IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES, APLICABILIDAD REAL DE LA NORMATIVA COSTARRICENSE Y EL MODELO DE LA REGULACIÓN ESPAÑOLA

Juan Diego Elizondo Vargas*

Introducción

Probablemente en ningún momento de la historia del ser humano, lo concerniente a los datos personales y su protección ha tenido mayor importancia que en la actualidad. En la era digital en la cual nos encontramos inmersos, la obtención, así como el almacenamiento de información personal son aspectos esenciales. La tecnología ha llegado a un grado de avance que es probable que exista más información sobre una persona (tanto en ficheros de solvencia, en la red y en sistemas de información) de la que una persona se pueda imaginar. Los datos son utilizados por todo tipo de empresas, desde compañías de seguros y bancos hasta medios de comunicación sociales, pasando por motores de búsqueda y compañías de análisis de otorgamiento de crédito o inclusive por empresas para el otorgamiento de un empleo.

Todo este uso indiscriminado de la información va en detrimento de nuestro honor e intimidad personal y familiar. Los datos personales han cobrado tanto interés que ha requerido que se regule el uso que se hace de estos datos; se pretende que éstos no anden a la libre, sin ningún control, sino que tengan un propósito que se considere legal y legítimo. De aquí la importancia de estudiar en qué consiste la protección de datos personales, qué comprenden estos datos, de qué manera pueden ser utilizados, qué derechos tienen las personas y cómo se pueden defender en caso de ser violentados. Nos encontramos frente a un tema bastante novedoso a nivel jurídico, que merece la pena desmarañar para que las personas estén más anuentes de sus derechos y no sean víctimas de ilegalidades.

Es de gran interés establecer qué modelo podemos seguir para que los datos personales sean protegidos y respetados como merecen. El caso de España es ejemplar, se encuentra a la vanguardia respecto al tema, al constituirse como un país que consagra la protección de datos personales como un derecho fundamental de manera real, donde las personas tienen acceso a los derechos de acceso, rectificación, cancelación y cuenta con un organismo encargado de la efectiva protección y sanción a las entidades que transgredan la legislación imponiendo multas cuantiosas y suspendiéndolas en casos graves. Es por esto que se intentará

* Especialista en derecho notarial y registral U.C.R. y Especialista en Derecho Comercial U.C.R.

ir asociando en cada uno de los temas, lo que establece la normativa española para tener un punto de comparación para nuestra legislación.

Ante la discusión que existe en la actualidad a nivel europeo, sobre la sustitución de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, surge la interrogante a nivel nacional del estado actual de nuestra ley, publicada el 5 de setiembre del 2011, si resulta aplicable o se está aplicando en este momento y la labor que le espera en el futuro.

El tema es más complejo de lo que se pueda pensar, por lo que no pretendo hacer un análisis exhaustivo de esta ley, sino esbozar los aspectos más relevantes, para así provocar un interés en el tema que le permita a la persona ahondar con mayor detalle.

Precisiones conceptuales

Para iniciar resulta necesario abordar algunos términos relevantes para comprender de manera general el tema, precisar conceptos que ayuden a entender la protección de datos personales, qué se busca proteger y de qué manera lo pretende llevar a cabo.

Según lo señala la Universidad de Alcalá son datos de carácter personal "todos aquellos que se refieren a una persona física identificada, desde su nombre hasta cualquier otro que revele información sobre sus hábitos, preferencias, forma de vida, etc."[1]

Por otro lado, la Directiva de la Unión Europea 95/46/CE, en su artículo 2.a define el dato personal como:

> *"toda información sobre una persona identificada o identificable (...) se considerará identificable toda persona, 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"*[2]

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

El artículo 3 de la Ley Orgánica Española de Protección de Datos Personales (Ley Orgánica 15/1999) utiliza una definición muy genérica de Datos de Carácter Personal:

> *"cualquier información concerniente a personas físicas identificadas o identificables". Lo cual se asemeja bastante a lo que estipula la normativa costarricense de protección de datos personales.*

1 https://portal.uah.es/portal/page/portal/proteccion_datos/datos_personales, accedido el 25-1-13.
2 http://www.datacustody.com/index.php?option=com_content&view=article&id=3&Itemid=7, accedido el 25-1-13.

Esta definición en la ley española ha sido ampliada por el artículo 5 del Reglamento de Desarrollo de la Ley de Protección de Datos Personales al referirse a los mismos como:

> *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".*

Hay que tener presente que el nombre, los apellidos, la fecha de nacimiento, la dirección postal o la dirección de correo electrónico, el número de teléfono, el número de identificación fiscal, el número de matrícula del coche, la huella digital, el ADN, una fotografía, el número de seguridad social, son datos que identifican a una persona, ya sea directa o indirectamente.

Merece mención aparte lo concerniente a los datos personales denominados sensibles, por lo que estos implican. Son los datos que, de divulgarse de manera indebida, afectarían la esfera más íntima del ser humano. Ejemplos de este tipo de datos son: el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y las preferencias sexuales. Estos datos requieren mayor protección y la Ley establece un tratamiento especial.

La ley costarricense en su artículo tercero, letra e, los define como: "información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros."

Derecho de protección de datos personales

La Constitución Europea ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, Título VI (De la vida democrática de la Unión), el artículo I-51 (Protección de datos de carácter personal) establece en el epígrafe primero que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" y en la Parte II (Carta de los Derechos Fundamentales de la Unión), Título II (Libertades), se introduce en el artículo II-68 la segunda referencia al derecho a la protección de datos, señalando de nuevo que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y añadiendo que "estos datos 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", y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación". Asimismo, en ambos preceptos se establece que una autoridad independiente se encargará de la garantía del derecho fundamental a la protección de datos personales.

El derecho fundamental a la protección de datos personales consiste a tribuir al ciudadano el poder de disposición sobre sus datos, de modo que con base en su consentimiento, puedan disponer de los mismos. Es decir, es la persona titular de los datos quien tiene el control de su información y no al revés, como habitualmente había funcionado.

Según lo indica el artículo primero de nuestra ley de protección de la persona frente al

tratamiento de sus datos personales, esta normativa tiene como objetivo:

> *"garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."*[3]

El consentimiento es el eje central en torno al cual gira toda la ley, puesto que si no existe el consentimiento no podrán tratarse los datos salvo por ciertas excepciones. El artículo 5, punto 2 de la ley costarricense menciona que este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo.

Continúa diciendo que no será necesario el consentimiento expreso cuando:

a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.

b) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.

c) Los datos deban ser entregados por disposición constitucional o legal."[4]

Una persona facilita sus datos personales cuando abre una cuenta en el banco, cuando se matricula en un curso de idiomas, cuando se apunta al gimnasio, cuando solicita participar en un concurso, cuando reserva un vuelo o un hotel, cuando pide hora para una consulta médica, cuando busca trabajo, cada vez que efectúa un pago con su tarjeta de crédito, cuando navega por Internet. Son variados los rastros de datos que se dejan a menudo en todas estas gestiones.

Requisitos para la obtención de datos

Para que los datos de carácter personal puedan ser recolectados, almacenados o empleados estos, tanto la Directiva Europea, la legislación española como la costarricense establecen que tienen que cumplirse con los requisitos de:

- Actualidad: lo que implica que los datos deberán ser actuales, se deberán de eliminar de una base si dejan de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos o registrados.

- Veracidad: deberán estar apegados a la verdad.

- Exactitud: los datos deberán ser exactos y completos, en cuanto a montos resulta de gran importancia.

---

3 http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC, accedido el 25-1-13.

4 Ibídem

- Adecuación al fin: los datos tienen que ser recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

Derechos de los ciudadanos

La LOPD española desarrolla los siguientes derechos:

- El ciudadano tiene derecho a ser informado, en el momento que facilita sus datos personales. El responsable de un fichero tiene la obligación de informar a los ciudadanos de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos correspondientes.

- El derecho de consulta permite al ciudadano, dirigiéndose al Registro General de Protección de Datos de la AEPD, conocer de la existencia de un fichero o tratamiento de datos.

- El ciudadano puede ejercitar los derechos de acceso, rectificación, cancelación y oposición ante el responsable de un fichero o de un tratamiento con el fin de conocer sus datos personales, para solicitar que sean modificados o cancelados, o bien para oponerse a su tratamiento

El caso costarricense es muy similar, en el tanto nuestra ley es muy similar a la legislación española. Contiene los derechos de acceso, rectificación y cancelación y a mi criterio implícitamente está incluido el derecho de oposición, el cual se contempla en caso de que la persona quiera oponerse al tratamiento de sus datos.

Derecho de Acceso

El derecho de acceso consiste en dirigirse al responsable o encargado de un fichero o tratamiento para conocer la totalidad de los datos personales que le afecten y así mismo, recibir una copia inteligible de los mismos, y cualquier información sobre su origen. Ejerciendo el derecho de acceso, la persona puede informase de las finalidades del tratamiento, del tipo de datos registrados, de su origen, de los destinatarios de los datos y de las posibles transferencias de datos a otros países. En virtud del derecho de acceso, regulado en el art. 15 de la LOPD, el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como la información disponible sobre el origen de dichos datos y de las comunicaciones realizadas o que se prevean realizar.

Derecho de Rectificación

Es el derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales. La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada.

Derecho de Cancelación

Este derecho ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales. Este derecho puede ejercerse

cuando el tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando los datos resulten inexactos o incompletos. En la solicitud de cancelación, el interesado debe indicar la existencia del dato erróneo o inexacto, en cuyo caso deberá acompañar la documentación justificativa.

Derecho de Oposición

Toda persona tiene la posibilidad de oponerse, por un motivo legitimo y fundado, referido a una situación personal concreta, a figurar en un fichero o al tratamiento de sus datos personales, siempre que una ley no disponga lo contrario. En principio, el ciudadano tiene la facultad de disponer y decidir sobre los usos de los datos personales que le conciernen, y por lo tanto, puede oponerse a aparecer en un determinado fichero o a que sus datos sean comunicados a terceros. Se ejercita mediante una solicitud por escrito dirigida al responsable del fichero o tratamiento, en la que se hagan constar los motivos fundados y legítimos relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho. En relación a los tratamientos de datos con fines de publicidad y de prospección comercial, los ciudadanos pueden ejercer el derecho de oposición y, a su simple solicitud, el responsable tiene que dar de baja sus datos personales en el tratamiento, cancelando de este modo las informaciones que figuraban en el mismo.

Mecanismos ante la transgresión de derechos

Tutela de Derechos

En el caso de España, en el cual es muy eficiente ante las reclamaciones de los ciudadanos, en caso del ciudadano al que le haya sido denegado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición puede ponerlo en conocimiento de la AEPD, para que ésta constate la procedencia o improcedencia de la denegación. Para solicitar la tutela de derechos, el ciudadano tiene que presentar en la AEPD un escrito, en el que se expresen con claridad sus datos, el contenido de la reclamación y los preceptos de la LOPD que considere vulnerados. La Agencia, a continuación, da traslado de la reclamación al responsable del fichero o tratamiento instándole para que, en el plazo de quince días, formule las alegaciones que estime pertinentes. Los procedimientos de tutela de derechos no tienen carácter sancionador, limitándose a estimar o desestimar las reclamaciones planteadas por los ciudadanos ante la Agencia. Sin embargo, en algunas ocasiones, los hechos constatados en los citados procedimientos pueden dar lugar a la iniciación de procedimientos sancionadores.
Costa Rica ha abarcado de manera un tanto escueta este tema, puesto que no establece un proceso específico para el caso de que no se respeten los derechos de los ciudadanos, sino que hace referencia a una denuncia, en donde la persona puede denunciar ante la PRODHAB (Agencia que se encarga de velar por el cumplimiento de la Ley y proteger los derechos de los ciudadanos), que una base de datos actúa en contravención de las reglas o los principios básicos para la protección de los datos.

Procedimiento Sancionador

El artículo 27 de la Ley costarricense, establece que de oficio o a instancia de parte, la PRODHAB podrá iniciar un procedimiento tendiente a demostrar si una base de datos

regulada por esta ley está siendo empleada de conformidad con sus principios; para ello, deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido. El sistema Español funciona de la misma forma, al poderse dar por instancia de parte o de oficio.

Los arts. 43 a 49 de la LOPD española regulan el procedimiento sancionador que podrá tramitar la AEPD. Este procedimiento se inicia contra los responsables de ficheros cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD. El procedimiento sancionador se inicia siempre de oficio mediante acuerdo del Director de la Agencia cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

El régimen sancionador establecido en los arts. 43 y siguientes de la LOPD española, articula las infracciones en tres tipos: leves, graves y muy graves. Esto va emparejado con lo establecido en el artículo 28 de nuestra normativa, en donde se estipulan las mismas tres categorías de faltas. Cabe señalar que las sanciones en el caso de España son sumamente altas, mucho más que en el resto de Europa, y suceden con frecuencia, lo que hace entrever que ahí el tema se lo toman en serio.

La Normativa Europea vs. Normativa Costarricense, aplicabilidad

Mientras Europa se mantiene discutiendo el nuevo proyecto de reglamento en donde se busca aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas, en Costa Rica todavía nos encontramos asimilando nuestra ley que entró a regir hasta hace muy poco tiempo.

La Comisión Europea ha propuesto una reforma general de las normas de protección de datos de la UE de 1995 con objeto de ampliar los derechos a la privacidad en línea e impulsar la economía digital europea. El progreso tecnológico y la globalización han modificado profundamente las vías de obtención, acceso y utilización de los datos. Además, los 27 Estados miembros de la UE han aplicado las normas de 1995 de manera diferente, lo que ha creado divergencias en cuanto a su ejecución y cumplimiento. Mediante un único acto legislativo, se suprimirán la fragmentación y las costosas cargas administrativas actuales. Esta iniciativa contribuirá a reforzar la confianza de los consumidores en los servicios en línea y, con ello, otorgará un impulso muy necesario al crecimiento, la creación de empleo y la innovación en Europa.

Las propuestas de la Comisión actualizan y modernizan los principios consagrados en la Directiva sobre protección de datos de 1995 con el fin de preservar los derechos a la privacidad en el futuro. Constan de una Comunicación en la que se exponen los objetivos de la Comisión y dos propuestas legislativas: un Reglamento que establece un marco general de la UE para la protección de datos y una Directiva sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y en relación con las actividades judiciales correspondientes.

A nivel europeo, la práctica en el uso de la Directiva y las leyes en cada uno de los países,

han permitido visualizar modificaciones para mejorar la protección de los datos personales. Entre los temas de mayor importancia están que siempre que el tratamiento de los datos exija el consentimiento del interesado, deberá dejarse claro que dicho consentimiento debe obtenerse explícitamente y no presuponerse. El "derecho al olvido" ayudará a los ciudadanos a gestionar mejor los riesgos inherentes a la protección de los datos en línea: los usuarios podrán borrar sus datos cuando no existan razones legítimas para conservarlos, esto hará que las personas confíen más en internet, en especial en nuestros días en donde existen muchas plataformas de información, como facebook, twitter, linkedIn, google+, etc.

Costa Rica por el momento se encuentra en pañales en el tratamiento de la materia, pese a existir legislación al respecto, existe mucho desconocimiento en torno al tema. Las instituciones públicas han sido las principales culpables de la desprotección de datos, puesto que éstas se han dedicado a vender información a empresas recopiladores de datos. El proceso de asimilación de la Ley en nuestro país ha sido lento, la Agencia de Protección de Datos de los Habitantes se conformó 6 meses después de haberse publicado la Ley, y el Reglamento más de un año después. Las empresas que deberían estar ya preparadas para la entrada en eficacia de la Ley en todo su ámbito de aplicación, han dicho no estar preparadas para cumplir con ella, según lo estableció un artículo de El Financiero, lo cual es preocupante y poco alentador.

También existe la interrogante sobre la preparación que puedan tener quienes conforman la Agencia, si han sido capacitados en torno al tema, qué tan empapados están respecto la protección de datos personales en Europa, quien es la que lleva la batuta respecto a la materia. Existen muchas dudas al respecto, las personas no están familiarizadas con los derechos que les atañen, son muchos años de soportar los abusos de empresas que han dispuesto de la información de los ciudadanos sin ningún tipo de control. Para muchas personas es normal vivir recibiendo mensajes promocionales en su celular sin haber consentido con ello, o que las empresas comercialicen sus datos al mejor postor. Todo esto tiene que acabar, y para que esto sea así, las personas tienen que estar conscientes de cómo el sistema los puede proteger, cosa que en ningún momento ha hecho el Gobierno en la población, es la desinformación la que prevalece y es evidente que debe existir un cambio cultural. Existe un gran desafío adelante, puesto que muchas situaciones que se suscitaban en el pasado ya no serán aceptables jurídicamente, lo que permite establecer que en el futuro tendrá gran preponderancia esta Ley y su Agencia, en su prosecución de proteger a los ciudadanos y sus datos personales.

Conclusión

Cabe concluir que el tema aquí apenas empieza a calentar, se está apenas preparando el terreno para lo que se viene, va a empezar a tomar importancia conforme entré en funcionamiento real la ley, el Reglamento, la Agencia, y las personas empiecen a enterarse de los derechos que tienen y los mecanismo que pueden ejercer frente a las compañías inescrupulosas que utilizan sus datos de manera ilegítima. Como se pudo apreciar en este estudio, es fundamental la importancia que tiene la protección de datos personales en la

actual era digital, en donde la información se encuentra en todos lados y se moviliza rápidamente. Es de gran importancia, conocer los diferentes conceptos que integran este entramado normativo, así como los derechos y mecanismos para protegerlos. Sirve como modelo a seguir el español, el cual apoyado en una directiva europea, se ha encargado de hacer una ley acorde a las exigencias de la época y la ha aplicado de manera efectiva.

De igual forma, mientras la Unión Europea sigue avanzando en el tema, al discutir un nuevo reglamento de protección de datos personales, basándose en los últimos avances tecnológicos y las necesidades actuales, Costa Rica está por el momento en un modo de “stand by”, hasta que empiece a funcionar de manera real la ley, con el pensamiento positivo que tengamos la capacidad para afrontar lo que se avecina.