a un médico respecto de sistemas anticonceptivos o de contracepción, debiera ser consultado respecto de si desea que sus padres puedan acceder a esta información y en la negativa no debiera permitirse el acceso a estos datos personales, en la medida que la salud de los menores no se encuentre en riesgo.

De su parte, los organismos públicos no requieren este consentimiento cuando realicen actividades de tratamiento de datos que queden comprendidas dentro de la órbita de su competencia. Es el caso, por ejemplo, del Fondo Nacional de Salud, con los datos de sus afiliados y beneficiarios, de la Superintendencia de Salud, respecto de los datos a que accede con ocasión de la fiscalización de las empresas del sector, de la Superintendencia de Seguridad Social, en el caso de las licencias médicas, etcétera.

Lo que queda claro es que no es posible a estos organismos tratar datos más allá de sus competencias, pues éstas determinan y modelan la finalidad del tratamiento de datos personales.

ii. **Protección a los derechos del afectado por el tratamiento de datos personales (Artículos 12 y 16 Ley 19.628):** Los prestadores de salud y sectores asociados, que realicen tratamiento de datos de esta naturaleza deben cumplir con los llamados derechos ARCO, esto es, acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Entendemos que los derechos de acceso y rectificación podrán exigirse en todo caso. Sin embargo, los derechos de oposición y cancelación requieren un análisis en cada caso concreto, a los efectos de determinar si se configura alguna de las causales de excepción legal, ya sea que estos derechos afecten las facultades fiscalizadoras del Estado, el interés de la nación o la seguridad nacional.

Estas excepciones se vislumbran claramente respecto de los organismos públicos ligados a la salud, pero también pueden decir relación con los tratamientos de datos en caso de enfermedades consideradas infecto contagiosas, que podrían derivar por ejemplo en una pandemia.

Ahora bien, queda claro que esta es otra fuente de abusos de las empresas del sector, en el sentido de que no se establecen los mecanismos ni facilidades adecuadas para que la persona vea satisfechos estos derechos.

Además de lo anterior cobra relevancia lo dispuesto en el artículo 11 de la Ley 19.628, en cuanto dispone que el responsable del registro o banco de datos donde se almacenen los datos personales con posterioridad a su recolección debe cuidar de ellos con la debida diligencia, haciéndose responsable por los daños. De esto deriva que además de los derechos del titular de datos personales, contemplados en la Ley 19.628 y la normativa sectorial, tendrá derecho a accionar por los daños producidos por el tratamiento de datos personales con infracción a los principios y normas analizados.

VI. Conclusiones: Principales desafíos del tratamiento de datos personales adecuado en el área de la salud

Los problemas que se han vivido en Chile en materia de tratamiento de datos personales de salud son simplemente un reflejo de la situación nacional en esta materia. Es así como la falta de regulación adecuada, sumada a la incapacidad del mercado de autorregularse, ha llevado a que en definitiva exista un tráfico de datos personales de salud que está afectando a sus titulares por distintas vías.

Entendemos que los principales problemas en esta materia dicen relación con los siguientes aspectos:

(...) la falta de regulación adecuada, sumada a la incapacidad del mercado de autorregularse, ha llevado a que en definitiva exista un tráfico de datos personales de salud que está afectando a sus titulares por distintas vías.

a. Falta de seguridad en el tratamiento de datos personales

Las fugas de datos personales que se han advertido en el medio nacional no dicen relación necesariamente con la falta de regulación sino con la inexistencia de mecanismos eficientes de control a los agentes del mercado.

Esta es una manifestación de la inexistencia de una Agencia de Protección de Datos Personales, que vele por el tratamiento adecuado de datos personales en nuestro entorno.

Asimismo, es un síntoma de la falta de preocupación de las mismas personas, quienes prefieren adherir a los sistemas de descuentos o de fidelización por la vía de tarjetas de puntos que existen en el mercado en vez de proteger su información personal. Esto puede deberse a su ignorancia respecto de los efectos que tiene la entrega de los datos a estos agentes.

(...) es un síntoma de la falta de preocupación de las mismas personas, quienes prefieren adherir a los sistemas de descuentos o de fidelización por la vía de tarjetas de puntos que existen en el mercado en vez de proteger su información personal. Esto puede deberse a su ignorancia respecto de los efectos que tiene la entrega de los datos a estos agentes.

A ello se suma el desarrollo de sistemas de salud en línea por prácticamente todas las clínicas privadas. En concreto, la Clínica Alemana de Santiago, en abril de 2009, anunció la creación del servicio en línea "Mi página de salud", que permite consultar a los pacientes, mediante el número de RUT y una clave secreta, la información médica y administrativa desde el año 2005. Se señala además que gracias a este servicio los padres podrán acceder a la información de sus hijos, sin necesidad de recordar el RUT ni conocer la clave de ellos. El sistema tampoco excluye la información sobre el otro cónyuge que también es mayor de edad.

Estimamos que por razones de seguridad, estos sistemas debieran considerar la posibilidad de que todos los sujetos, en la medida que sean mayores de edad, sólo puedan visualizar la información que les concierne, sin que sea posible que terceros (aunque se trate de familiares) los revisen.

b. Requisitos de autenticidad

A los efectos de garantizar la autenticidad de las personas que acceden a los sistemas de tratamiento de datos de salud parece razonable que se implementen sistemas de firma electrónica que sean capaces de satisfacer los siguientes requisitos, que debieran ser solventados por la autoridad de salud correspondiente:

a) Enrolamiento previo de los profesionales de la salud habilitados para la operación de los sistemas de salud que contengan datos personales de salud, tales como la ficha médica, las recetas médicas, licencias médicas, exámenes de salud, etcétera, con definición de atributos y sistemas de firma electrónica que se active a través de mecanismos que el médico mantenga bajo su exclusivo control.

   a. Verificación fehaciente de la identidad del médico que prescribe los medicamentos y emite la receta.

   b. Verificación de la titulación que le habilita para prescribir medicamentos y/o intervenir en procedimientos de salud.

   c. Generación de certificado de firma electrónica con atributos tales como tipos de medicamentos que la titulación respectiva habilita para prescribir al correspondiente facultativo.

   b) Para los efectos de la extracción y/o agregación de datos al sistema deben establecerse mecanismos de establecimiento de sesiones que permitan vincular la información que se ingresa, consulta y/o extrae del sistema. El sistema debiera ser capaz de detectar todas las operaciones que se realicen sobre los datos personales, mas no debiera eliminarse la información que se genera en cada una de las sesiones, para los efectos de garantizar su trazabilidad, en el sentido que veremos en el punto siguiente.

El sistema debiera ser capaz de detectar todas las operaciones que se realicen sobre los datos personales.

c. Requisitos de registro y trazabilidad

Los documentos de salud debieran tener un código único, con sistemas de marcado que permitan conocer su estado en cada momento. Las transferencias electrónicas de información deben quedar registradas a los efectos de que exista la posibilidad cierta de trazar los datos personales que han sido objeto de consulta por terceros.

d. Perfeccionamiento de la legislación vigente

La regulación del tratamiento de datos de salud debiera referirse a este tipo de datos en términos generales, no así a los datos relativos a los "estados de salud". Ello permitiría dar mayor certeza jurídica a los agentes del mercado de datos personales, los prestadores de salud, la autoridad y los titulares de datos personales de esta naturaleza.

A estos efectos debiera modificarse la Ley 19.628, en el catálogo de datos sensibles y asimismo agregar las normas pertinentes en el código sanitario.

Adicionalmente, la Superintendencia de Salud al tener las competencias para los efectos de resolver reclamos por tratamiento inadecuado de los datos personales e incluso sancionar a los agentes del mercado por infracciones en esta materia, tal y como se evidenció en abril de 2010, frente al reclamo de la abogada Verónica Sánchez, debiera dictar un reglamento de tratamiento de datos personales por parte de los organismos de salud, que entregue los lineamientos básicos en esta materia.

Autora

Lorena Donoso Abarca

Licenciada en Ciencias Jurídicas y Sociales, Universidad de Chile; Magíster en Informática y Derecho, Universidad Complutense de Madrid. Profesora Asistente del Departamento de Derecho Procesal de la Universidad de Chile.

VII
Información sobre venta de medicamentos: ¿Datos sensibles?*

Vanessa Facuse Andreucci

* Las opiniones vertidas en este documento reflejan única y exclusivamente el parecer de su autora, y en ningún caso representan a la entidad donde ésta trabaja.

I. Introducción

Frecuentemente cuando acudimos a la farmacia a comprar medicamentos nos solicitan nuestro número de RUT —previo registro de nuestros datos personales e incluso, muchas veces, sin necesidad de hacer el ingreso porque ya están registrados—, ello a cambio de beneficios que se vinculan a descuentos o canjes exigibles en compras futuras. Esta práctica, sin que tengamos mucha conciencia, va construyendo un catastro de consumo de medicamentos de cada persona, pudiendo abarcar hasta su grupo familiar, sin que nos detengamos a cuestionarnos el tipo de información que estamos entregando, quién y cómo trata esa información, ni menos la exactitud de la misma.

Aunque tal práctica es realizada diariamente en nuestras acciones de consumo en supermercados, casas comerciales, contratación de servicios, entre otros, y es utilizada para definir las preferencias o perfiles de clientes; nos parece necesario destacar que al comprar medicamentos entregamos información de la mayor relevancia, por cuanto son "datos asociados a nuestro estado de salud". Así, el dato de compra de medicamentos debe ser considerado un dato "personal" —porque es información atribuible a una persona determinada o determinable— y "sensible" —al reflejar el estado de salud físico o psíquico de una persona—.

Así, el dato de compra de medicamentos debe ser considerado un dato "personal" —porque es información atribuible a una persona determinada o determinable— y "sensible" —al reflejar el estado de salud físico o psíquico de una persona—.

Atendido que los registros de las transacciones de venta de medicamentos por las farmacias son datos sensibles, su estándar de tratamiento, a nuestro juicio, requiere un nivel mayor de protección que permita, por un lado, asegurar que dicha información corresponderá a la situación real de las personas (calidad del dato) y, por el otro, garantizar que será tratada con la autorización expresa de su titular o en los casos permitidos por la ley, pues su uso indebido puede afectar garantías fundamentales.

Sin duda que para el funcionamiento del mercado farmacéutico es muy relevante la interacción entre los actores de los tres niveles del mercado —producción, distribución y venta—, siendo necesario el manejo de la información comercial de la venta de medicamentos. No obstante, desde la

óptica del tratamiento de los datos personales este trabajo se centrará sólo en el último nivel de la cadena, es decir, en la venta de medicamentos a público.

II. ¿Qué tipo de información emanada de la venta de medicamentos puede tratarse?

De acuerdo a lo dispuesto en el Código Sanitario la comercialización de los medicamentos para uso humano "*sólo podrá hacerse en las farmacias"*.[(1)/(2)] Es preciso consignar aquí que dicha norma también define qué debemos entender por *medicamento o fármaco*, al señalar que: "Se entenderá por producto farmacéutico cualquiera substancia, natural o sintética, o mezcla de ellas, que se destine a la administración al hombre o a los animales *con fines de curación, atenuación, tratamiento, prevención o diagnóstico de las enfermedades o de sus síntomas*".[(3)]

En cuanto a su clasificación, los medicamentos pueden ubicarse en varias categorías, sin embargo, nos concentraremos sólo en dos. Primero, tenemos las categorías farmacéuticas de acuerdo al *"uso terapéutico de los mismos"*. Para ello existe una metodología a nivel mundial utilizada por las consultoras especializadas en el área de la salud para la elaboración de estadísticas en la industria farmacéutica, que es la clasificación de los medicamentos EPhMRA (European Pharmaceutical Marketing and Research Association).[(4)] Dicha nomenclatura es conocida bajo el nombre de "anatómica" (ATC, anatomical therapeutical class)[(5)]/[(6)], y se refiere a la aplicación terapéutica de los medicamentos, que dice relación con el "uso principal" para el cual se emplean. Así, cada medicamento sólo puede estar en una categoría, de modo que cuando una persona lo compre exista consenso a nivel mundial respecto al tratamiento de qué patología éste se encuentra asociado.

(1) Artículo 123 del Código Sanitario que regula los aspectos relacionados con fomento, protección y recuperación de la salud de los habitantes.

(2) Se hace presente que se encuentra en tramitación en el Congreso un proyecto de ley que propone que los medicamentos de venta libre se puedan también ofrecer en supermercados.

(3) Artículo 97 del Código Sanitario. Las cursivas son nuestras.

(4) Asociación europea de marketing farmacéutico, integrada por los principales laboratorios a nivel mundial.

(5) La clasificación ATC se encuentra administrada actualmente por la WHO (World Health Organization), Collaboration Centre for Drugs Statistics Methology de las Naciones Unidas- http://www.whocc.no

(6) Una completa explicación del funcionamiento del sistema de clasificación ATC se encuentra en: http://medtrad.org/panacea/IndiceGeneral/n15_tribuna-Saladrigas.pdf.

De esta forma, el dato de compra de medicamentos se relaciona con su uso terapéutico, proporcionando información sobre el estado de salud físico (antihipertensivos, antialérgicos) o psicológico de una persona (consumo de sicotrópicos, antidepresivos, entre otros).

(...) el dato de compra de medicamentos se relaciona con su uso terapéutico, proporcionando información sobre el estado de salud físico (antihipertensivos, antialérgico, anhipertensivos) o psicológico de una persona (consumo de sicotrópicos, antidepresivos, entre otros).

Una segunda clasificación está dada por la "condición de venta" de los fármacos, distinguiendo entre *medicamentos Éticos* (Rx) —aquellos que requieren receta para su dispensación— y de *Venta Libre* (OTC).[7] A su vez, dentro de los medicamentos éticos, distinguimos los de receta simple, receta retenida, receta cheque —administración de psicotrópicos—, etcétera.

La categorización anterior es útil para dejar asentado que existe una asimetría regulatoria en el Código Sanitario en lo que se refiere a la protección de los datos personales que emanan de la comercialización de medicamentos, otorgando una mayor protección a los éticos (Rx). Así, el artículo 127 del referido Código, modificado por la misma Ley 19.628 sobre Protección de Datos Personales, dispuso que: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo". Para concluir que: "En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".

Así dicha disposición prohíbe la divulgación tanto del contenido de la receta médica como de los datos que se vinculen a la venta del medicamento (como el paciente y médico tratante), salvo consentimiento *expreso* del paciente, lo que se condice con el artículo 10 de la Ley 19.628, exigiendo, además, que el consentimiento sea otorgado "por escrito". Reiteramos, el alcance de la

(7) Decreto N° 466 de 1984, del Ministerio de Salud, Reglamento de farmacias, droguerías, almacenes farmacéuticos, botiquines y depósitos autorizados.

referida protección está asociado exclusivamente a la venta de medicamentos que se comercializan con receta médica.

La asimetría regulatoria —desfavorable a los medicamentos OTC— no tiene justificación a la luz de los principios sobre protección de datos personales, e incluso no se condice con el mismo texto de la Ley 19.628, que al establecer lo que debe entenderse por datos sensibles[8] considera los estados de salud físicos y psíquicos de las personas y, consecuentemente, en tal calidad establece un estándar de tratamiento más elevado.

La asimetría regulatoria —desfavorable a los medicamentos OTC—, no tiene justificación a la luz de los principios sobre protección de datos personales, e incluso no se condice con el mismo texto de la Ley 19.628, que al establecer lo que debe entenderse por datos sensibles considera los estados de salud (...)

Más aún, si consideramos que se encuentra en tramitación un proyecto de ley que justamente autoriza a vender medicamentos OTC a otras entidades distintas de las farmacias, por ejemplo, los supermercados,[9] y que éstos ya tratan datos de perfiles de consumo de sus clientes, ahora podrá agregar la información sobre el estado de salud físico y psíquico de sus clientes. Por lo anterior, debemos poner las alertas para tratar este tema en forma responsable, elaborando políticas públicas que protejan debidamente los derechos de personas, transparentando la finalidad con que se recogen esos datos.

En vista de lo ya expuesto, resulta urgente otorgar a los datos emanados de la venta de medicamentos, *cualquiera sea su condición de venta*, el régimen de regulación de los datos sensibles con su efectiva fiscalización, por cuanto ahora ya puede ser tarde para frenar su difusión y uso no autorizado.

Es preciso mencionar que la regulación sanitaria, en armonía con la Ley 19.628, establece "usos autorizados" del tratamiento de los datos farmacéuticos, sin requerir el consentimiento de su titular. Así el mismo artículo 127 referido, dispone que las farmacias puedan dar a conocer, para fines estadísticos,

(8) **Dato "sensible" se define** en el artículo 2°, la letra g) de la Ley 19.628, como "*aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas,* ***los estados de salud físicos o psíquicos*** *y la vida sexual*".

(9) Boletín Nº 2100-11.

las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. Otro ejemplo, consiste en que las farmacias deben registrar los datos asociados a la venta de estupefacientes, entre estos, el nombre, domicilio y cédula de identidad del paciente, los que se comunican al Instituto de Salud Pública.(10)

Otro caso de "uso autorizado" que contempla el artículo 10 de la Ley 19.628 ocurre cuando los datos son necesarios "*para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares*". Preciso es consignar que dicha excepción debe interpretarse restrictivamente, en cuanto sólo podrán utilizarse para la determinación y otorgamiento de "prestaciones del sistema de salud previsional" que estén a cargo de entes públicos o privados.(11)

En el mismo sentido ha recogido dicha autorización la Directiva 95/46/CE(12) en su sección 34 al disponer que *"se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas"*.(13)

(10) Decreto Supremo N° 404, de 1983, Reglamento de Control de Consumo de Estupefacientes.

(11) Consta en la discusión del proyecto de ley sobre Protección a la Vida Privada, que el Director del Fondo de Salud Nacional señaló frente a esto: "Así, por ejemplo, para un programa de Sida, es necesario trabajar con una serie de datos respecto de las personas, los cuales obviamente incluyen conductas sexuales, estados de salud y otros, o bien, para analizar un problema de salud mental, los datos requeridos obviamente se referirán a conductas de vida y severidad del caso. Es necesario trabajar también con alguno de los datos sensibles cuando se estructuran grupos de riesgo de la población en términos de prevalencia de enfermedades, tales como el sexo o la raza de las personas, lo cual es altamente relevante para la correcta determinación de los beneficios que se van a otorgar a cada grupo".

(12) Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

(13) Este principio en la legislación española se consagra en el artículo 77, apartado 8 de la Ley 29/2006, de Garantías y Uso Racional de los Medicamentos y productos Sanitarios, que dispone: "No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud".

Los actores del mercado farmacéutico podrían discutir si el otorgamiento de beneficios económicos asociados a descuentos o unidades gratis puede ser considerado como un beneficio de salud y, por tanto, no requeriría de autorización del cliente; a nuestro parecer dicha interpretación se aleja del espíritu de la norma y la protección a la vida privada, en aspectos de alta sensibilidad, como es su estado de salud, por lo que requeriría el consentimiento de su titular. Reiteramos que llegar a esa conclusión en ningún caso es caprichoso, sobre todo si consideramos que existe consenso a nivel mundial de que cada medicamento está asociado a un uso terapéutico para el tratamiento de determinadas patologías.

No obstante, existe información que es de público conocimiento[14] y que evidencia que los datos de venta de medicamentos, en particular los que constan en las recetas, sí son recolectados, aun existiendo regulación que lo prohíbe, sin conocimiento y menos consentimiento expreso y escrito del consumidor-paciente.

La posible solución a la problemática expuesta en ningún caso pretende el ocultamiento de los datos, prohibiendo la circulación de los mismos, sino más bien tendría que apuntar a establecer ciertos requisitos que permitan garantizar un tratamiento adecuado por los titulares de las bases de datos (...)

La posible solución a la problemática expuesta en ningún caso pretende el ocultamiento de los datos, prohibiendo la circulación de los mismos, sino más bien tendría que apuntar a establecer ciertos requisitos que permitan garantizar un tratamiento adecuado por los titulares de las bases de datos, para lo cual se requiere que el cliente conozca cuál es la finalidad del uso del dato, que sea información real y exacta, por tratarse de datos del estado de salud de las personas.

III. Recolección de datos de salud en la comercialización de medicamentos y sus riesgos

Considerando las principales referencias regulatorias en esta materia, no nos queremos quedar con el ejercicio meramente exegético del alcance y sentido de la normativa y la aplicación que debiera darse a la misma respecto a los datos de "salud" derivados de la venta de medicamentos, sino que más

(14) Por ejemplo, programa Contacto de Canal 13.

bien nos interesa poner las alertas de que efectivamente se están tratando datos sensibles, y que si no ponemos los límites y condiciones de su tratamiento puede ser demasiado tarde para identificar quiénes los tienen y con qué finalidad.

En los hechos, existen empresas cuyo negocio es la recolección de datos personales en la venta de los medicamentos éticos y OTC para luego venderlos, principalmente a los laboratorios. Éstas operan en el mercado sin el conocimiento de los consumidores-pacientes, quienes al entregar la receta para que el vendedor verifique que tiene el producto en stock, la entregan también para que ésta sea copiada.

Así, nos encontramos con una lucrativa práctica que se desarrolla, por una parte, al margen de la ley y de espaldas al titular de los datos personales, el consumidor-paciente. Aquí el desconocimiento de cuáles otras operaciones se realizan con la información recolectada es tan grave como lo advertido respecto a la recogida de los datos. Ello ya que por la forma en que está compuesto el mercado de la salud en Chile, es difícil imaginarse que la información termina su circulación ahí. No es necesario hacer mucha ficción como para pensar que dicha información de consumo de medicamentos pueda —o sea— cedida a otras entidades, como las Isapres, compañías de seguros u otros que pudieren estar interesados en tenerla y con ello terminar vulnerando un sinfín de derechos fundamentales de los titulares de datos, los consumidores-pacientes.

No es necesario hacer mucha ficción como para pensar que dicha información de consumo de medicamentos pueda —o sea— cedida a otras entidades, como las Isapres, compañías de seguros u otros que pudieren estar interesados en tenerla y con ello terminar vulnerando un sinfín de derechos fundamentales (...)

Estimamos que es imprescindible linkear esta problemática a la forma en que los datos personales son tratados efectivamente por quienes los comercializan, para lo cual centraremos el análisis de la *calidad de la recolección* de datos personales en el proceso de comercialización.

La *calidad de la información* es un pilar fundamental para el correcto tratamiento de los datos personales, conforme a los cuales sólo podrán ser tratados los datos adecuados, pertinentes y no excesivos.(15) Lo anterior, considerando que un gran número de clientes compra medicamentos para que

(15) Inciso segundo art. 9 Ley 19.628: "En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos".

otros los consuman —los padres a sus hijos, los cónyuges, hermanos, etcétera— produciéndose una disociación entre el titular de los datos de compra y el titular-destinatario de la prescripción.

¿Qué pasa entonces cuando se traspasa esa información a terceros? ¿A quién y para qué se traspasa? ¿Quién controla la calidad de los datos? Dichas interrogantes no son triviales si pensamos que las farmacias tienen convenios con diversas entidades para otorgar "beneficios" a los clientes, así puedo pagar con tarjetas de casas comerciales, supermercados o bancarias, isapres, compañías de seguros, incluso puedo acumular millas en una línea aérea, tener convenios con empresas a cambio de que sus trabajadores obtengan descuentos. Sin embargo, no hay que olvidar que esta información no son meros datos de consumo, sino que se refieren al estado de salud de las personas, y con ello se pueden limitar el acceso o restringir: créditos, la obtención de seguros, el derecho al trabajo, y la afectación de otros derechos fundamentales.

Si bien ninguna de las situaciones expuestas es negativa por sí sola, se propone que se impongan límites al tratamiento de dicha información, es decir, la autorización expresa de su titular, transparentando la finalidad para la cual van a ser recogidos, registrados, almacenados y transferidos dichos datos de compra de medicamentos.

(...) ninguna de las situaciones expuestas es negativa por sí sola, se propone que se impongan límites al tratamiento de dicha información, es decir, la autorización expresa de su titular, transparentando la finalidad para la cual van a ser recogidos, registrados, almacenados y transferidos dichos datos (...)

Así, si la información de compra de medicamentos es traspasada por las farmacias a los bancos, por ejemplo, que se haga sólo para efectos del cobro de la transacción comercial, y en ningún caso que el banco pueda limitar el acceso al crédito o aumente el riesgo de un individuo en base a la información que tiene de su estado de salud. Para ello es fundamental que las personas tengamos siempre la posibilidad de conocer quién tiene nuestra información, qué información poseen y cuál es la finalidad de su tratamiento; y más importante aún es permitir, verificar y rectificar la exactitud de los datos, considerando como ya dijimos la disociación entre el titular de la compra y el titular de la prescripción, generando un riesgo cierto de error en la calidad de la misma.

En esa línea parece interesante referirse a las prácticas internacionales en la materia. En Canadá e Inglaterra las farmacias tienen disponibles sus

políticas de privacidad y seguridad en el tratamiento de la información de sus clientes en general y de la información médica en particular, estableciendo que sólo podrán recoger, usar o divulgar su información personal para los fines que fue recopilada, salvo que exista consentimiento del titular o cuando sea requerido o permitido por ley, indicando cuáles son los usos autorizados. Se destaca como una buena práctica la creación de un Oficial de Privacidad,(16) cuya función es supervisar el cumplimiento de la legislación pertinente, así como el contacto con los clientes y las solicitudes de acceso a la información que dispone sobre ellos.

Conclusiones

1. Existe una recopilación de la información asociada a la comercialización de medicamentos cuyas condiciones de tratamiento (registro, recolección, almacenamiento, uso, destinatarios, exactitud, etcétera) son desconocidas por los ciudadanos.

2. La información que se trata en la comercialización de medicamentos corresponde a datos sensibles ya que se refiere al estado de salud física y sicológica de las personas.

3. La regulación sobre la materia es deficiente, porque es parcial, contradictoria y no responde a los estándares mínimos internacionales.

4. El tratamiento indiscriminado y no consentido de la información sobre el estado de salud de las personas puede afectar derechos fundamentales, como el acceso a beneficios de salud, crédito, trabajo.

5. Los criterios que se proponen para regular estas materias deben considerar como variables la afectación a los derechos fundamentales versus el beneficio que obtiene el consumidor con su divulgación.

(16) http://www.ldinsurance.ca/privacypolicy.aspx

Autora

Vanessa Facuse Andreucci

Abogada de la Universidad de Chile, magíster (c) en Derecho Informático y de las Telecomunicaciones. Subjefa de Litigios de la Fiscalía Nacional Económica.

VIII
Privacidad versus seguridad

Felipe Harboe Bascuñán

I. Introducción

Los atentados a las torres gemelas marcaron un punto de inflexión en la relación entre derechos y privacidad en la legislación norteamericana. Hasta entonces, la doctrina imperante señalaba que la administración pública tenía derecho a conocer los datos y antecedentes personales de aquellos individuos que, por alguna razón, hubiesen transitado por el sistema judicial con resultado condenatorio. Es decir, el acceso a los datos personales se circunscribía a infractores del sistema penal, excluyendo al resto de los ciudadanos y habitantes. Ahora bien, la proliferación de fuentes de información de acceso público y su eficiente tratamiento dotaba a la administración —en la práctica— de un cúmulo de información relevante que le permitía construir un perfil de cada sujeto. Un *"perfil de riesgo"* que se utilizaba al momento de desarrollar labores de inteligencia o seguridad preventiva.

(...) hasta antes de los eventos del 11 de septiembre las diversas visiones ideológicas imperantes en materia de seguridad debatían sobre la relación entre seguridad y privacidad. Prevención y coacción de libertades.

En efecto, hasta antes de los eventos del 11 de septiembre las diversas visiones ideológicas imperantes en materia de seguridad debatían sobre la relación entre seguridad y privacidad. Prevención y coacción de libertades. En fin, la seguridad para unos constituía en sí misma una limitación de los derechos fundamentales de otros y tornaba la vida civil en un espacio acosado por la autoridad pública. Por otra parte, había quienes consideraban que gracias a las medidas preventivas los ciudadanos podían ejercer los derechos garantizados o reconocidos por los textos constitucionales. "Sin seguridad no hay libertad" pregonaban aquellos que defendían el derecho de las administraciones de reducir los espacios de privacidad e incrementar los niveles de control o acceso a información privada.

Lo anterior nos lleva a preguntarnos ¿cómo ha de ejercer la autoridad las funciones de seguridad en un régimen democrático? Mucho se ha escrito al respecto y lo cierto es que aún persisten tantas divergencias como visiones de sociedad. En todo caso, eso no será materia de este ensayo, sino que más bien lo que se pretende a continuación es provocar al lector para profundizar sobre un tema que será de creciente debate en las sociedades occidentales del siglo XXI y de cuya resolución dependerán tanto el reconocimiento como la amplitud de los derechos ciudadanos.

II. Desarrollo

Más allá de los debates doctrinarios, lo cierto es que luego de los atentados a las torres gemelas la discusión varió de manera sustancial. Los libertarios se vieron acorralados por los hechos, ya que en el corazón del país de las libertades y los derechos fundamentales se producía un ataque con miles de víctimas. Era hora de cambiar. Los sostenedores de la tesis del enemigo interno y de la doctrina de la seguridad nacional —liderados por el entonces Presidente George W. Bush— se apuraron en crear un escenario propicio para modificar las normas vigentes a la fecha a través de la dictación de la ley USA PATRIOT(1) en 2001. Bajo la premisa de que con mayor información y discrecionalidad se podría haber evitado dicho atentado, USA PATRIOT modificó para siempre el estándar de privacidad y discrecionalidad de las autoridades en materias de limitación de derechos y vulneración de la vida privada. Dentro de las facultades otorgadas por la citada ley cabe mencionar las siguientes:

- Registro de propiedades privadas: Permite a los representantes de la ley el allanamiento de morada, decomisar artículos sin explicación ni orden judicial previa (sección 213).

- Recopilar información sobre libros de estudio, compras, información comercial e historial médico de los ciudadanos: Otorga a las autoridades amplio poder de acceso a cualquier tipo de documentos, ya sea educacionales, médicos, financieros, comerciales, bibliotecarios, etcétera, sin causa probable de delito. Además, prohíbe a los poseedores de la información bajo la amenaza de encarcelamiento (por ejemplo bibliotecarias) que revelen el hecho del acceso al documento en cuestión. Aunque se requiere una orden judicial para obtener información, esta ley permite que el juez utilice un sello de goma como firma (sección 215).

- Ampliación del concepto de terrorista: Extiende el significado oficial de la palabra terrorismo, por lo que podrán ser calificados como terroristas

(1) USA PATRIOT: "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism".

muchos grupos activos en ciertos tipos de desobediencia civil (secciones 411, 802).

- Vigilancia e interceptación de correo electrónico y páginas web visitadas**:** Permite al gobierno vigilar, sin causa justificada, el tráfico de Internet y las comunicaciones por correo electrónico de cualquier proveedor, gracias a la obtención de la "ruta" o "domicilio" en la red. Aunque esta previsión está dirigida a los violadores de la ley, se complica al no poder separarse las actividades inocentes de las que no lo son (sección 216).

- Confiscación de propiedades**:** Permite al gobierno apoderarse de los bienes de un individuo u organización, sin previa notificación o audiencia, si el gobierno dice que han participado o están planeando un acto de terrorismo doméstico (sección 806).

- Acopio de información y datos personales sin autorización previa: Permite reunir mucha información sobre los ciudadanos estadounidenses, la cual será recolectada y compartida con la CIA sin la apropiada vigilancia judicial u otras seguridades (secciones 203 y 901).

- Prisión indefinida de inmigrantes: Faculta la encarcelación indefinida de inmigrantes u otros extranjeros no nacionalizados, sin que el gobierno deba demostrar que realmente son terroristas (sección 412).

- Interceptación telefónica ciega: La ley USA PATRIOT cambia la naturaleza de los mandamientos judiciales para la intervención de las líneas telefónicas, al requerir de los jueces que los aprueben sin que éstos tengan conocimiento de quién es el interceptado o dónde se va a llevar a efecto (sección 216).

Como es posible observar, la extensa limitación de los derechos fundamentales transformaba a la democracia norteamericana en un estado de libertades restringidas y derechos conculcados por la doctrina de la seguridad nacional. Dicha ley se puso en vigencia el 26 de octubre de 2001 y se estableció un período de validez transitoria hasta el 31 de diciembre de 2005. Sin embargo, como en otras ocasiones, antes de finalizar su período de vigencia se incre-

mentaron las presiones de las agencias de seguridad y de ciertos legisladores republicanos que plantearon la extensión de su validez, lo cual fue aprobado en la Cámara de Representantes y rechazado por el Senado, terminando en una comisión bicameral que decidió derogar sólo algunas de dichas facultades, con lo que quedó vigente la gran mayoría de estas "normas de excepción", las que finalmente se plasmaron en la ley promulgada por el Presidente George W. Bush el 09 de Marzo de 2006.

***A** partir de lo anterior resulta evidente que USA PATRIOT mutó definitivamente los conceptos de privacidad y datos personales; limitó de manera sustantiva el concepto de vida privada y su condición de derecho autónomo. En particular, los datos personales pasaron a ser parte del universo posible de interceptar, limitar y aún confiscar.*

A partir de lo anterior, resulta evidente que USA PATRIOT mutó definitivamente los conceptos de privacidad y datos personales; limitó de manera sustantiva el concepto de vida privada y su condición de derecho autónomo. En particular, los datos personales pasaron a ser parte del universo posible de interceptar, limitar y aún confiscar.

De este modo, ¿cuál es el límite de la seguridad en las democracias occidentales? ¿Serán los derechos de las personas o sólo su capacidad de ejercerlos? ¿Llegaremos a un Estado donde se cuestionen los derechos en su esencia por el imperativo de mantener la seguridad del orden colectivo?

En este sentido quizás uno de los elementos de mayor debate lo constituye la regulación aplicable a la protección de los sistemas de comunicación y la privacidad de las comunicaciones entre privados. Por lo pronto, previo al 11 de septiembre ninguna autoridad civil no jurisdiccional ni policial podía interceptar comunicaciones privadas sino era con autorización judicial previa. El sentido y alcance de dicha regulación se fundaba en el reconocimiento de la protección de la vida privada como un derecho fundamental, amparado por garantía de reconocimiento constitucional y resguardada por un nutrido contingente de fallos judiciales o jurisprudencia judicial que, en el caso del derecho norteamericano, constituye precedente y, por tanto, una importante fuente del Derecho.

La comunicación privada es un derecho inherente a la persona natural. La posibilidad de exteriorizar ideas, pensamientos, preocupaciones u otras sensaciones u opiniones de manera reservada se encuentra en sus elementos de la esencia, en los derechos consustanciales a la persona humana y, por ende, los diversos ordenamientos jurídicos no requieren consagrarla sino que

más bien reconocerla, protegerla y garantizarla; consignando los mecanismos jurisdiccionales y administrativos para exigir su protección al Estado.

En una reciente conversación Robert Steelle,[2] reconocido experto en inteligencia, éste afirmó que mientras el gobierno de los Estados Unidos gastó U$74 billones por año en inteligencia; sus productos sólo aportaron en un 4% a la resolución de casos, prevención de ataques o planificación de acciones militares, mientras que las masivas acciones de prevención o planificación militar se realizaron con información captada de fuentes abiertas.

Al observar la evolución de las "eras de inteligencia", es posible reconocer al menos tres etapas diversas a lo largo de la historia. En un primer momento (hasta 1980) se puede hablar de la era de la "Guerra Secreta" donde coexistió el espionaje, la acción encubierta y el interrogatorio como fuente de información. Luego la era del "Análisis estratégico" donde el valor de la inteligencia y seguridad preventiva estaba dado por la capacidad de análisis e interoperabilidad de los datos obtenidos por fuentes cerradas. A partir de 1995 se inauguró la actual era de la "Nación Inteligente" en la que la información vale en cuanto existe capacidad de trabajarla, cruzarla y tratarla de manera adecuada. En esta etapa las fuentes abiertas constituyen un elemento esencial del sistema de inteligencia.

Hoy es posible obtener información abierta que permite crear perfiles de riesgo e incluso definir políticas públicas basadas en dichas fuentes. Así, por ejemplo, en materia de seguridad tenemos a nivel mundial fuentes abiertas como Naciones Unidas; Nasa; Geo-Eye, Cisco, Google, Wikileaks, Facebook, Ops, entre otras.

(...) ¿será correcto otorgar amplias facultades a los organismos de control para recabar información de fuentes reservadas o secretas, mientras no se generen capacidades apropiadas para tratar la información de fuentes abiertas?

Basados en la realidad de esta nueva era de la "Nación Inteligente" ¿será correcto otorgar amplias facultades a los organismos de control para recabar información de fuentes reservadas o secretas, mientras no se generen capacidades apropiadas para tratar la información de fuentes abiertas? Para decirlo de otro modo, ¿debemos disminuir el nivel de privacidad de información personal en razón de la incapacidad de los sistemas para tratar información abierta?

(2) Robert David Stelle. CEO *Earth Intelligence Network.*

Aquí cabe destacar que a medida que se amplían las facultades persecutorias intrusivas se reduce proporcionalmente el ámbito de privacidad de los seres humanos. El concepto de persona se disminuye en razón del potenciamiento del "bien común", "seguridad nacional" u "orden interno".

Es en este debate donde surge la importancia de que los gobernantes reconozcan a través de sus legislaciones la protección de datos personales como derecho autónomo e independiente, tanto en su dimensión sustantiva como en su aspecto orgánico para dotar de mecanismos prácticos de protección a los ciudadanos.

Es en este debate donde surge la importancia de que los gobernantes reconozcan a través de sus legislaciones la protección de datos personales como derecho autónomo e independiente, tanto en su dimensión sustantiva como en su aspecto orgánico para dotar de mecanismos prácticos de protección a los ciudadanos. ¿De qué sirven los derechos sustantivos si los estados no crean los mecanismos de resguardo o protección? De poco o nada, por ello es que el modelo europeo de protección de datos ha consignado la necesidad de que sus estados miembro contemplen ambas variables del derecho a la protección de datos personales para ser considerados como un "país seguro" en esta materia y, por tanto, dignos de transferencia transfronteriza de datos.

III. Conclusiones

Chile está ciertamente influido por los acontecimientos internacionales; sin embargo, nuestro retraso en esta materia nos garantiza —por ahora— cierta inmunidad frente a este proceso norteamericano de reducción de los derechos individuales en función de la seguridad del colectivo. No obstante, el nivel actual en el que se sitúa el país nos ha puesto en una vulnerabilidad muy preocupante, tanto para la libertad individual como para la seguridad personal, familiar y, también, nacional.

En la actualidad existe acceso abierto de terceros países a la información de las principales autoridades (Facebook, Dicom, Wikipedia, Google, Aduanas), bases militares y espacios estratégicos (Google Maps, Street View), lo que nos convierte en una nación vulnerable en materia de seguridad de datos sensibles.

Lo anterior nos lleva a que como país necesitemos crear una ley de protección de datos que sea más que un mero marco regulatorio de la industria del tratamiento de datos personales. Chile precisa hoy de la creación de un cuerpo legal que ampare un derecho sustantivo, la protección de la vida privada como contrapartida de la autoridad persecutora.

En estos momentos estamos viviendo un escenario que marcará de manera definitiva el camino que abordaremos en materia de protección de datos y de protección de la vida privada. Lo primero a partir de la discusión de la nueva institucionalidad en protección de datos y lo segundo a partir del caso "interceptaciones telefónicas" en el marco del caso registro civil, donde se ha producido la colusión de derechos y normas, lo que la autoridad deberá resolver, marcando con su resolución el valor que la entidad persecutora le otorga a la vida privada y a la privacidad de las comunicaciones de los ciudadanos.

Autor

Felipe Harboe Bascuñán

Abogado de la Universidad Central de Chile. Ex Subsecretario del Interior.

IX

Uso de bases de datos como herramienta competitiva en el retail: Algunos aspectos relevantes desde la política de competencia*

Laura Poggi Rodríguez
Enrique Vergara Vial

* Las opiniones vertidas en este documento grafican única y exclusivamente el parecer de sus autores, y en ningún caso representan a la entidad donde éstos trabajan.

I. Introducción

En la actualidad uno de los desafíos más grandes que enfrentan las empresas del retail es entender adecuadamente los requerimientos, necesidades e inquietudes de sus clientes para así poder crear o generar productos y servicios competitivos. La captura de nuevos consumidores y su posterior fidelización es un elemento crítico para el éxito de sus negocios, tarea poco sencilla si se considera que los productos y servicios que ofrecen deben satisfacer a clientes cada vez más exigentes. Debido a esto, las estrategias de marketing sólo serán efectivas en la medida que la oferta se adecúe correctamente a las preferencias de los interesados. Por esta razón, la utilización de herramientas que permitan recopilar y procesar datos relevantes de los consumidores es fundamental para sobrevivir en el duro mundo de los negocios relacionados con el comercio minorista, cuestión que sin duda ha de tener como límite para la forma en que se trata dicha información el respeto de los derechos de los titulares de datos, para lo cual la actividad necesariamente ha de quedar circunscrita a lo preceptuado por la Ley 19.628 sobre protección de la vida privada. He ahí donde se establecen los límites primarios respecto a la forma en que se puede tratar dicha clase de información de manera leal.

(...) la utilización de herramientas que permitan recopilar y procesar datos relevantes de los consumidores es fundamental para sobrevivir en el duro mundo de los negocios relacionados con el comercio minorista, cuestión que sin duda ha de tener como límite para la forma en que se trata dicha información (...)

Hoy existen diversos sistemas informáticos que permiten transformar los datos en información y la información en conocimiento, a partir del cual las empresas construyen relaciones rentables y duraderas con sus clientes, pues cuando se conocen sus preferencias, niveles de ingreso y endeudamiento, patrones de consumo y gustos, se genera un activo fundamental que crea ventajas competitivas a las firmas que operan en un mercado determinado. Ahora bien, aquello que permite perfilar a los clientes se cierne como una amenaza para el adecuado ejercicio de derechos si es que el tratamiento de la información no respeta los principios rectores del tratamiento de datos personales.

Con los datos recopilados, las empresas crean bases de datos de clientes, de usuarios registrados y de posibles compradores, lo que permite a las empresas desarrollar, entre otras, las siguientes estrategias comerciales:

a. Mantener una comunicación constante con sus clientes
b. Conocer las tendencias de compra del mercado objetivo
c. Segmentar e identificar diversos nichos de mercado
d. Generar estrategias de *branding* y publicidad más efectivas

Como se comprenderá, todas estas funciones permiten la fidelización de clientes. De este modo, las bases de datos —en tanto valiosos instrumentos de información— se utilizan en conjunto con los diversos recursos informáticos disponibles (*software* y *hardware*) como un factor estratégico diferenciador que permite incrementar la rentabilidad de las compañías, generando propuestas de valor y experiencias más segmentadas.

Hechos estos alcances, el objetivo este artículo es presentar algunos problemas que el tratamiento de los datos de las personas destinado a su fidelización pueden producir desde la perspectiva de la política de libre competencia.

II. Uso de bases de datos en el retail: Sinergia de la información en una industria cada vez más integrada

Como se ha dicho, la necesidad que tienen las empresas de conocer los patrones de consumo y endeudamiento de los consumidores para poder competir de manera eficaz y eficiente en la industria del retail las obliga a desarrollar y procesar una gran cantidad de información relacionada con sus gustos y preferencias. En buenas cuentas, para sobrevivir requieren tratar[(1)] los datos personales[(2)] de los consumidores, almacenarlos[(3)] e incorporarlos a un registro o banco de datos[(4)] que les permita cruzarlos entre sí, de manera de poder dirigir sus estrategias de comercialización del modo más focalizado y eficiente posible.

(1) De acuerdo con lo dispuesto en el artículo 3º letra o de la Ley 19.628, por tratamiento de datos se entiende cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

(2) De acuerdo con lo dispuesto en el artículo 3º letra f de la Ley 19.628, por datos personales han de entenderse aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

(3) De acuerdo con lo dispuesto en el artículo 3º letra a de la Ley 19.628, el almacenamiento de datos se refiere a la conservación o custodia de datos en un registro o banco de datos.

(4) De acuerdo con lo dispuesto en el artículo 3º letra m de la Ley 19.628, el registro o banco de datos es el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

Para recolectar dichos datos, las empresas desarrollan innumerables estrategias. Dentro de las más efectivas se encuentran aquellas en que se ofrece un descuento a los consumidores que proveen datos e información relevante de su situación personal. Son las famosas rebajas de precios por concesión del número de RUT. Incluso en el último tiempo, el dinamismo del comercio ha producido que las empresas desarrollen sistemas cada vez más sofisticados de recolección de datos, algunos de los cuales permiten recabar información sin que el consumidor pueda darse cuenta de ello, cuestión que desde la óptica de la protección de datos debe ser rechazada, al faltar el elemento esencial para que éste sea legítimo, cual es que el titular de los datos esté informado y otorgue su consentimiento para el tratamiento de su información.

(...) el dinamismo del comercio ha producido que las empresas desarrollen sistemas cada vez más sofisticados de recolección de datos, algunos de los cuales permiten recabar información sin que el consumidor pueda darse cuenta de ello (...)

Un ejemplo ilustrativo de esto último es la reciente y novedosa promoción que realizó en Brasil la marca de detergente en polvo OMO de Unilever,[5] la cual insertó en 50 cajas de detergente dispositivos de GPS no perceptibles por los consumidores al momento de comprarlos. Estos dispositivos se accionaban cuando la caja salía del supermercado y permitían seguir al consumidor hasta su hogar, sin que éste supiera que estaba siendo seguido y, por supuesto, sin su consentimiento previo. Para evitar eventuales reclamaciones de los afectados, la estrategia contemplaba incluso la eventual entrega de obsequios.

Como se puede apreciar, a primera vista el modelo de negocios conforme al cual hoy compiten las empresas en el mercado del comercio minorista parece ser muy atractivo para los consumidores, pues mediante el estudio y análisis de sus datos, tales como sus hábitos de compra, sus preferencias, la georreferencia y muchos otros, las compañías se esfuerzan en elaborar un verdadero traje a su medida.

Observemos lo anterior con otro caso concreto. La filial de *Domino's Pizza* en Japón[6] desarrolló una estrategia de venta en la que unió los beneficios

(5) http://www.brainstorm9.com.br/advertising/omo-com-gps-um-vale-brinde-que-encontra-o-consumidor/

(6) Mackinsey Quarterly, marzo de 2010, *"Learning from the japanese consumer: Three executives on next-generation marketing"*.

del manejo de las bases de datos de sus clientes con la tecnología informática disponible, logrando incrementar la efectividad de sus publicidades a un costo irrisorio. La referida cadena identificó que en su filial en dicho país el consumo de pizza se incrementaba cuando llovía o había partidos de fútbol de ligas importantes, razón por la cual creó una estrategia de venta dirigida que consistía en el envío de *flyers* justo cuando empezaba a llover. De esta forma, utilizaron la información disponible (incremento del consumo de pizzas en días lluviosos) junto a la base de datos de sus clientes (e-mails), con el fin de promover el consumo impulsivo de pizzas en el momento propicio. La efectividad de la iniciativa superó las expectativas, pues mientras las campañas de publicidad a través del envío de *flyers* dirigidos presentan tasas de efectividad del orden del 2 al 3%, la emprendida por *Domino's Pizza* en Japón presentó una tasa de efectividad superior al 10%.

Cabe agregar, que el manejo de tales datos permite a las empresas identificar las relaciones de complementariedad existentes entre muchos productos disponibles en el mercado, permitiendo el desarrollo de negocios en que gran cantidad de las necesidades de los clientes son satisfechas en un mismo lugar, lo que se conoce como el fenómeno del *One Stop Shopping*, esto es, la tendencia a la concentración de la venta de una amplia canasta de productos en un solo lugar. El beneficio que esto tiene para el consumidor se traduce en un menor costo de búsqueda y para el comercio en ventajosas economías de ámbito.(7)

(...) el manejo de tales datos permite a las empresas identificar las relaciones de complementariedad existentes entre muchos productos disponibles en el mercado, permitiendo el desarrollo de negocios en que gran cantidad de las necesidades de los clientes son satisfechas (...)

Por último, además de la comodidad que significa para un consumidor poder realizar todas las compras de un determinado tipo en el mismo lugar, éste obtiene otros beneficios derivados de los denominados "programas de fidelización", a través de los cuales la empresa premia su lealtad, ofreciéndole mejores precios a través de descuentos, regalos, puntos, etcétera.

(7) Son aquellas que se presentan en situaciones en las que es más eficiente que una sola empresa produzca dos o más bienes que los mismos sean producidos por distintas empresas.

III. No todo lo que brilla es oro: Bases de datos, programas de fidelización y libre competencia

Junto con los innegables beneficios que para los consumidores ha traído esta nueva forma de competir, tanto el procesamiento y manejo de datos personales como los programas de fidelización pueden, sin embargo, producir efectos negativos para la libre competencia, los que, en general, son muy difíciles de captar a simple vista por parte de los consumidores.

El manejo de datos y sus efectos en la competencia no es un tema nuevo en la experiencia comparada. Así, por ejemplo, el año 2005 la compañía europea de telecomunicaciones CONDUIT presentó ante uno de los tribunales de lo mercantil de Madrid una denuncia contra Telefónica por la infracción del artículo 82 del Tratado de la Comunidad Europea, porque había abusado de su posición dominante en el mercado de los servicios de información telefónica al haberle negado el acceso a la información de su base de datos de abonados, lo que había sido prohibido con anterioridad por el regulador sectorial —la Comisión del Mercado de las Telecomunicaciones— que señaló que Telefónica, como proveedor monopólico, estaba obligada a facilitar el acceso de esa información a CONDUIT y al resto de las compañías que participan en este mercado, pues era esencial para prestar el servicio de información telefónica en forma gratuita y en un determinado formato. En primera instancia, el Tribunal de lo Mercantil de Madrid falló favorablemente a CONDUIT.[8]

En el caso de Chile, el retail con sus negocios integrados está muy concentrado, razón por la cual gran parte de la información de los consumidores está en manos de pocas empresas (...)

Analicemos brevemente algunas problemáticas parecidas surgidas en el retail. En el caso de Chile, el retail con sus negocios integrados está muy concentrado,[9] razón por la cual gran parte de la información de los consumidores está en manos de pocas empresas, las cuales pueden además obtener dicha información de manera rápida y a bajos costos.

(8) http://www.naider.com/ateneo/articulo_blog.asp?id=357

(9) A modo de ejemplo, en la industria supermercadista las tres principales cadenas controlan cerca del 85% del mercado; en el mercado farmacéutico, las tres firmas más grandes más del 90%.

En efecto, cuando estas grandes empresas del retail acceden a volúmenes de información relacionados con los patrones de compras de sus consumidores la cruzan e interrelacionan con fuentes de distinta naturaleza, obtienen un grado de conocimiento sobre los gustos y necesidades de clientes actuales o potenciales prácticamente imbatible. Lo anterior les facilita, por ejemplo, utilizar datos de manera más precisa y, por ende, ganar profundidad de análisis, como también complementar sus bases de datos con las otras unidades de negocios.(10)

El caso D&S-Falabella y la utilización de bases de datos

La fallida fusión entre las empresas D&S y Falabella es un caso paradigmático en esta materia, pues por primera vez se valoró la información de los clientes de tal manera que permitió concluir que su concentración en manos de un actor relevante del mercado podría generar distorsiones a la libre y sana competencia, al permitirle desarrollar estrategias de marketing y programas de fidelización personalizados y segmentados para tipologías específicas de preferencias de consumo que ningún otro actor en el mercado sería capaz de desarrollar.

La fallida fusión entre las empresas D&S y Falabella es un caso paradigmático en esta materia, pues por primera vez se valoró la información de los clientes de tal manera que permitió concluir que su concentración en manos de un actor relevante del mercado podría generar distorsiones (...)

Efectivamente, el Tribunal de Defensa de la Libre Competencia (TDLC) en su resolución Nº 24 relevó la importancia de lo anterior al punto de considerar que el procesamiento de datos generaría ventajas competitivas irreplicables para otros actores del mercado y, en consecuencia, entregaría un brutal poder de mercado a las empresas que consultaron la operación.

De este modo, el TDLC analizó el modelo de negocio del retail en Chile bajo el concepto de *"retail integrado"*, estableciendo que: "En la actualidad las principales empresas del retail desarrollan un modelo de negocios que han denominado *retail integrado*, mediante el cual se busca llevar adelante de

(10) "Con la compra del 88% de supermercados San Francisco en agosto de 2004, Falabella ingresó como un actor relevante en el rubro de alimentos en Chile, pasando a cubrir con sus diversas actividades aproximadamente el 60% de las necesidades de compra del consumidor", Memoria Anual de Falabella 2004, disponible en http://www.falabella.com/pdf/MemoriaAnual/2004/Memoria_Anual_2004.pdf., página 11.

manera integrada los negocios de supermercados, tiendas por departamento, tiendas para el mejoramiento del hogar, administración de tarjetas de crédito, servicios bancarios, desarrollo de proyectos inmobiliarios complementarios, y diversos servicios adicionales tales como seguros generales, agencias de viajes, servicios de mudanza, entre otros. Con esta estrategia, operadores de *retail integrado* han logrado alcanzar importantes participaciones de mercado, cubriendo la oferta de diversos productos y servicios que, en conjunto, representan un porcentaje significativo del gasto mensual de los consumidores".

En su raciocinio, el Tribunal reconoció, de manera expresa, la importancia que el manejo de bases de datos puede tener para la libre competencia, al considerar que las sinergias derivadas de la utilización de las bases de datos les permitiría crear estrategias de comercialización muy difíciles de desarrollar para sus competidores, actuales o potenciales.

En este sentido, el tribunal destacó como información relevante las preferencias de distintos grupos de consumidores y sus perfiles de pago en su rol como deudores, identificando las diferencias entre cada segmento y la potencialidad que tenían para complementarse entre ellos.(11)

(...) a pesar de los innegables beneficios que para los consumidores ha traído esta nueva forma de competir, en forma paralela, el manejo de datos por parte de pocas empresas producirá en el mediano y largo plazo problemas para su bienestar porque el poder de mercado de las firmas que operan en este mercado es cada vez mayor y existe el riesgo cierto de que se ejerza de manera abusiva (...)

Por lo anterior, a pesar de los innegables beneficios que para los consumidores ha traído esta nueva forma de competir, en forma paralela, el manejo de datos por parte de pocas empresas producirá en el mediano y largo plazo problemas para su bienestar porque el poder de mercado de las firmas que operan en este mercado es cada vez mayor y existe el riesgo cierto de que se ejerza de manera abusiva, sobre todo si, como lo predice el Tribunal, existen bajísimas probabilidades que se las pueda desafiar.

(11) Por ejemplo, la información de compras en supermercados permite formar bases de datos de este tipo en forma más rápida que en otros segmentos del retail, dada la frecuencia de visitas del consumidor a los supermercados, además sin enfrentar el riesgo de las variaciones en las "modas" que son mucho más fuertes en las tiendas por departamento. También el Tribunal da el ejemplo de los centros comerciales, en los que destaca la capacidad de sus controladores para obtener información sobre patrones y tendencias de consumo del conjunto de visitantes, dados los contratos de arriendo de espacios de venta por parte de un amplio y diverso conjunto de tiendas de venta minorista, en los cuales el valor de dichos arriendos incluye cobros en base a las ventas obtenidas por cada locatario. Ver resolución Nº 24 del TDLC, página 91.

Programas de fidelización y sus efectos en la competencia

Como se ha venido argumentando, a consecuencia de la utilización de nuestros datos personales pueden surgir problemas más sutiles, casi imperceptibles para los consumidores, los que pueden afectar su bienestar en el mediano y largo plazo.

Dentro de los problemas que para la libre competencia trae aparejado el tratamiento de datos a esa escala, en forma creciente se ha destacado el de la cautividad de los consumidores como consecuencia de los ya citados programas de fidelización.

Desde el punto de vista de la libre competencia y bajo una óptica de organización industrial, la OCDE los ha definido como aquellas estructuras de precios más bajos ofrecidas por las empresas a aquellos consumidores que, expresa o tácitamente, abastecen gran parte de sus necesidades con la misma. Estos pueden tomar una gran variedad de formas, desde precios más bajos hasta, como se señaló, diversos regalos u objetos con precios rebajados.

Estos programas son capaces de alterar las libres decisiones de compra de los consumidores, toda vez que, dependiendo de su diseño, elevan sustancialmente los costos de cambio a empresas alternativas (*switting cost*). En la doctrina y jurisprudencia de libre competencia abundan ejemplos de ese tipo, siendo los más comunes aquellos que se relacionan con los programas de pasajeros frecuentes y su aptitud para constituirse, al mismo tiempo, en barreras a la entrada de nuevos competidores por los altos costos de cambio que presentan para los consumidores.

***Estos programas son capaces de alterar las libres decisiones de compra de los consumidores, toda vez que, dependiendo de su diseño, elevan sustancialmente los costos de cambio a empresas alternativas* (switting cost).**

Con su introducción y posterior masificación en distintos mercados, especialmente los asociados al retail, los programas de fidelización han cambiado el paradigma de la competencia. Se ha transitado desde una competencia por el margen de precios hacia una competencia por el cliente.

Quizás el ejemplo más conocido es el de los programas de pasajeros frecuentes que ofrecen hoy las principales líneas áreas del mundo, herramienta sin la cual es casi imposible competir. Los consumidores están felices y cómo

no estarlo si cada cierto tiempo pueden viajar "gratis" con el millaje acumulado. Sin embargo, lo que los consumidores no ven es que van quedando cautivos de la línea aérea que les ofrece el millaje, lo que hace extraordinariamente difícil para una nueva compañía entrar a este mercado por los costos de cambio involucrados, con lo cual los consumidores cada vez se van quedando con menos alternativas.

(...) lo que los consumidores no ven es que van quedando cautivos de la línea aérea que les ofrece el millaje, lo que hace extraordinariamente difícil para una nueva compañía entrar a este mercado por los costos de cambio involucrados (...)

Como señaló el TDLC en su sentencia Nº 44, dado que estos programas imponen como requisito un nivel mínimo de compras antes de poder cobrar un premio, el que se ofrece de manera marginalmente creciente por mayores volúmenes de compra, incentivando de este modo al consumidor a concentrar sus compras con un único proveedor, produciéndose una importante barrera de entrada a los nuevos competidores, lo que ha producido la consiguiente preocupación de las autoridades de competencia, las que, incluso, en algunos países han obligado a las compañías dominantes a abrir estos programas a las aerolíneas pequeñas.

Una situación similar está ocurriendo en el retail. La masificación de programas de fidelización representados, principalmente, en tarjetas de crédito ofrecidas por grandes superficies ha generado importantes barreras a la entrada en esos mercados. Esta situación ya fue develada por la Fiscalía Nacional Económica en el requerimiento presentado en el mes de agosto de 2006 en contra de las principales cadenas de supermercados del país, D&S y Cencosud, en el cual identificó como una de las barreras que presentaba esta industria la masa crítica de titulares de tarjetas de propia emisión que fidelizan y cautivan a los clientes.

IV. Conclusiones

El manejo de información ha permitido grandes avances en la forma como las empresas compiten. En la medida que la misma haya sido obtenida de manera leal, nada puede reprocharse sobre su uso; es más, el desarrollo de bases de datos ha permitido que los consumidores ahorren tiempo y dinero en sus actos de consumo, obteniendo atractivos descuentos, premios y beneficios.

Así se compite hoy, sobre todo en la industria del comercio minorista. Para asegurar la lealtad en el tratamiento de datos resulta útil la determinación de una especie de "*test de la blancura"* a través del cual se asegure la adecuada implementación de los principios de legitimidad, exactitud, finalidad, proporcionalidad, transparencia, no discriminación y seguridad en el tratamiento de datos personales, en las políticas de tratamiento de datos personales que las empresas implementan.

Sin embargo, los casos citados, en especial el análisis que hace el TDLC cuando revisó la fusión de D&S con Falabella, revelan que esta forma de competir puede producir efectos adversos en la competencia en el mediano y largo plazo, los que al final van a recaer en los mismos consumidores que hoy están felices.

Lo anterior no significa, necesariamente, que el tratamiento de datos como herramienta de comercialización sea una conducta anticompetitiva *per se*, pero al menos se ha podido concluir que, en algunos casos, puede inhibir la entrada de nuevas competidores. Por consiguiente, resulta muy importante incorporar esta variable en los análisis de los casos de libre competencia cuando se revisan las condiciones o barreras de entrada del mercado relevante.

Autores

Laura Poggi Rodríguez

Economista. Coordinadora de la División de Investigaciones de la Fiscalía Nacional Económica (FNE).

Enrique Vergara Vial

Abogado. Ex Fiscal Nacional Económico.

X

Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación*

Enrique Rajevic Mosler

* Ponencia presentada en el taller "Chile y la Protección de Datos Personales", organizado por Expansiva (Santiago, 26 de noviembre de 2010). Agradezco las observaciones realizadas por los asistentes a dicho encuentro y las formuladas a la primera versión de este texto por la profesora de la U. de Chile Andrea Ruiz R., aunque asumo mi responsabilidad personal por el resultado final y las opiniones aquí vertidas (erajevic@uahurtado.cl).

I. Introducción

Con casi una década de diferencia los legisladores chilenos aprobaron la Ley 19.628, de 1999,[1] para regular la protección de datos personales (en adelante, LPDP), y la Ley 20.285, de 2008,[2] para normar el régimen del acceso a la información pública. Ambos cuerpos legales regulan el mismo objeto: la información. El primero cautela la información que concierne a personas naturales identificadas o identificables, desde una perspectiva que pretende garantizar que sus titulares sean quienes decidan sobre su uso. El ámbito del segundo, en cambio, es la información que obra en poder de los órganos del Estado (básicamente la administración pública) —la que puede incluir datos personales— con la óptica de favorecer su conocimiento por parte de la ciudadanía. La protección de los datos personales resguarda la intimidad y la autodeterminación informativa; la transparencia administrativa favorece la probidad y potencia la participación ciudadana. Todos ellos son bienes jurídicos reconocidos por nuestra Constitución y, potencialmente, antagónicos.

El conflicto, entonces, es inevitable, ¿qué principios aplicaremos cuando nos enfrentemos a esta intersección? ¿El deber de resguardar la confidencialidad de los datos personales o el derecho de las personas a acceder a la información pública? ¿A quién le encargaremos resolver este conflicto?

En efecto, parte de la información que obra en poder de los órganos públicos está constituida por datos personales. Ejemplos sobran, como los de los alumnos que estudian en colegios públicos, los jubilados en el sistema público de pensiones, los pacientes atendidos en hospitales públicos, los propios funcionarios o los beneficiarios de las múltiples prestaciones que otorga la administración estatal. El conflicto, entonces, es inevitable, ¿qué principios aplicaremos cuando nos enfrentemos a esta intersección? ¿El deber de resguardar la confidencialidad de los datos personales o el derecho de las personas a acceder a la información pública? ¿A quién le encargaremos resolver este conflicto? ¿A una sola autoridad administrativa que maneje ambos temas o a los tribunales de justicia? No se trata de preguntas que sólo se generen entre

(1) Publicada en el D.O. de 28/08/1999.

(2) Publicada en el D.O. de 20/08/2008.

nosotros, sino que de cuestionamientos que están presentes en todos los sistemas jurídicos que han llegado a regular estas instituciones.(3) Sin embargo, cada país debe construir una solución a la medida de las convicciones de sus ciudadanos y de su desarrollo institucional.

De este modo en las páginas que siguen abordaré cómo estamos afrontando este reto en Chile. Para ello describiré sucintamente los principios básicos de las normativas chilenas sobre protección de datos personales y acceso a la información pública, así como su anclaje constitucional; centrándome en esta última en la Ley de Transparencia (en adelante LT) contenida en el artículo primero de la Ley 20.285. A continuación me referiré a algunas fricciones entre ambas normativas y relataré cómo las ha ido resolviendo el organismo encargado de dirimir las contiendas sobre acceso a la información de la administración del Estado, el denominado "Consejo para la Transparencia" (en adelante CPT). Terminaré con algunas conclusiones y propuestas.

II. La protección de datos personales: Fundamentos y situación en el sector público

La LPDP define datos personales como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables (art. 2º f), a diferencia de los datos estadísticos que son aquellos que, en su origen, o como consecuencia de su tratamiento, no pueden ser asociados a un titular identificado o identificable (art. 2º e). Dentro de los datos personales existe una categoría que recibe mayor protección: los datos sensibles, que son los referidos "…a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos

La LPDP define datos personales como aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

(3) A modo de ejemplo puede verse sobre el caso español a José L. Piñar M., *Seguridad, transparencia y protección de datos: El futuro de un necesario e incierto equilibrio*, Documento de Trabajo 147/2009, Madrid: Laboratorio de Alternativas. 2009, 64 p., y sobre el caso uruguayo a Carlos E. Delpiazzo, "A la búsqueda del equilibrio entre privacidad y acceso", en Carlos E. Delpiazzo (coord.) *Protección de datos y acceso a la información pública*, Agesic-FCU, Montevideo, 2008, p. 9-22.

y la vida sexual" (art. 2º. g). La misma definición se encuentra en la LT con un ligero matiz: "origen social" en vez de "racial" (art. 7º i, inc. 2º).

Nuestra ley no es sino el eco de las leyes de protección de datos que aparecieron en el último medio siglo de la mano del creciente desarrollo de la informática, el que ha permitido procesar datos de una manera que antes era completamente inconcebible y que desde el advenimiento de Internet permite transferirlos con enorme facilidad, todo lo cual pone en evidente riesgo la intimidad de las personas. Precisamente la LPDP parte anunciando que regula el "tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares" (art. 1º). Dos términos son aquí esenciales:

Nuestra ley no es sino el eco de las leyes de protección de datos que aparecieron en el último medio siglo de la mano del creciente desarrollo de la informática, el que ha permitido procesar datos de una manera que antes era completamente inconcebible y que desde el advenimiento de Internet permite transferirlos con enorme facilidad.

- Banco de datos, que es el "conjunto organizado de datos personales, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos" (art. 2 m). En consecuencia, no es cualquier dato suelto sino aquél que forma parte de un conjunto organizado que permita relacionamientos.

- Tratamiento, en tanto, es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma pública" (art. 2 o). La cantidad de verbos da cuenta de la amplitud de esta noción. Prácticamente toda utilización de un dato cabe dentro del concepto.

En el entorno comparado los orígenes de estas regulaciones pueden situarse en una ley estadounidense de 1974, la llamada "Privacy Act". En Europa, algunas constituciones en esa misma década afrontaron este tema —como el art. 18.4 de la Constitución española de 1978 o el art. 35 de la

Constitución Portuguesa de 1976— y en 1981 el Consejo de Europa aprobó el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Se trata de textos que influirán en todas las normas posteriores.(4) A nivel internacional se destaca luego la Directiva 95/46/CE del Parlamento y del Consejo Europeo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,(5) que en tal carácter será el molde de las legislaciones de sus países miembros (en el caso español, por ejemplo, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).(6) A su vez, el art. 8º de la Carta de Derechos Fundamentales de la Unión Europea (2000) reconoce a toda persona el "…derecho a la protección de los datos de carácter personal que le conciernan", añadiendo que aquéllos "se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Termina indicando que "toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación".

(...) no se trata del puro derecho a ser dejado solo, en la formulación decimonónica del derecho a la intimidad* (the right to be let alone)*, sino del derecho a la autodeterminación informativa, esto es, el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad.

La protección de los datos personales es una derivación del derecho a la intimidad que, según la doctrina, llega a configurar un nuevo y específico derecho fundamental de tercera generación,(7) reconocido ya en 1983 en la sentencia del tribunal constitucional alemán en el caso de la Ley de Censo de Población. En efecto, no se trata del puro derecho a ser dejado solo, en la formulación decimonónica del derecho a la intimidad (*the right to be let alone*),

(4) A modo de ejemplo la definición de datos personales en el Convenio 108 es "cualquier información relativa a una persona física identificada o identificable" (art. 2º a) y, aunque no habla de datos sensibles, declara que: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales" (art. 6º).

(5) DOCE L 281, de 23/11/1995.

(6) BOE núm. 298, de 14/12/1999.

(7) Véase la sentencia del Tribunal Constitucional español 292/2000, del 30 de noviembre, esp. su FJ 7, y sobre esta generación de derechos Antonio Pérez L., La Tercera Generación de Derechos Humanos, Navarra: Aranzadi, 2006, 320 p.

sino del derecho a la autodeterminación informativa, esto es, el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad.(8) En otras palabras, no sólo se trata de una noción negativa o abstencionista (excluir a otros) sino también una positiva (controlar mis datos). Con todo, la protección no se opone a reconocer que la circulación de estos datos también es una necesidad social. Se trata, en definitiva, de aprovechar los beneficios que brindan a la sociedad las nuevas tecnologías informáticas de una manera que respeten los derechos de las personas.

En Chile el derecho a la intimidad se encuentra reconocido en el artículo 19 Nº 4 de la Constitución que asegura el "respeto y protección a la vida privada y a la honra de la persona y su familia".

En Chile el derecho a la intimidad se encuentra reconocido en el artículo 19 Nº 4 de la Constitución que asegura el "respeto y protección a la vida privada y a la honra de la persona y su familia". De hecho, la Ley 19.628 aparece titulada como "ley sobre protección de la vida privada" además de "ley sobre protección de datos de carácter personal". Con todo, tras este frontis "protector" lo primero que hace es reconocer que toda persona puede tratar datos personales si se ajusta a sus normas. La doctrina ha puesto de relieve sus insuficiencias, como la ausencia de un órgano efectivo de fiscalización, un *habeas data* judicial poco operativo (de hecho, apenas utilizado) y un talante tolerante con los tratamientos que realizan algunos agentes privados en materia comercial.(9) Esto hace que no cumplamos integralmente ni con las directrices de la OCDE(10) ni con los estándares de la Directiva 95/46/CE para que la UE nos declarase un país seguro para el flujo de datos desde sus estados miembros (cosa que ya han logrado Argentina en 2006 y Uruguay en 2010).

Pese a la necesidad de los apuntados perfeccionamientos, los preceptos de la LPDP establecen un sistema que ha venido a ordenar el tratamiento de datos

(8) Véase sobre esto Isabel-Cecilia del Castillo V. *Protección de datos: Cuestiones constitucionales y administrativas.* Madrid: Thomson-Civitas, 2007, p. 213-241.

(9) Puede verse a este respecto Renato Jijena L. *Comercio Electrónico, Firma Digital y Derecho*. Santiago, Editorial Jurídica, 2002. p. 75-78. También puede consultarse Pedro Anguita R. *La Protección de datos personales y el derecho a la vida privada*. Santiago, Editorial Jurídica, 2007. p. 331-342, y Raúl Arrieta C., "Chile y la Protección de Datos Personales: Compromisos internacionales", en *VV.AA. Chile y la Protección de Datos Personales: ¿Están en crisis nuestros derechos fundamentales?*, Expansiva UDP, Santiago de Chile, 2009, p. 18-21.

(10) Me refiero a las "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", de 23/09/1980. Pueden verse en español en el sitio de la Agencia Española de Protección de Datos (http://www.agpd.es).

personales evitando al menos algunos abusos. Lo primero que merece consignarse es que puede derivarse una serie de principios para el tratamiento, todos los cuales se aplican a la administración pública. Se trata de los siguientes:

a) El principio de licitud que deriva de los artículos 2º, 4º incisos 1º y 6º, y según el cual el tratamiento sólo cabe si existe autorización legal o de parte del titular, debiendo en este último caso tratarse de un consentimiento expreso.

b) El principio de información al titular respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público, establecido en el art. 4°, inc. 2º.

c) El principio de veracidad de los datos, que exige corregir los que sean erróneos, inexactos, equívocos o incompletos (art. 6°, inc. 2°).

d) El principio de finalidad de los datos, que fluye del art. 9º, y conforme al cual debe respetarse la finalidad para la que fueron recogidos los datos, de manera que exista una relación directa entre aquella y el dato recabado.

e) El principio de seguridad de los datos, contemplado y cautelado en el art. 11 y, tratándose de los órganos de la Administración, por el D.S. N° 83/2004, SEGPRES.

f) El principio de confidencialidad que se aplica cuando se trata de datos obtenidos de fuentes no accesibles al público según el art. 7º.

Por otro lado, la ley reconoce un conjunto de derechos a los titulares de datos personales. Se trata de los derechos de acceso, rectificación, cancelación y bloqueo. El primero permite a toda persona exigir al responsable de un banco información sobre qué datos de su titularidad está tratando y, además, sobre "…su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente" (art. 12, inc. 1º). El derecho a rectificar permite exigirle que modifique los datos "erróneos, inexactos, equívocos o incompletos" (art. 12, inc. 2º) y el de cancelación, que los elimine "en caso de que su

almacenamiento carezca de fundamento legal o cuando estuvieren caducos" (art. 12, inc. 3º) o cuando cese el consentimiento para su uso, si fueron obtenidos voluntariamente o se usan para comunicaciones comerciales (art. 12, inc. 4º). En esta última hipótesis también cabe el derecho de bloqueo, esto es, a exigir la suspensión temporal de cualquier operación de tratamiento. Debe señalarse que no existe un derecho de oposición al tratamiento, en los términos que existen en el derecho comparado.

El ejercicio de estos derechos es irrenunciable (art. 13), pero no cabe respecto de los órganos públicos cuando "impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional" o, si el almacenamiento fue por mandato legal, "fuera de los casos contemplados en la ley respectiva" (art. 15).(11)

El art. 16 de la LPDP garantiza el ejercicio de estos derechos a través de una acción que debe interponerse ante el juez de letras en lo civil del domicilio del responsable del banco de datos o ante la Corte Suprema, si la causal invocada para denegar la solicitud fuese la seguridad de la nación o el interés nacional. De acogerse la reclamación puede aplicarse una multa de hasta 50 unidades tributarias mensuales. Hay, asimismo, derecho a ser indemnizado por el daño patrimonial y moral que causare el tratamiento indebido de los datos en los términos del art. 23 de la LPDP.

(...) la ley proscribe el tratamiento de los datos sensibles salvo que la ley lo autorice, exista consentimiento del titular o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (...)

Finalmente, debe destacarse que la ley proscribe el tratamiento de los datos sensibles salvo que la ley lo autorice, exista consentimiento del titular o se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (art. 10).

El título V de la LPDP, de apenas tres artículos, regula el tratamiento de datos por parte de los organismos públicos. Cabe recordar que el art. 1º aplica a éstos ultimos las normas generales, de manera que este título contiene sólo especificaciones para los organismos públicos.

(11) El inciso 2º del art. 15 es una norma oscura, pues los órganos de la Administración no debiesen almacenar datos sin mandato legal, pero no hay espacio para ahondar en ello.

El artículo 20 refuerza el principio general de licitud al restringir el tratamiento de datos a las materias que sean de competencia de cada organismo y "con sujeción a las reglas precedentes". En esas condiciones, añade, la administración "no necesitará el consentimiento del titular". Esto constituye, en mi opinión, una autorización que abre el tratamiento de datos personales con relativa amplitud —incluso en el ámbito de las potestades domésticas de la Administración— pero con el resguardo de aplicar a este tratamiento las demás reglas de la ley que salvaguardan los derechos de los particulares. Para ello tiene especial interés la regla de la finalidad establecida en el art. 9º, que al restringir el uso de los datos a los fines para los cuales fueron recolectados proscribe su entrega a terceros para otras finalidades, en lo que no es sino una aplicación estricta del sistema de vinculación positiva del principio de juridicidad.(12)

El art. 21, por su parte, impide a los organismos que sometan a tratamiento "datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias" que los comuniquen "una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena". Se trata de una especie de "derecho al olvido" que favorece la reinserción de las personas, especialmente tratándose de condenas penales. Se exceptúan de lo anterior las solicitudes formuladas por los tribunales u otros organismos públicos dentro del ámbito de su competencia (art. 21, inc. 2º).

Finalmente, el art. 22 encarga al Servicio de Registro Civil e Identificación llevar un registro de los bancos de datos personales a cargo de organismos públicos, el que fue reglamentado por el D.S. N° 779/2000, del Ministerio de Justicia.(13) No hay, sin embargo, sanciones para el incumplimiento de este deber.

III. El acceso a la información pública como derecho

El derecho de acceso a la información pública fue reconocido en Chile por la Ley 19.653, de 1999, sobre Probidad Administrativa, que consagró como regla general la publicidad de los actos administrativos y la de "los documentos que les sirvan de sustento o complemento directo y esencial", restringiendo la

(12) Art. 2º de la Ley 18.575, de 1986, cuyo texto refundido, coordinado y sistematizado fue fijado por el D.F.L. N° 1/19.653 (D.O. 17.11.2001).

(13) Disponible en http://www.srcei.cl/f_banco_de_datos.html.

reserva a un listado basado en cuatro causales que podía ser desarrollado por vía reglamentaria y admitiendo una impugnación en sede judicial. Es interesante destacar que esta última era semejante a la del art. 16 de la LPDP, incluso con la diferenciación de un procedimiento ante el juez en lo civil y otro ante la Corte Suprema, este último cuando se alegase la afectación de la seguridad de la nación o el interés nacional (art. 14).

Pues bien, en tan sólo una década diversos factores llevaron a un cambio radical. Entre éstos conviene destacar la sentencia de la Corte Interamericana de Derechos Humanos en el caso "Claude Reyes y otros vs. Chile",(14) que declaró que el sistema de acceso a la información chileno infringía el art. 13 de la Convención Americana sobre Derechos Humanos o Pacto de San José, pues éste garantizaba "el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado" (párrafo 77). Ello venía a significar que este derecho se integraba a nuestra Carta Fundamental en virtud de su art. 5°, que exige a los órganos del Estado respetar y promover los derechos esenciales que emanan de la naturaleza humana garantizados "por los tratados internacionales ratificados por Chile y que se encuentren vigentes", uno de los cuales es el Pacto de San José. El propio Tribunal Constitucional declaró que el acceso a la información administrativa estaba implícitamente reconocido por la Constitución, pues el art. 19 Nº 12 de la Constitución además de contemplar la "libertad de emitir opinión e informar" abarcaba el derecho a buscar y recibir información.(15) Además, desde la reforma constitucional de 2005(16) la transparencia pasó a constituir una de las Bases de la Institucionalidad pública chilena, al incorporarse un nuevo artículo 8º a nuestra Carta Fundamental, cuyo inciso 2º dispone que: "Son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquéllos o de éstos, cuando la publicidad afectare el debido cumplimiento de las funciones

(...) en tan sólo una década diversos factores llevaron a un cambio radical. Entre éstos conviene destacar la sentencia de la Corte Interamericana de Derechos Humanos.

(14) Serie C 151, de 19 de septiembre de 2006.

(15) Sentencia del Tribunal Constitucional Rol Nº 634/2006, de 9 de agosto de 2007, considerando 9º.

(16) Ley de Reforma Constitucional Nº 20.050 (D.O. 26.08.2005).

de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional".

Sobre esta base se dictó la LT, que establece el deber de los órganos públicos de publicar en Internet información relevante sobre su gestión (la llamada "Transparencia Activa") y de entregar la demás información que le sea requerida y obre en su poder, salvo que concurran los casos de reserva que detalla en sus artículos 21 y 22. Con todo, la innovación principal es la creación del "Consejo para la Transparencia" (en adelante CPT), organismo encargado de fiscalizar el cumplimiento de las normas sobre transparencia activa y resolver los reclamos en contra de las negativas a las solicitudes de acceso a la información, además de velar porque la administración pública cumpla con la LPDP. Su configuración favorece fuertemente su autonomía efectiva: es una "corporación autónoma de derecho público" (art. 31) que propone al Presidente sus propios "estatutos" (art. 41), cuya dirección y administración superior corresponde a un consejo directivo integrado por 4 consejeros, designados por el Presidente de la República "previo acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio" (art. 36) y que gozan de inamovilidad relativa (art. 38). Todo ello transforma al CPT en una verdadera "administración independiente",[17] facultada para sancionar a subsecretarios y jefes de servicio en general (arts. 45 a 49). El procedimiento de acceso, en tanto, es relativamente ágil y contempla una reclamación de ilegalidad ante la Corte de Apelaciones (arts. 28 y ss.).

(...) la innovación principal es la creación del "Consejo para la Transparencia" (en adelante CPT), organismo encargado de fiscalizar el cumplimiento de las normas sobre transparencia activa y resolver los reclamos en contra de las negativas a las solicitudes de acceso a la información.

Desde la vigencia de la LT, el 20 de abril de 2009, y hasta finalizado el 2010, el CPT ha resuelto cerca de 1.600 casos.[18] Esto que marca un fuerte contraste con el escaso puñado de sentencias judiciales que resolvieron reclamaciones de esta índole en los 10 años de vigencia del sistema de la Ley 19.653.

(17) Véase Enrique Rajevic M., "El Consejo para la Transparencia como «Administración Independiente»", en Raúl Letelier W. y Enrique Rajevic M. (coords.) *Transparencia en la Administración Pública*, Abeledo Perrot, Santiago de Chile, 2010, p. 241-8.

(18) Sobre esto puede verse Enrique Rajevic M., "El primer año de la jurisprudencia del Consejo para la Transparencia". /en/ VV.AA. *Transparencia en el Ámbito Público y Privado. Balance y Desafíos Pendientes.* Santiago de Chile, Chile Transparente, p. 55-71.

IV. La intersección entre la transparencia y la protección de datos personales: Algunos ejemplos y criterios de solución en la jurisprudencia del Consejo para la Transparencia

Definido sucintamente el ámbito de la protección de datos personales y de la transparencia administrativa conviene recordar que ya el artículo 8º de la Constitución reconoce como uno de los límites de la difusión de la información de los órganos del Estado la afectación de los derechos de las personas. La LT señala que entre estos derechos se encuentran los relativos a la seguridad de las personas, su salud, la esfera de su vida privada o derechos de carácter comercial o económico (art. 21 Nº 2). La referencia a la vida privada abre de inmediato campo a la LPDP. Ello es particularmente importante porque el art. 5º de la LT declara que toda la información que obre en poder de los órganos de la administración es pública, mientras su artículo 11, letra a, presume relevante toda información que éstos posean, cualquiera sea su origen o procesamiento. En consecuencia, la carga de la prueba de la reserva le corresponde al titular del derecho afectado que, además, debe ser atribuido por el ordenamiento "…en título de derecho y no de simple interés", conforme el art. 7º Nº 2 del reglamento de la ley.(19)

Para ello el art. 20 establece que los terceros que pudieren ver afectados sus derechos producto de una solicitud de información tienen derecho a ser notificados de ella y a oponerse dentro de tres días, lo que impide su entrega y exige del requirente acudir al CPT si es que desea persistir en la solicitud. Esta parece ser la forma en que debiera operar la causal de reserva del art. 21 Nº 2. Sin embargo, esto no es absoluto. El artículo 21 Nº 5 de la LT establece también el secreto de los "documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política", y su art. 1º transitorio entiende que cumplen con este quórum calificado los preceptos legales vigentes que establecen casos de

(...) los terceros que pudieren ver afectados sus derechos producto de una solicitud de información tienen derecho a ser notificados de ella y a oponerse dentro de tres días, lo que impide su entrega y exige del requirente acudir al CPT si es que desea persistir en la solicitud.

(19) Aprobado por el D.S. N° 13/2009, del Ministerio Secretaría General de la Presidencia (D.O. 13.04.2009).

secreto y son anteriores a la reforma constitucional de 2005 —que exigió ese quórum reforzado— con tal que se ajusten a las causales que señala el artículo 8º de la Constitución Política. En esas condiciones, la reserva que establece el artículo 7º de la LPDP —fundada en los derechos de las personas, como admite la Constitución— es válida y puede ser aplicada directamente.

En materia de transparencia activa la LT establece el deber de publicar en Internet las nóminas de beneficiarios de los programas sociales en ejecución, pero añade que no se incluirán en estos antecedentes los datos sensibles (art. 7º, letra i), criterio que el Consejo extendió a la publicación de actos y resoluciones que tengan efectos sobre terceros en su Instrucción General Nº 4, sobre transparencia activa aplicando directamente la LPDP.(20)

Finalmente, el artículo 33, letra m, encarga al CPT "velar por el adecuado cumplimiento de la Ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado". En esto se siguió la inspiración del *Information Commissioner*, del Reino Unido, que está encargado de fiscalizar el cumplimiento de las leyes de transparencia y protección de datos personales, pero sólo embrionariamente como se desprende del literal citado.

Cerca de la cuarta parte de las decisiones de fondo dictadas por el CPT durante el último trimestre tuvieron que ver con datos personales en mayor o menor medida, esto es, una de cada cuatro, lo que significa que en sede de acceso a la información es relativamente frecuente que deba aplicarse la LPDP.

Dicho esto conviene recordar las reflexiones iniciales de este trabajo que apuntaban a las inevitables tensiones entre el derecho de acceso a la información. La evidencia no hace sino confirmarlo. Cerca de la cuarta parte de las decisiones de fondo dictadas por el CPT durante el último trimestre tuvieron que ver con datos personales en mayor o menor medida, esto es, una de cada cuatro, lo que significa que en sede de acceso a la información es relativamente frecuente que deba aplicarse la LPDP. Algunos casos en los que esto ha ocurrido son los siguientes:(21)

(20) La oración final de su punto 1.7 ordena a los órganos administrativos "…abstenerse de publicar datos personales que tengan carácter reservado conforme a lo establecido en los artículos 7°, 10, 20 y siguientes de la Ley 19.628, de protección de datos de carácter personal" (D.O. 03.02.2010).

(21) Cito las decisiones del CPT según el rol del caso. Su texto puede consultarse en el sitio web del Consejo (http://www.consejotransparencia.cl/).

a) **Protección del Rol Único Tributario (o RUT) y del domicilio:** El RUT es un código numérico creado por el D.F.L. N° 3/1969, ministerio de Justicia (D.O. 15/02/1969), con el fin de identificar "…a todos los contribuyentes del país, de los diversos impuestos, y otras personas o entes que se señalan más adelante" (art. 1°, inc. 1°). En las decisiones A10-09 y A126-09, del 31 de julio de 2009, se rechazó entregar los RUTs de un grupo de funcionarios y ex funcionarios afirmando que éste constituía un dato personal «…cuyo tratamiento sólo puede efectuarse cuando dicha ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello (art. 4° LPDP). En tal carácter, quienes trabajen "en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público" (art. 7° Ley 19.628), esto es, aquéllas de acceso no restringido o reservado a los solicitantes» (considerando 8º). Aplicando el art. 20 de la LPDP se afirmó que «el R.U.T. de los funcionarios es un dato personal obtenido de los propios interesados en acceder a la función pública (art. 13 del Estatuto Administrativo), y no directamente de un registro público, sólo para su tratamiento al interior del servicio público respectivo y no para su cesión a terceros, por lo que debiera ser secreto o reservado». Por otro lado, como el personal de los organismos públicos se informa a través de la nómina de sus nombres en los sitios webs de transparencia activa de cada servicio, como dispone el art. 7° d) de la Ley de Transparencia, la información solicitada se entregó asociándola a los nombres, como dato ya conocido (como también establece el art. 17, letra b, de la Ley 19.880), resolviéndose así la ponderación entre transparencia y protección de datos. Este razonamiento ha sido empleado también respecto del RUT de los particulares y a propósito de los domicilios particulares de los funcionarios (por ejemplo la decisión C446-09).

b) **Sanciones y multas cumplidas o prescritas o con acción prescrita**: En materia de sanciones disciplinarias el Consejo ha aplicado el derecho al olvido del art. 21 LPDP (por ejemplo, los casos C73-10 y C111-10), salvo cuando existe un elevado interés público en el conocimiento de esta información (como ocurrió en las decisiones de los casos C411-09 y

C664-10). Un ejemplo son los resultados de sumarios sanitarios, pues tras el ejercicio de ponderación el Consejo ha estimado que la transparencia debe prevalecer sobre la protección de los datos personales.

c) **Datos relativos a los procesos de calificación o al cumplimiento de jornada de los funcionarios públicos:** Si bien se trata de datos personales el CPT ha entendido que al ser información elaborada con fondos públicos es, en principio, de acceso público, conforme al art. 5º LT, lo que se confirma al no haber una verdadera afectación de derechos dado que "…los funcionarios públicos poseen una esfera de vida privada más delimitada en virtud precisamente de la función que ejercen" (decisión A47-09, considerando 12°). En el mismo sentido se ha dicho que si las remuneraciones de los funcionarios son públicas en virtud del art. 7º, letra d, de la LT, e incluso objeto de transparencia activa —publicación en Internet—, también deben ser públicos los registros de control de asistencia, añadiendo que han sido producidos en el ejercicio de una función pública y que su conocimiento es relevante para el adecuado control social de aquella, lo que refuerza el art. 30 de la Ley 19.733 o Ley de Prensa al calificar como hechos de interés público los referentes al desempeño de funciones públicas (decisiones de los amparos A181-09, C434-09, C485-09, C492-09, C209-10 y C846-10). En consecuencia, en este caso la ponderación se resuelve a favor de la transparencia.

d) **Datos personales relativos a concursos públicos de personal:** En materia de concursos la ponderación ha llevado a una serie de distinciones, prevaleciendo en algunos casos el derecho de acceso y en otros la protección de los datos, si bien en estricto rigor estos últimos son resguardados como una exigencia para el debido funcionamiento de los sistemas de concurso y no en virtud de la LPDP. Así, el Consejo admite la solicitud de puntajes propios y de terceros, siempre que la identidad de estos últimos sea previamente conocida (en caso contrario debe aplicarse el art. 20 LT), pero no ha aceptado entregar los informes psicolaborales ni tampoco las referencias dadas por terceros por entender que ello afectaría sustantivamente el debido funcionamiento de los sistemas de reclutamiento. Con todo, tratándose de los candidatos designados para el

cargo últimamente el Consejo ha aceptado entregar tales informes en los concursos de alta dirección pública, afirmando que en tales cargos hay un alto interés público que supone un estándar de escrutinio ante el que debe ceder la privacidad (como en el caso de la decisión A336-10). Cabe señalar que en lo relacionado con los concursos de la Alta Dirección Pública la Dirección Nacional del Servicio Civil ha defendido el secreto de los procesos y los candidatos, fundada en los artículos 50º y 55º de la Ley 19.882 y reclamando la ilegalidad de las decisiones del Consejo. A la fecha existen dos sentencias de la Corte de Apelaciones de Santiago, una acogiendo y otra rechazando.[22]

e) **Datos sensibles:** El CPT ha declarado la reserva de datos relativos a la salud de las personas (p. ej., decisiones A211-09 y C240-10) y su militancia política (A152-09). Acá, en consecuencia, no se ha ponderado acceso con protección sino que ha prevalecido directamente la protección de los datos.

f) **Padrón Electoral:** En su decisión C407-09 el Consejo validó la entrega del padrón electoral del Servicio Electoral debido a que la Ley 18.556, orgánica constitucional del Sistema Electoral, prescribe categóricamente que los registros electorales deben ser públicos y que en base a ellos el Servicio Electoral elabora su padrón computacional. Si bien esta ley se aplicó por sobre la LPDP[23] también según esta última podría entenderse que no era confidencial, en tanto información contenida en una fuente accesible al público (art. 7º LPDP).[24] También el Consejo valoró que el control social del padrón electoral permitiría verificar que no existan inscripciones duplicadas (lo que incluso justifica en este caso entregar el RUT). Aunque se llegó a este resultado el Consejo sopesó también la afectación de los datos personales y admitió explícitamente su preocupación por la difusión resultante, para terminar afirmando que ante

(22) Se trata de las sentencias roles 943-2010, de 03/09/2010, y 2080-2010, de 22/11/2010, ambas de la cuarta sala y la última, recurrida de queja.

(23) La decisión da a entender que se trata de un tema de jerarquía normativa. En mi opinión se trataría de un problema de competencia de las normas, esto es, el acceso al padrón electoral sería una materia orgánica constitucional vedada a la regulación de la ley simple.

(24) Aunque en tal caso debiese haberse reservado la condición de invidencia, lo que no se hizo.

la claridad de la Ley 18.556, "…corresponde a los órganos colegisladores y no a este Consejo resolver, a futuro, si es preciso modificar este estado de cosas".[25]

g) **Personas Jurídicas:** El Consejo ha desconocido la protección de datos personales relativos a personas jurídicas por aplicación de la LPDP, que las excluye (por ejemplo, decisiones A39-09 y A309-09), pero ha reservado datos relativos a éstas fundándose en otros derechos por aplicación del art. 21 Nº 2 LT (p. ej., decisión A265-09) en otro ejercicio de ponderación.

h) **Ejercicio del derecho de acceso a datos personales en poder de la Administración Pública a través de la LT:** Por último, y para cerrar esta breve recapitulación, el CPT ha admitido que los titulares de datos personales puedan requerirlos a través de los mecanismos de la LT y no sólo mediante el *habeas data* regulado por la LPDP, de manera que se trataría de mecanismos alternativos para obtener el mismo propósito. Así ha ocurrido con datos relativos a concursos, solicitud de indultos, procedimientos administrativos, etcétera (como las decisiones C178-10 y C426-10).

Creo que los casos anteriores son suficientemente ilustradores de la importancia que tiene la LPDP en la tarea que realiza el CPT. Probablemente se trata del organismo público que ha debido darle una aplicación más intensiva, al punto que esté estudiando la elaboración de una recomendación sobre esta materia. En los casos que hemos revisado el CPT valora los datos personales como una posible excepción a la transparencia administrativa, siguiendo la lógica del art. 8º de la Constitución y el art. 21 de la Ley de Transpa-

Creo que los casos anteriores son suficientemente ilustradores de la importancia que tiene la LPDP en la tarea que realiza el CPT. Probablemente se trata del organismo público que ha debido darle una aplicación más intensiva, al punto que esté estudiando la elaboración de una recomendación sobre esta materia.

(25) Hay una disidencia del Consejero y entonces Presidente Juan Pablo Olmedo, quien aplicando el principio de finalidad postuló que el padrón computacional sólo podía entregarse suprimiendo la profesión, fecha de nacimiento, domicilio, RUT e indicación de la condición de no vidente o analfabeto de las personas inscritas.

rencia. Existen otros ordenamientos que invierten la regla, de manera que si la información solicitada a la Administración puede afectar la privacidad de una persona se entiende que es reservada, debiendo el solicitante acreditar la existencia de un interés público que justificase su revelación.(26)

No obstante, para evaluar la procedencia o improcedencia de las causales de reserva invocadas, el CPT ha aplicado numerosas veces un test de daño (decisión A45-09, del 28 de julio de 2009, considerandos 8º a 11º) y un test de interés público (decisión A115-09, del 22 de agosto de 2009, considerandos 11º y 12º): "Ambos, que pueden ser complementarios, consisten en realizar un balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación. El primero se centra en ponderar si la divulgación puede generar un daño presente, probable y específico a los intereses o valores protegidos de mayor entidad que los beneficios obtenidos; el segundo, en ponderar si el interés público a obtener con la entrega de la información justifica su divulgación y vence, con ello, la reserva" (decisión C193-10). Se trata de un ejercicio de ponderación de derechos, como se dijo en la decisión A45-09, que exige respetar el principio de proporcionalidad y el contenido esencial de uno y otro derecho.(27)

(26) Por ejemplo, la Privacy Act canadiense, en vigor desde el 1º de julio de 1983, parte del principio de la reserva de los datos personales y permite en su art. 8 que puedan comunicarse a terceros sin consentimiento del titular sólo en casos excepcionales, uno de los cuales es que, en opinión del jefe de la institución, *"(i) el interés público en la divulgación sea claramente mayor que el perjuicio a la privacidad que podría generarse, o (ii) la divulgación beneficie claramente a la persona a quien se refiere la información"* (art. 8.2.m). A este respecto se ha dicho que "…la discrecionalidad en el otorgamiento a la Administración de la potestad para otorgar o no el acceso a la información es aquí doble: la ley de protección de datos deja la decisión al juicio del responsable de la institución, y la Ley de Acceso, como dijimos, establece, en general, que en los casos de comunicaciones inconsentidas conforme al artículo 8 de la Ley de Protección de Datos [*Privacy Act*] el acceso puede (o no) acordarse. Se trata de un supuesto que requiere un aquilatado juicio ponderativo para el que la Administración goza de un importante margen de discrecionalidad". Emilio Guichot R. Publicidad y privacidad de la información administrativa. Madrid: Civitas, 2009, p. 36.

(27) Su considerando 10º señala que: ["...Establecido que estamos en presencia de un derecho de rango constitucional la reserva o secreto pasa a limitarlo o restringirlo, por lo que debe respetar el principio de proporcionalidad que supone analizar, conforme señala la doctrina: a) si la medida es eficaz, b) si no existe un medio más moderado para la consecución eficaz del propósito buscado (en este caso, cautelar el secreto) y, por último, c) si de la medida a adoptar (en este caso, el secreto absoluto) derivan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (véase BERNAL P., Carlos. El principio de proporcionalidad y los derechos fundamentales, 2ª ed. Madrid: Centro de Estudios Políticos y Constitucionales, 2005, y GARCÍA P., Gonzalo y CONTRERAS V., Pablo. Derecho de Acceso a la Información en Chile: Nueva Regulación e Implicancias para el Sector de la Defensa Nacional. /en/ Estudios Constitucionales año 7, N° 1, 2009, p. 144)". En términos semejantes nuestro Tribunal Constitucional ha dicho sobre este principio lo siguiente: "Reiterando nuestra jurisprudencia constitucional anterior (Sentencia Rol N° 226, Considerando 47, y Sentencia Rol Nº 280, Considerando 29), una limitación a un derecho fundamental es justificable cuando dicho mecanismo es el estrictamente necesario o conveniente para lograr un objetivo constitucionalmente válido, debiendo consecuentemente el legislador elegir aquellas limitaciones que impliquen gravar en menor forma los derechos fundamentales" (Sentencia Rol N° 519/2006, de 5 de junio de 2007, consid. 19°)"].

V. Conclusiones

Del análisis realizado se desprende con claridad que la protección de datos personales y la transparencia son desarrollos de derechos fundamentales que se proyectan sobre un mismo objeto: la información que está a disposición de los organismos públicos. De allí que se haya dicho que sean dos caras de una misma moneda.

Del análisis realizado se desprende con claridad que la protección de datos personales y la transparencia son desarrollos de derechos fundamentales que se proyectan sobre un mismo objeto: la información que está a disposición de los organismos públicos.

Lo anterior exige que necesariamente deban armonizarse a través del mecanismo de la ponderación de derechos, para lo cual existen distintos enfoques y soluciones institucionales en el derecho comparado, desde las que promueven una sola entidad a cargo de ambos temas, como el Information Commissioner Office (ICO) en Reino Unido —que es el modelo que se propuso en el proyecto de ley discutido en la Cámara de Diputados[28]—, o el Instituto Federal de Acceso a la Información (IFAI) mexicano, hasta los que auspician la existencia de dos órganos perfectamente diferenciados, como ocurre en Canadá y Francia. En cualquier modelo es clave la autonomía e independencia de esta autoridad.[29] De seguir Chile la primera alternativa sería precisa una profunda reorganización del CPT (acompañada de los medios necesarios) y/o una reorientación en las capacidades de su personal, que le permitiera actuar eficazmente en el ámbito de la protección de datos en poder de agentes privados, ámbito que cuantitativamente es más significativo que el de los datos en poder del Estado.[30] Optar por la creación

(28) En el marco de la tramitación del proyecto de ley que introduce modificaciones a la Ley 19.628 y a la ley N° 20.285 (Boletín N° 6120-07), actualmente en primer trámite constitucional, que transforma al CPT en el "Consejo para la Transparencia y Protección de Datos Personales".

(29) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOUE L 281, de 23.11.1995), exige en su art. 28 Nº 1 que las autoridades encargadas de controlar la aplicación de las disposiciones sobre protección de datos personales ejerzan las funciones que les son atribuidas "…con total independencia", cuestión que "constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales" (considerando 62 de la directiva).

(30) Pueden verse críticas a esta opción en Renato Jijena L. "Transparencia, no Datos Personales", en La Tercera 29/06/2010 (http://latercera.com/contenido/895_271915_9.shtml). Dicha columna responde a una anterior de Juan Enrique Vargas V., que defiende la opción del CPT: "Transparencia y Datos Personales", en La Tercera 29/06/2010 (http://diario.latercera.com/2010/06/21/01/contenido/7_30413_9.shtml).

de un nuevo organismo a cargo de la protección de datos requeriría generar mecanismos para resolver posibles conflictos competenciales con el CPT. Sería indeseable que finalmente éstos escalaran a los tribunales, pues en tal caso se arriesgaría buena parte de la eficacia del modelo. Sin embargo, es inevitable que al final de la jornada existan muchos casos en que la resolución del problema de acceso a la información o *habeas data* en el ámbito de la administración pública requiera de una ponderación conjunta entre el derecho de acceso a la información pública y el derecho a la autodeterminación informativa. Si no tenemos una instancia administrativa única que lo haga, deberemos entregarle esta misión al Poder Judicial.

(...) al margen de la discusión acerca del organismo encargado de esta tarea hay numerosos otros aspectos regulatorios que requieren de un perfeccionamiento, de manera que los ciudadanos tengan un control efectivo de sus datos y no sean "capturados" junto con ellos.

Otra conclusión nada de novedosa es que es preciso mejorar a la brevedad los estándares de la protección de datos personales en Chile. El ejemplo del CPT sugiere que la creación de una institución para la protección de datos, o la asignación de esta tarea al CPT, contribuiría notablemente a la difusión e implantación efectiva del derecho a la autodeterminación informativa. Probablemente también experimentaríamos una verdadera eclosión de este derecho, al modo de la vivida por el derecho de acceso a la información desde abril de 2008. Sin embargo, al margen de la discusión acerca del organismo encargado de esta tarea hay numerosos otros aspectos regulatorios que requieren de un perfeccionamiento, de manera que los ciudadanos tengan un control efectivo de sus datos y no sean "capturados" junto con ellos.

Autor

Enrique Rajevic Mosler

Máster en Política Territorial y Urbanística, Profesor de Derecho Administrativo de la Universidad Alberto Hurtado y Director Jurídico del Consejo para la Transparencia.

XI
Brazaletes telemáticos, régimen penitenciario y principios de protección de datos

Carlos Reusser Monsálvez

I. Introducción

Desde hace algún tiempo, y con mucha fuerza tras una serie de tragedias vividas en el ámbito carcelario, se viene propugnando en Chile la idea de implementar la utilización de dispositivos de vigilancia o control a distancia que, usualmente, adoptan la forma de brazaletes o grilletes electrónicos adheridos al cuerpo de las personas, ya sea como medida alternativa a la privación de libertad, opción al procesamiento penal, beneficio penitenciario e incluso como pena.

La promoción de tal idea se deriva de la convicción social de que cuando internamos a las personas en recintos penales lo único que podemos asegurar es que al salir éstas serán más peligrosas que antes y tendrán menos habilidades para su reinserción social. Por supuesto, es de esperar que lo anterior quede demostrado cuando cometan un nuevo delito, en ese momento —aparte de cuestionar al Estado por el fracaso de las políticas públicas de resocialización— la ciudadanía abogará porque el victimario sea internado otra vez en la cárcel para así comenzar una vez más a repetir el ciclo.

(...) el sistema penitenciario está tan enfermo que hace vanos los esfuerzos de resocialización, lo que deriva tanto en el hacinamiento extremo por sobrepoblación carcelaria, como en el cultivo de malos hábitos entre los internos (y sus carceleros), además de la "profesionalización" del delincuente tras los muros de las prisiones.

Ignoro las razones de por qué como sociedad hemos permitido que esta esquizofrenia siga adelante, pero lo que sí tengo claro es que se trata de un círculo carente de sentido y que una de las vías de solución puede ser, perfectamente, el uso de la tecnología en pos de humanizar las lógicas penitenciarias, adecuando los castigos a los requerimientos de la comunidad con el fin de que éstos sean eficaces y, sobre todo, útiles.[1] Esto, sin perder de vista que el sistema penitenciario está tan enfermo que hace vanos los esfuerzos de resocialización, lo que deriva

(1) Hay que tener presente que muchas veces las penas que son útiles a la comunidad social son contrarias a la pretensión punitiva del Estado. Así lo ejemplificó con el siguiente caso el profesor Francisco Muñoz Conde en una reciente conferencia que dictó en nuestro país: en un villorrio indígena de México, durante una borrachera, una persona mató a su amigo de toda la vida. Constituido el pueblo en tribunal condenó al homicida a hacerse cargo de la manutención de la mujer e hijos del amigo, pero el Estado no quedó conforme, invalidó al tribunal y lo llevó a la justicia ordinaria que le encarceló por 30 años, sentenciando en la práctica a la miseria a la mujer e hijos del imputado y también a toda la familia del asesinado.

tanto en el hacinamiento extremo por sobrepoblación carcelaria, como en el cultivo de malos hábitos entre los internos (y sus carceleros), además de la "profesionalización" del delincuente tras los muros de las prisiones.

Sin embargo, gracias a la tecnociencia y sus aplicaciones penitenciarias —desarrolladas primero en base a radiofrecuencias y ahora también a partir de sistemas de posicionamiento global (GPS)— es posible que hoy nos planteemos la idea de hacer desaparecer las murallas de las cárceles y que las condenas se cumplan fuera de éstas, mediante un régimen de control y vigilancia desarrollado a través de grilletes electrónicos.

(...) gracias a la tecnociencia y sus aplicaciones penitenciarias —desarrolladas primero en base a radiofrecuencias y ahora también a partir de sistemas de posicionamiento global (GPS)— es posible que hoy nos planteemos la idea de hacer desaparecer las murallas de las cárceles (...)

El uso de estos dispositivos telemáticos tiene múltiples ventajas: su portador puede permanecer con la familia, no pierde el trabajo, no sufre estigmatización por estar en la cárcel ni pierde oportunidades laborales, se mantiene alejado de un ambiente cimentado sobre el odio hacia la sociedad, se evita la profesionalización del delincuente y, por último, se le da una cama donde dormir y ciertas seguridades respecto de que no será apuñalado o quemado vivo, bastante más de lo que puede ofrecer hoy nuestro sistema penitenciario. A todo esto se suma el interés del Estado de reducir costos y aminorar los cuestionamientos a los resultados de su política criminal y penitenciaria.

Sin embargo, en Chile antes de decidir sobre el uso de estos dispositivos debemos examinar y remodelar nuestro sistema jurídico, de forma tal que haga efectivamente posible la reinserción dentro de un marco de libertades y derechos, velando porque no sólo se convierta a las personas en una especie de perro con un collar de GPS que nos permita saber siempre dónde se encuentra, de modo que no se nos pierda y de asegurarnos que no está haciendo "travesuras".

Con el paso del tiempo las tecnologías han ido complejizando los dispositivos telemáticos, los que hoy no son sólo capaces de informar en qué lugar específico del planeta se ubica una persona, sino que además han ido incorporando elementos de análisis del sudor, frecuencia cardiaca, tono de voz,

consumo de alcohol, uso de drogas, etcétera, convirtiendo a los individuos en unidades de transmisión de datos personales procesados para el poder público.(2) Esto, en el fondo, es el sueño dorado del Estado totalitario y el santo grial de la policía y las compañías de seguros, pues si el conocimiento es poder éste se incrementa cuando controlamos lo más íntimo y reservado de cada habitante.

Ante dicha realidad, y en nuestro rol de ciudadanos, junto con alegrarnos de que el progreso tecnocientífico abra mayores oportunidades y posibilidades en el ámbito penitenciario, debemos ocuparnos de que el Derecho construya el marco adecuado para la protección de los datos personales, garantía de todos los demás derechos. A su vez tenemos que velar porque el Estado no se constituya en el *Panopticón* de Bentham,(3) esto, es el lugar en el cual quienes detentan el poder lo ven todo aunque nadie pueda verlos a ellos.

II. Desarrollo

A estas alturas está perfectamente claro que la información que transmiten los brazaletes electrónicos respecto del portador y su entorno tiene el carácter de personal, pues corresponde a personas identificadas (sus portadores) o fácilmente identificables (su medio), cuyos datos son objeto de tratamiento, en último término, bajo responsabilidad del Estado, ya sea que éste efectúe el tratamiento por sí mismo o que haya abierto el mercado para dar cabida a prestadores de servicios de tratamiento.

(...) está perfectamente claro que la información que transmiten los brazaletes electrónicos respecto del portador y su entorno tiene el carácter de personal, pues corresponde a personas identificadas (sus portadores) o fácilmente identificables (su medio) (...)

(2) Podría pensarse que para evitar estos riesgos de abuso bastaría que no se utilizaran en las personas los dispositivos más complejos sino sólo los que revelen posición (que también llevan aparejados problemas), pero la verdad es que estamos en la noche de las libertades en la que el Estado quiere saberlo todo olvidándose de los límites. Basta recordar que para el poder público los mapuches ya no son un pueblo originario sino que un grupo terrorista, los estudiantes que protestan lanzando una *molotov* en la calle "afectan la seguridad interior del Estado", se juzga a los menores de edad en tribunales penales y si alguien interrumpe la canción nacional se le aplica la ley de seguridad interior del Estado. Todos somos sospechosos y debemos ser vigilados.

(3) La idea del *Panopticón* y su aplicación al diseño de las prisiones ha sido extensamente abordada por Michel Foucault, en su ya célebre *Vigilar y Castigar. Nacimiento de la prisión*, publicado por diversas editoriales, entre ellas la mexicana Siglo XXI en 1984 con sucesivas reimpresiones.

Esta situación global debe revisarse a la luz de los principios internacionales de protección de datos, particularmente los fijados en la Resolución de Madrid de 2009. En ellos se señala que el tratamiento de datos —en este caso los vinculados a dispositivos telemáticos de control o vigilancia en el ámbito penitenciario— debe ser legitimado a través de diversas causas, como que éstos sean necesarios para el cumplimiento de una obligación impuesta por la legislación nacional o que ocurran circunstancias que ponen en peligro la vida, la salud o la seguridad del portador del grillete o de otra persona, tal es el típico ejemplo de las órdenes de alejamiento por amenazas graves o violencia intrafamiliar.

Es evidente, además, que la información obtenida a partir de estos dispositivos puede ser calificada como datos sensibles, es decir, aquellos que precisan medidas especiales de protección, pues aparte de que pueden afectar la esfera más íntima de las personas la información que se conoce a través de ellos podría dar origen a discriminaciones ilegales o arbitrarias del entorno social.(4)

Entonces, tenemos que de acuerdo a los principios generales de protección de datos existen deberes de lealtad, legalidad y respeto a los derechos y libertades de las personas, pero ¿de qué personas estamos hablando? Nos referimos no sólo al portador del dispositivo telemático, sino que a todo su entorno familiar y social, pues en la práctica se está procesando y relacionando información atingente a todos ellos: fechas, lugares, comportamientos, alzas de presión sanguínea, esfuerzo, etcétera. Lo anterior tiene consecuencias jurídicas, ya que si bien el grillete lo lleva sólo una persona, habiendo fundamento legal para ello, el entorno —al menos el más cercano— no tiene obligaciones de soportar carga alguna, lo que nos conduce a pensar que se deberá obtener su consentimiento expreso para el tratamiento de la información.

(...) de acuerdo a los principios generales de protección de datos existen deberes de lealtad, legalidad y respeto a los derechos y libertades de las personas, pero ¿de qué personas estamos hablando?

Un poco más problemático es analizar que se cumplan los fines para los que se fijó la sanción de cargar con un dispositivo telemático, pues el procesamiento de datos incompatibles con los fines perseguidos también requerirá de consentimiento expreso. Es decir, no podrían utilizarse los datos obtenidos a través de estos medios para iniciar investigaciones criminales o de otra especie

(4) Ello dejando completamente de lado todo el tema de la estigmatización y discriminación resultante del mero hecho de cargar un brazalete electrónico e incluso los riesgos graves de ataques físicos o linchamientos por parte de la ciudadanía.

respecto de personas distintas a las directamente controladas o vigiladas, a menos que se tome el camino de la autorización explícita, aunque tengo serias dudas sobre la real autonomía de la voluntad cuando se trata de privaciones de la libertad, sin perjuicio de las autorizaciones judiciales necesarias, pues de alguna forma los dispositivos telemáticos son también sistemas de "escucha".

Hay que agregar que es evidente también la existencia de problemas con el principio de proporcionalidad, pues se debe velar porque los datos en cuestión sean adecuados, relevantes y no excesivos. Así, por ejemplo, si la sanción implica cumplir con arresto domiciliario nocturno, como sería la obligación de permanecer en casa todos los días de 21:00 horas a las 07:00 horas del día siguiente, cabe preguntarse ¿con qué fin se mantiene vigilado al sujeto el resto del día? Por otro lado, si lo que existe es una orden de alejamiento ¿para qué se consignan los datos de la actividad física del portador del brazalete?

Incluso, la información relativa a la ubicación física de una persona puede tornarse desproporcionada respecto de los fines que se persiguen, lo que trae como consecuencia que el Estado deba realizar los ajustes pertinentes para reducir los datos personales al mínimo necesario, pues no hay que olvidar que los métodos electrónicos de vigilancia inciden en el retroceso o merma de los derechos fundamentales como la identidad, la libertad de asociación, de reunión, de práctica de convicciones religiosas y, sobre todo, de dignidad.

En cuanto a la revisión del efectivo cumplimiento del principio de calidad, ésta nos lleva a cuestionarnos cuánto tiempo puede conservar el Estado los datos transmitidos por estos dispositivos, ¿un mes, un año, a perpetuidad?

La tendencia de los Estados, y sus agresivas concepciones sobre la seguridad pública, los lleva a adjudicarse facultades de conservación que van mucho más allá de las finalidades que en un principio se persiguieron al someter a un individuo a vigilancia y control a distancia. Esto nos conduce a fortalecer la idea de que una vez que se hayan cumplido las penas que dieron origen a la sanción, los datos obtenidos deberían ser anulados o bien convertidos en información anónima.

La tendencia de los Estados, y sus agresivas concepciones sobre la seguridad pública, los lleva a adjudicarse facultades de conservación que van mucho más allá de las finalidades que en un principio se persiguieron al someter a un individuo a vigilancia y control a distancia.

Sobre el deber o principio de transparencia, cabe señalar que los dispositivos telemáticos tienen que ser regulados por ley, pues imponen restriccio-

nes de derechos constitucionales (algunos de ellos de carácter fundamental), lo que implica que el Estado debe procurar a las personas toda la información que sea necesaria para garantizar y vigilar el adecuado tratamiento de los datos personales, a la vez que se delimitan los grados de responsabilidad entre los diferentes intervinientes en el proceso de tratamiento de datos personales, estableciendo mecanismos concretos que permitan corregir situaciones fuera de la ley y todo lo relativo al efectivo ejercicio de los derechos de acceso, rectificación, oposición y cancelación, la única manera de entender la vigencia de estos principios.

(...) el Estado debe procurar a las personas toda la información que sea necesaria para garantizar y vigilar el adecuado tratamiento de los datos personales (...)

III. Conclusiones

No pretendo sostener aquí que no deban buscarse soluciones alternativas a la cárcel, sí estimo que los análisis que hay que hacer frente a una solución tecnológica no pasan simplemente por decidir si ésta se utilizará o no, pues por un lado tenemos la prisión —con el trato cruel, inhumano y degradante que está a la orden del día en nuestro país— y, por otro, está la imperiosa necesidad de poner remedio a esa situación haciéndola evolucionar hacia la reinserción social de quienes infringen la ley.

De hecho, el uso de dispositivos electrónicos se ha mostrado especialmente útil para verificar el cumplimiento de determinadas obligaciones, como el no beber alcohol, no acercarse a determinados lugares o personas, no alejarse de ciertos perímetros y, en general, todo lo que apunte a restringir la libertad ambulatoria de las personas, como en los casos de arresto domiciliario.

Sin embargo, lo expuesto no nos debe conducir a olvidar que, tal como afirma Luigi Ferrajoli, el teórico del garantismo jurídico, la historia de las penas es más horrenda e infamante para la humanidad que los propios delitos que les dieron causa. Así, no creo que controlar los datos referidos a las actividades de una persona las 24 horas del día vaya en la dirección correcta, pues una cosa es usar el Derecho en función de la resocialización y otra diferente es emplearlo como instrumento de dominación del cuerpo social.

Nuestro real desafío es entonces construir un sistema de garantías centrado en la protección de datos que obstaculice los abusos, pues lo que hay que tener presente es que detrás de los aparatos telemáticos no está sólo la idea de conocer el posicionamiento de un sujeto sobre el planeta, sino que se encuentra el procesamiento automatizado de una ingente cantidad de datos personales. En la medida en que estos mecanismos se le van instalando a más personas alteran el equilibrio de los poderes sociales, al obtener información sobre: hábitos diurnos y nocturnos, preferencias, identidad sexual, consumo de alcohol, estados de excitación, relaciones familiares y afectivas, entre otras, todas cuestiones que estarán a disposición y pueden ser usadas por el Estado en nombre del orden y de la seguridad pública.

(...) lo que hay que tener presente es que detrás de los aparatos telemáticos no está sólo la idea de conocer el posicionamiento de un sujeto sobre el planeta, sino que se encuentra el procesamiento automatizado de una ingente cantidad de datos personales.

Finalmente, para cerrar esta reflexión me parece conveniente recordar a Benjamín Franklin: "Aquellos que sacrifican una libertad imprescindible para conseguir una seguridad temporal no merecen ni la libertad ni la seguridad", frase que ilustra que la pretensión de protegernos contra la delincuencia no puede conducirnos a vulnerar los derechos fundamentales de los demás, ni a mutilar nuestras propias garantías.

Referencias

- LEAL, CÉSAR. *La Vigilancia Electrónica a Distancia. Instrumento de control y alternativa a la prisión en América Latina*. Porrúa, Ciudad de México (México), 2010.
- RODRÍGUEZ-MAGARIÑOS, FAUSTINO. *Cárcel Electrónica. Bases para la creación del sistema penitenciario del siglo XXI*. Tirant lo Blanch, Valencia (España), 2007.
- GUDIN RODRÍGUEZ-MAGARIÑOS, FAUSTINO. *Sistema Penitenciario y Revolución Telemática: ¿El fin de los muros en las prisiones? Un análisis desde la perspectiva del Derecho comparado*. Slovento, Madrid (España), 2005.
- OTERO GONZÁLEZ, PILAR. *Control Telemático de Penados. Análisis jurídico, económico y social*. Tirant lo Blanch, Valencia (España), 2008.
- TIRADO SERRANO, FRANCISCO; DOMÉNECH I ARGEMÍ, MIQUEL (editores). *Lo Social y lo Virtual. Nuevas formas de control y transformación social*. Editorial UOC, Barcelona (España), 2006.
- VEGA ALOCÉN, MANUEL. *El Tercer Grado con Control Telemático*. Comares, Granada (España), 2010.

Autor

Carlos Reusser Monsálvez

Máster en Informática y Derecho de la Universidad Complutense de Madrid y Especialista en Derechos Humanos de la misma Universidad. Experto en Gestión del Conocimiento de la Universidad Carlos III de Madrid. Diplomado en Derecho Informático y Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile. Consejero del Instituto Chileno de Derecho y Tecnologías y académico de la Universidad Central de Chile.

XII
El derecho a la protección de datos de los adolescentes infractores de la ley penal

Francisco Trejo Ortega

I. El adolescente infractor de la ley penal

La Ley 20.084 fue promulgada el 28 de noviembre del 2005 y publicada el 7 de diciembre del mismo año, pero por una postergación legal finalmente entró en vigencia el 8 de junio de 2007, instaurando así un sistema de responsabilidad para los adolescentes mayores de 14 y menores de 18 años de edad que quebranten la ley penal.

Si bien el cuerpo legal en cuestión establece responsabilidades penales para este segmento etario, es importante señalar que esta ley inaugura un nuevo sistema, el que implica un cambio de mentalidad íntimamente ligado al principio de "interés superior del niño", que establece y guía la Convención de los Derechos del Niño y que dicha norma denominó "interés superior del adolescente". Este principio se manifiesta a lo largo de todo el texto legal y, en especial, dispone que: "En todas las actuaciones judiciales o administrativas relativas a los procedimientos, sanciones y medidas aplicables a los adolescentes infractores de la ley penal se deberá tener en consideración el interés superior del adolescente, que se expresa en el reconocimiento y respeto de sus derechos".(1) En este punto, dicho principio pasa a ser no sólo una declaración de intenciones sino que se manifiesta, por ejemplo, imponiendo a las instituciones que participan del circuito penal determinadas obligaciones, tales como el deber de "los jueces de garantía, los jueces del tribunal de juicio oral en lo penal, así como los fiscales adjuntos y los defensores penales públicos que intervengan en las causas de adolescentes, de capacitarse en estudios e información criminológica vinculada a la ocurrencia de estas infracciones, en la Convención de los Derechos del Niño, en las características y especificidades de la etapa adolescente y en el sistema de ejecución de sanciones establecido en esta misma ley".(2) De la misma forma, similar regla se aplica a las policías al señalarse que: "Las insti-

Si bien el cuerpo legal en cuestión establece responsabilidades penales para este segmento etario, es importante señalar que esta ley inaugura un nuevo sistema, el que implica un cambio de mentalidad.

(1) Art. 2° Ley 20.084.

(2) Art. 29 de la Ley 20.084.

tuciones policiales incorporarán dentro de sus programas de formación y perfeccionamiento, los estudios necesarios para que los agentes policiales cuenten con los conocimientos relativos a los objetivos y contenidos de la presente ley, a la Convención de los Derechos del Niño y a los fenómenos criminológicos asociados a la ocurrencia de estas infracciones".(3) Como se evidencia, existe un adecuado razonamiento de inculcar en los actores del circuito penal los fundamentos e inspiración del nuevo sistema.

Además, la Ley 20.084 se plantea como un objetivo matriz la reinserción social de los jóvenes, para lo cual, entre otras cosas, establece una serie de programas especiales de reinserción, crea nuevos procedimientos, pone fin al trámite del discernimiento, y fija la responsabilidad penal de los mayores de 14 años y menores de 18 años.

En términos generales, esta normativa contempló dos grandes clases de sanciones, las privativas de libertad y las no privativas de libertad, en sustitución de las penas contempladas en el Código Penal y en las leyes complementarias.

En términos generales, esta normativa contempló dos grandes clases de sanciones, las privativas de libertad y las no privativas de libertad, en sustitución de las penas contempladas en el Código Penal y en las leyes complementarias. Igualmente, este cuerpo legal otorga la posibilidad de aplicar sanciones mixtas.

Para observar el alcance de la Ley 20.084 en términos numéricos, podemos decir que al segundo trimestre del 2010 un total de 12.365 adolescentes eran sujetos de alguna sanción contemplada en ella, de los cuales 1.127 eran mujeres y 11.238 hombres.(4)

II. Los datos personales de los adolescentes infractores de la ley penal

Constituyen datos de carácter personal o datos personales "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables".(5) Como una especie de ellos, encontramos a los denominados

(3) Art. 30 de la Ley 20.084.

(4) Boletines Estadísticos, Servicio Nacional de Menores.

(5) Art. 2º Ley 19.628, letra f).

"datos sensibles", que corresponden a "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".(6)

Habiendo aclarado esta definición y frente a la realidad de la protección de los datos de las personas en nuestro país, cabe preguntarse ¿cuál será entonces la naturaleza de los datos de los adolescentes infractores de ley y qué problemas se derivan a partir del manejo de esta información?

Al igual que cualquier individuo, en la información derivada de los datos de estos adolescentes coexisten ambas categorías, vale decir, el dato personal "simple" y el "dato sensible".

Al igual que cualquier individuo, en la información derivada de los datos de estos adolescentes coexisten ambas categorías, vale decir, el dato personal "simple" y el "dato sensible". El problema radicará en el "tratamiento" de dichos datos y en la complejidad adicional de sopesar distintos bienes jurídicos.

Pensemos en un menor condenado por el delito de violación, este hecho implicará que en el tratamiento de su información la autoridad tendrá un conocimiento sobre su "vida sexual". Así también, un determinado delito puede mostrar si hay alguna "ideología" que motivó al menor a cometerlo, o bien, un adolescente afectado por una enfermedad de trasmisión sexual llevará necesariamente a conocer su "estado de salud" y hará a la autoridad tomar ciertos resguardos sanitarios, ya sea en cuanto a su custodia o bien en lo que es particularmente relevante en este trabajo, el registro de dicha información en sus bancos de datos (información clínica).

Ahora bien, pese a que estos jóvenes han cometido un delito, como personas poseen los mismos derechos que cualquier individuo en relación con su autodeterminación informativa, es decir, tienen los mismos derechos comunes que son: el derecho de acceso o información, derecho de modificación o rectificación, derecho de bloqueo, y derecho de cancelación o eliminación, volveremos más adelante sobre éstos y su ejercicio. Ahora bien, cada caso habrá de ser sopesado en su justa medida por las razones obvias del mismo.

(6) Art. 2º Ley 19.628, letra g).

Legitimación de la autoridad administrativa para tratar datos personales de adolescentes infractores de ley penal (condenados)

Según lo establece la ley, uno de los organismos encargados de realizar el tratamiento de los datos de los adolescentes que infrinjan la ley penal es el Servicio Nacional de Menores (SENAME). Esta entidad, entre otras cosas, ha sido concebida como la encargada de contribuir a proteger y promover los derechos de los niños, niñas y adolescentes que han sido vulnerados en el ejercicio de los mismos, encargándose también de la reinserción social de los adolescentes infractores de la ley penal.(7) En lo que respecta a esta última función, la reinserción, se manifiesta en "dirigir especialmente su acción a los adolescentes imputados de haber cometido una infracción a la ley penal, incluyéndose en éstos a aquellos sujetos a una medida privativa o no privativa de libertad decretada por el tribunal competente o a una pena como consecuencia de haberla cometido".(8)

Esta entidad, entre otras cosas, ha sido concebida como la encargada de contribuir a proteger y promover los derechos de los niños, niñas y adolescentes que han sido vulnerados en el ejercicio de los mismos (...)

Como se observa, la legitimación de este servicio público emana de sus propias normas legales, debiendo armonizarse con la Ley 19.628, la que señala que: "El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular"(9). En definitiva, SENAME cumple con su cometido legal también efectuando el respectivo tratamiento de los datos personales de los jóvenes infractores de la ley penal.

III. Derecho de protección de datos del adolescente infractor de ley penal, enfoque en sede administrativa (SENAME)

Como expresa Francisco Zúñiga, "en una sociedad postindustrial, la procura existencial por el Estado asistencial hace de la Administración un agente

(7) Art. 1º, DL N° 2.465, de 1979.
(8) Art. 2º, DL N° 2.465, de 1979.
(9) Art. 20 Ley 19.628.

potencial de lesión de la esfera privada e íntima, dado que para programar y planificar requiere de información. En este contexto emerge el derecho a la autodeterminación informativa. La protección de la esfera privada frente al procesamiento de datos, sea electrónico o manual, debe ser objeto de regulación."(10)

(...) en una sociedad postindustrial, la procura existencial por el Estado asistencial hace de la Administración un agente potencial de lesión de la esfera privada e íntima, dado que para programar y planificar requiere de información.

Es "titular de los datos, la persona natural a la que se refieren los datos de carácter personal".(11) En este sentido, lo normal será que cada titular ejerza por sí los derechos que la propia ley le establece. En el caso de los adolescentes sujetos al régimen de la Ley 20.084, se estima que éstos estarían en condiciones de cautelar el uso de sus datos, encontrándose ciertas particularidades que habrá que observar en base a la sanción que se les aplique. Así por ejemplo, será mucho más expedito al menor sancionado con una "multa" o "amonestación", de las contempladas en la Ley 20.084, presentar una solicitud asociada a su derecho de rectificación. Usando el mismo ejemplo será, a mi juicio, mucho más complejo para un menor sancionado con la pena de internación en régimen cerrado ejercer su derecho de acceso o información.

Enunciadas las consideraciones generales, en adelante nos enfocaremos en un conjunto de recomendaciones específicas, las que serán formuladas bajo la perspectiva del derecho mismo, sus fuentes y las asociaciones con nuestra legislación penal especial, junto a su correlación con la ley sobre Protección a la Vida Privada .

1. Derecho de acceso o información del adolescente infractor de ley penal

"Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia, destinatario, el propósito del almacenamiento y la individualización de las personas y orga-

(10) El derecho a la intimidad y sus paradigmas [en línea], Zúñiga, Francisco, Chile, Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca [fecha de consulta 05 de septiembre de 2010], disponible en http://redalyc.uaemex.mx/redalyc/pdf/197/19730125.pdf

(11) Art. 2º Ley 19.628, letra ñ).

nismos a los cuales sus datos son transmitidos regularmente".(12) El derecho al que aquí se hace referencia posee como características que puede ser ejercido en intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo, en cuyo caso podrá ejercerlo antes . Será gratuito siempre que la solicitud se haga personalmente y, una vez ejercido, se tendrá que proporcionar a solicitud del titular una copia del registro alterado.

El derecho al que aquí se hace referencia posee como características que puede ser ejercido en intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo (...)

Recordemos que la Ley 20.084 se funda en el denominado principio de "*interés superior del adolescente"*, el cual se manifiesta cuando el Servicio Nacional de Menores, en sus actuaciones administrativas relativas a los procedimientos, sanciones y medidas aplicables a los adolescentes infractores de la ley penal, tiene en consideración dicho interés, el que se expresa en el reconocimiento y respeto de sus derechos, dentro de los que se incluye la garantía de acceso o de información.

La relación entre el principio mencionado y el derecho de acceso se hace patente, por ejemplo, cuando se ordena el ingreso de un adolescente a un centro de reclusión, lo que hace necesaria la creación de un expediente de ejecución completo y fidedigno que debe contener una serie de información personal y procesal del menor.(13) Dicho expediente será de exclusivo uso del personal autorizado por el director del programa o jefe de la unidad, sin perjuicio de que también podrá acceder al material el defensor del adolescente o a quien éste designe bajo su responsabilidad como profesional de apoyo a la defensa.

Con el fin de no dar espacio para equivocaciones, la regulación especial ha señalado expresamente que la entrega de información relativa a los datos contenidos en el expediente, y que digan relación con aspectos personales del adolescente se encuentra sujeta a lo dispuesto en la Ley 19.628 sobre Protección a la Vida Privada. Como se observa, aquí el ejercicio del derecho de acceso o información encuentra terreno fértil, incluso si se dan los supuestos, estimamos podría hacer uso del derecho antes del plazo general contemplado en el artículo 12 de la ley Nº 19.628, así este *"interés legítimo"* podrá estar dado para estructurar una

(12) Art. 12 Ley 19.628.

(13) Art. 35, Reglamento Ley 20.084.

defensa, solicitar el cambio de un programa para cuyo caso deberá conocer los datos asociados a él y que lo sindican a determinado programa.

Otro aspecto que podemos asociar al ejercicio del derecho de acceso o información lo encontramos en el conjunto de normas relativas al tratamiento de rehabilitación por adicción a las drogas o alcohol, disponiéndose que junto con informar al adolescente de las normas de funcionamiento de la institución o programa debe señalársele las particularidades de su plan de intervención, las consecuencias de su incumplimiento y la responsabilidad que le cabe a la institución o programa en cuanto a comunicar acerca de su situación deberá explicitarse que aquella información que el adolescente entregase a los miembros del equipo profesional podrá ser expuesta en un informe o, en su defecto, ser usada en el contexto de una audiencia oral, sin perjuicio de que la información dada en términos confidenciales estará resguardada por las normas del secreto profesional.(14)

Otro aspecto que podemos asociar al ejercicio del derecho de acceso o información, lo encontramos en el conjunto de normas relativas al tratamiento de rehabilitación por adicción a las drogas o alcohol (...)

Finalmente, diremos que existen una serie de directrices internacionales que contemplan y recomiendan normas relativas a los expedientes de los menores en los centros de internación,(15) estableciendo al efecto normas sobre acceso y rectificación de los mismos.

2. Derecho de modificación o rectificación del adolescente infractor de ley penal

Esta garantía consiste en que toda persona tiene derecho a exigirle a quien sea responsable de un banco de datos, que se dedique en forma pública o privada al tratamiento de datos personales que se modifique su información, en caso de que ésta sea errónea, inexacta, equívoca o incompleta.(16)

Parte del ejercicio del citado derecho supone que el dato sea "erróneo", es decir, el que es falso o equivocado, "inexacto" aquel falto de

(14) Art. 27 Reglamento Ley 20.084.

(15) Reglas de las Naciones Unidas para la protección de los menores privados de libertad - "Reglas de La Habana", adoptadas por la Asamblea General en su resolución 45/113, de 14 de diciembre de 1990.

(16) Art. 12 Ley 19.628.

fidelidad, "equívoco" que produce confusión o interpretaciones disímiles, e "incompleto" que le falta información.

Salvo la nota de pie de página, y no tratadas profusamente en el presente artículo, podemos señalar que las Reglas de La Habana(17) señalan que el expediente del adolescente infractor de ley menor será "confidencial", teniendo el menor el derecho a impugnar cualquier hecho u opinión que figure en su expediente, de manera que se puedan rectificar las afirmaciones inexactas, infundadas o injustas (N° 19, relativo a la administración de centros de menores). Como se observa, esta norma guarda una estrecha relación con el principio de calidad del dato que pesa sobre los organismos públicos (Servicio Nacional de Menores). Asimismo, el ejercicio del derecho contribuye desde el punto de vista del menor a la obligación del organismo público de llevar "registros fiables de datos", según instruyen las citadas reglas que encuentran aplicación en Chile.

(...) esta norma guarda una estrecha relación con el principio de calidad del dato que pesa sobre los organismos públicos (Servicio Nacional de Menores).

3. Derecho de bloqueo del adolescente infractor de ley penal

Consiste en que toda persona tiene derecho(18) a exigir el bloqueo de sus datos a quien sea responsable de un banco de datos, ya sea que se dedique en forma pública o privada al tratamiento de datos personales. Lo anterior se materializa mediante la suspensión temporal de cualquier operación de tratamiento de los datos almacenados. Una asociación con este derecho se encuentra en el denominado "proceso de egreso"(19) de un adolescente infractor de ley penal, ya que tal y como establece la ley, cuando el adolescente cumple su sanción y queda en libertad su expediente será cerrado y, transcurridos los plazos que correspondan, será destruido de conformidad a las normas legales pertinentes. En caso de haberse sustituido la sanción de internación por otra, el expediente se cerrará sólo cuando se cumpla un año del total cumplimiento de la segunda. Es decir, en concomitancia con las normas sobre protección de datos, estimamos que mientras su expediente esté cerrado podrá ejercerse el derecho a bloqueo.

(17) Ver nota al pie N° 15.
(18) Art. 12 Ley 19.628.
(19) Art. 89, Reglamento Ley 20.084.

4. Derecho de cancelación o eliminación del adolescente infractor de ley penal

Consiste en que toda persona tiene derecho[20] a exigir a quien sea responsable de un banco que se dedique en forma pública o privada al tratamiento de datos personales la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello. Tal cual señalamos para el derecho de bloqueo, el contrapunto acá será, por ejemplo, en el denominado "proceso de egreso" de un adolescente infractor de ley que una vez transcurridos los plazos legales el expediente del menor sea destruido. Estimamos que lo anterior no es más que una manifestación del derecho de eliminación bajo las normas de la Ley 20.084.

(...) para el derecho de bloqueo, el contrapunto acá será, por ejemplo, en el denominado "proceso de egreso" de un adolescente infractor de ley que una vez transcurridos los plazos legales el expediente del menor sea destruido.

Como complemento las Reglas de La Habana, en su numeral 19 señalan que el expediente del menor será cerrado y en su oportunidad si éste lo solicita debe ser destruido.

IV. Limitaciones al ejercicio de los derechos del adolescente infractor de ley penal contenidos en la Ley 19.628

Como expresamos, los derechos del titular del dato se encuentran contenidos en la Ley 19.628, la que en su artículo 13 establece que: "El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención".[21] Es decir, no podrá la voluntad manifestada unilateral o bilateralmente establecer pactos o imposiciones que finalmente hagan ilusorio el derecho.

Con todo, nos parece importante señalar que estos derechos no son incondicionales y cada petición debe ser analizada en su justa medida por la autoridad, no hay que olvidar que el menor se encuentra cumpliendo una condena por haber cometido un delito, por lo que, por ejemplo, no será factible que éste

(20) Art. 12 Ley 19.628.
(21) Art. 13 Ley 19.628

haciendo uso del "derecho de cancelación" o del "derecho de bloqueo" solicite que el Servicio Nacional de Menores elimine en primer término o suspenda el tratamiento de todo o parte sus datos , pero sí resultaría factible que en uso del "derecho de modificación o rectificación" se corrijan datos erróneos.

Desde otra mirada, pensemos en el ejercicio del "derecho de acceso o información", el que no podría llevar a conocer los datos del adolescente infractor de la ley penal para efectos de burlar su condena o saber caprichosamente antecedentes que, por una disposición legal, son de carácter reservado o secreto. En definitiva, no estamos en presencia de "derechos absolutos" y es la propia Ley 19.628 la que en uno de sus articulados refleja una norma que, nos parece, apunta en la dirección correcta al señalar que el titular del dato no podrá solicitar información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o el secreto establecidos en disposiciones legales o reglamentarias, la seguridad o el interés nacional.(22)

(...) estamos conscientes de que pueden existir situaciones límites, las que habrá que analizar caso a caso, y frente a las cuales el adolescente podrá, ya sea por sí mismo o a través de su representante, denunciar la amenaza o violación de alguno de sus derechos (...)

Para finalizar, diremos que estamos conscientes de que pueden existir situaciones límites, las que habrá que analizar caso a caso, y frente a las cuales el adolescente podrá, ya sea por sí mismo o a través de su representante, denunciar la amenaza o violación de alguno de sus derechos ante el juez conforme le faculta la normativa especial. En este supuesto, la Ley 20.084 en su artículo 50 relativo a la competencia en el control de la ejecución, señaló que: "Los conflictos de derecho que se susciten durante la ejecución de alguna de las sanciones que contempla la presente ley serán resueltos por el juez de garantía del lugar donde ésta deba cumplirse. En virtud de ello y previa audiencia, el juez de garantía adoptará las medidas tendientes al respeto y cumplimiento de la legalidad de la ejecución y resolverá, en su caso, lo que corresponda en caso de quebrantamiento".

(22) Art. 15 Ley 19.628.

V. Consideraciones, reflexiones y aportes al debate

En este breve análisis hemos observado que existe un consenso real en orden a respetar la vida privada de los menores que infringen la ley penal, en especial podemos decir que estas normas se inspiran en la Convención de los Derechos del Niño que posee rango legal en Chile. Igualmente, nuestra actual Constitución Política tampoco hace distingos en cuanto a la calidad del sujeto, la que en el numeral 4º del artículo 19 asegura a todas las personas: "El respeto y protección a la vida privada y a la honra de la persona y su familia". Como bien lo señalan algunos constitucionalistas, "no se trata de derechos que la Constitución cree, sino de derechos que ella reconoce, que le corresponde asegurar y regular su ejercicio en la comunidad nacional". Son derechos que emanan y tienen su fundamento en la naturaleza humana, que es anterior al Estado".(23) En este escenario, los adolescentes infractores de la ley penal, no obstante su condición y con las salvedades propias de su situación, encuentran también un respeto y protección a sus derechos.

(...) consenso real en orden a respetar la vida privada de los menores que infringen la ley penal, en especial podemos decir que estas normas se inspiran en la Convención de los Derechos del Niño que posee rango legal en Chile.

En la misma línea y como elemento de reflexión, es importante destacar que dentro de los derechos que asisten al adolescente infractor de ley penal —conforme la reglamentación especial— está el ser informado de sus derechos y deberes con relación a las personas e instituciones que lo tuvieren bajo su responsabilidad. Es decir, dentro de la óptica de nuestro análisis convendrá saber cuál es el grado de desarrollo y conocimiento de los derechos que encuentran su origen en la "autodeterminación informativa" y que se contienen en la Ley 19.628 en este tipo de lugares.

Cabe preguntarse también si en el desarrollo de sus funciones el órgano de la administración del Estado —en el tratamiento de los datos personales que efectúa, por ende en los registros o bancos de datos que crea— cumple con la normativa dispuesta en el Reglamento del Registro de Bancos de Datos Personales,(24) a cargo del Servicio de Registro Civil e Identificación.

(23) Molina Guaita Hernán, Derecho Constitucional, Nº 92, pág. 198, 10ª Edición, 2010, Legal Publishing, Santiago, Chile.
(24) DS N° 779, de 2000, del Ministerio de Justicia.

Autor

Francisco Trejo Ortega

Abogado de la Universidad Central de Chile, Magíster (c) en Derecho Informático y Telecomunicaciones, Universidad de Chile. Coordinador Área de Compras y Contrataciones Públicas, División Jurídica, Ministerio de Planificación.