6. LOS FICHEROS DE DATOS PERSONALES: SU UTILIZACIÓN GARANTIZANDO LA PROTECCIÓN DE LOS DATOS

Si observamos la cantidad de ficheros con datos de carácter personal, parece que el número de quejas en esta materia debería ser mayor de lo que es.

Puede que ello se deba a que el sistema de mecanismos de control es aún bajo, comparado con el nivel de protección que el ordenamiento reconoce al ciudadano para procurar el control de sus datos, o también a que éste aún no tiene una concienciación suficiente de ese derecho a controlar sus datos de carácter personal.

Es esta percepción, unida a que la insuficiente concienciación afectaría de igual modo a algunos titulares de los ficheros y a sus usuarios, la que nos mueve a incluir en el informe de este año las reflexiones que aquí haremos, las cuales se justifican en el marco de la promoción de los derechos que la institución del Ararteko realiza. Para ello abordaremos aquellos aspectos que nos parece que merecen especial atención para que los ciudadanos puedan ejercer su derecho a la protección de datos, con objeto de que todas las partes afectadas tengan el protagonismo que corresponde a sus derechos y obligaciones.

Las consideraciones que haremos no tienen que ver con los medios técnicos propiamente dichos -que deberán adecuarse constantemente-, sino con aquellos otros factores que siempre han de estar presentes en la conducta de quienes por su trabajo son usuarios de datos personales, y de quien es titular del fichero que los contiene.

Desde esta perspectiva, debemos tener en cuenta que lo que se conoce como cultura de la confidencialidad es predicable de todos los ficheros de datos de carácter personal, sean o no tratados por medios informáticos, y además no únicamente de los que contienen datos que el ordenamiento califica como especialmente protegidos. Todos los datos de carácter personal están protegidos, debido a la posibilidad de que, a partir de datos que parecen irrelevantes, se pueda elaborar un perfil de las personas.

Parece indiscutible que los datos de carácter personal que constan en todos los ficheros –también los de las administraciones públicas, aunque respondan a intereses generales– han de quedar protegidos frente a cualquier intromisión ajena a la finalidad con la que se crean tales ficheros. Por otro lado, teniendo en cuenta que cumplen un fin que el ordenamiento ve justificado, no dudamos de las ventajas que supone el tratamiento automatizado de los datos.

Pero que la finalidad sea legítima no desvirtúa su naturaleza de personales, y, por ello, el ordenamiento los protege de los peligros inherentes al medio utilizado.

Las ventajas serán indudables, y no hay razón para pensar que su creación obedece a fines distintos a los encomendados a los poderes públicos que disponen de nuestros datos personales. Aún así, no nos deben parecer infundadas las cautelas de los ciudadanos ante el uso de la informática cuando, en relación con el derecho a la intimidad, la propia Constitución, en su art. 18.4, se refiere de manera expresa a la necesidad de limitar su utilización.

Ni el riesgo ni la vulneración del derecho a la intimidad nacen con la informática, y de hecho, la vigente Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPDP), se ocupa de todos los ficheros que contengan datos personales, sean o no objeto de tratamiento automatizado. Sin embargo, parece que la implantación de la informática ha llevado a que la confidencialidad sobre los datos personales recupere su protagonismo.

Paradójicamente, la informática, que ofrece mecanismos para que sean únicamente las personas autorizadas las que accedan a los datos personales de los ficheros automatizados, y que debería dejar constancia de accesos no autorizados, genera también los mayores riesgos de uso inadecuado de estos datos.

Evidentemente, la seguridad de los ficheros depende en buena medida de cuál sea el *nivel de los medios técnicos*. Pero cualquiera caerá en la cuenta de que su implantación sólo cumplirá su objetivo si los usuarios son conscientes de la confidencialidad de los datos y de lo esencial que es la utilización correcta del sistema de información del que se trate.

La sentencia de la Audiencia Nacional RJCA 1999\3467, en relación con un acceso no justificado por una persona usuaria de la Agencia Estatal de Administración Tributaria, puede ilustrar lo que es un uso inadecuado, sea activa o pasivamente: *"…en documentos obrantes en el expediente, que acreditan y recogen los 17 accesos a la base de datos provincial llevados a cabo por la misma, o por otra persona no identificada, por causa de su negligencia, sin justificación alguna por razón del trabajo que desempeña en la Administración Tributaria, por razones obvias de estricta confidencialidad de los datos de los administrados contenidos en dichas bases, así como en sus propias declaraciones, (...) y que en consecuencia, es posible que se dejara en algún momento la pantalla abierta, no pudiendo precisar si alguna persona utilizó su ordenador, alegaciones que no justifican en absoluto tales accesos, sino al contrario, teniendo en cuenta el especial deber de custodia, secreto y sigilo riguroso que, respecto de los asuntos que conozca en razón de su cargo, impone a los funcionarios…"*

La presencia casi absoluta de la informática en la gestión de las administraciones públicas hace posible que datos personales que antes eran neutros puedan ahora no serlo, precisamente por las posibilidades que ofrece su tratamiento automatizado. Es decir, a partir de datos que, aislados, son irrelevantes, se puede elaborar el perfil de una persona.

Tratando de evitar este riesgo, el ordenamiento impone a los titulares de los ficheros una serie de obligaciones consustanciales, pero, de modo correlativo a esas obligaciones, reconoce al ciudadano unas facultades que le permitirán controlar la información que le afecta. La Sentencia del Tribunal Constitucional 202/1999 se refiere de este modo a estas facultades: *"…la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención. "*

Para que esta capacidad de actuar se pueda materializar, es imprescindible que el ciudadano reciba una información que vaya más allá de la publicación en el correspondiente diario oficial.

La Ley Orgánica 15/1999, en su artículo 5, con las especificidades que prevé, establece que los interesados a los que se soliciten datos personales, deberán ser previamente informados de modo expreso y preciso.

Para que este derecho a la información sea efectivo, como ocurre con las demás facultades relacionadas con el derecho a la protección de datos, es necesario que seamos conscientes de su existencia y alcance.

Es posible que no dudemos de la obligación de informar a quien lo pide, pero quizás nos preguntemos si debemos adelantarnos a informar a quien no lo ha solicitado. Tal interrogante puede ser lógica si no somos conscientes o desconocemos el derecho del ciudadano a ser informado sobre la existencia de un fichero al que se incorporarán sus datos.

Por ejemplo, teniendo en cuenta cuál es la relación entre un paciente y su médico, parece razonable pensar que aquél está de acuerdo en que quede constancia de los datos necesarios para su asistencia sanitaria. Quizás por ello nos preguntamos sobre el sentido de esta obligación de informar al respecto al paciente.

También es posible que cuando se obvie la obligación de informar, ello se deba a que se entienda que éste carece de sentido, pues, en principio, no existe un correlativo derecho del paciente a negar su consentimiento al tratamiento de sus datos.

Esta conducta estaría olvidando, en primer lugar, la obligación legal que arriba hemos señalado (art. 5 de la LOPDP), y también que, además del consentimiento, existen otros derechos que posteriormente se pueden ejercer, como son los de acceso, cancelación, etc., reconocidos como tales por el ordenamiento, y cuya aclaración o anticipación de criterios de actuación es conveniente, para hacer posible un correcto ejercicio de estos derechos.

Las dudas que en ocasiones se observan a este respecto, pueden ser una muestra de una concienciación insuficiente sobre el derecho del ciudadano a controlar sus datos personales.

Esa importancia que tiene la información la observamos en algunas quejas presentadas por personas que manifestaban sus cautelas o desacuerdos, ya que entendían que el tratamiento de sus datos clínicos suponía una intromisión en su derecho a la intimidad.

Para explicar un determinado sistema de información que fue objeto de queja, Osakidetza había tratado de explicar sus ventajas, así como las medidas de seguridad, pero apreciamos que no había abordado de igual modo aquellos aspectos que eran manifestación del derecho de los pacientes a proteger sus datos personales. En este sentido, derechos tales como el referido a la información, al consentimiento, al acceso, o a la rectificación, y cancelación, en su caso, eran cuestiones que no se habían abordado adecuadamente.

Algunas de estas quejas nos mostraban, además, una situación de información insuficiente sobre las medidas que se adoptan para proteger el acceso indebido de los datos de carácter personal, y cabe pensar que fue en ese contexto en el que un aspecto del sistema de información que, en criterio de esta institución, no era esencial (su centralización), cobró un protagonismo mayor del que merecía desde el punto de vista de la normativa en materia de protección de datos.

Tras las actuaciones que realizamos con motivo de estas quejas (recogidas en el capítulo II de este Informe al Parlamento, en el apartado correspondiente a Sanidad), concluimos que, en su diseño, el sistema cuestionado en la queja cumplía las medidas de seguridad, pero también que es necesario, en igual grado, informar adecuadamente a los ciudadanos y promover una cultura que hemos llamado de confidencialidad, en cuyo seno podrían encontrar respuesta muchas de las cuestiones que se suscitan en este ámbito.

Hemos indicado que la efectividad de las facultades relacionadas con el derecho a la protección de datos exige que seamos conscientes de su existencia y alcance.

Algunas facultades recogidas en la Ley como parte del derecho a la protección de datos personales requieren un desarrollo o establecimiento de criterios de actuación que sean útiles para atender las peticiones que los ciudadanos puedan formular cuando pretendan ejercer tales derechos. Nos referimos a las peticiones de acceso, consentimiento, o cancelación, cuyo correcto ejercicio dependerá en gran medida de esa labor, que evitará respuestas genéricas, o no fundamentadas.

A ese respecto, decíamos al comienzo que no se cuestiona que los datos personales sean confidenciales. Pero este reconocimiento puede no ser eficaz, si no se dedica un esfuerzo para materializarlo, lo que exigirá una dedicación suficiente de medios para fines que, en principio, son transversales a las funciones sectoriales propias de cada administración titular del fichero (funciones de recaudación, sanitarias, educativas, seguridad, etc.).

Lejos de entenderlo como una desviación de esfuerzos, la adopción de esas medidas debe ser asumida como algo consustancial al desarrollo del servicio cuya prestación tienen encomendadas las administraciones públicas, y no como una tensión de fuerzas opuestas.

No estamos, pues, ante un derecho de libre disposición, que sea secundario en relación con la competencia material que desarrolle una determinada administración pública, y en consecuencia, se debe procurar un equilibrio entre el principio de eficacia que debe presidir sus actuaciones sectoriales y el respeto del derecho a la protección de los datos personales.

Actividades como las desarrolladas por la Comisión de Documentación Clínica –en cuyas conclusiones de octubre de 2000 se recogen una serie de recomendaciones para garantizar la confidencialidad de la información clínica– ilustran esa conveniencia de trabajar en torno a este derecho transversal, y son mecanismos que pueden ayudar a resolver dudas sobre aspectos instrumentales relacionados con el derecho a la protección de datos: eventuales peticiones de cancelación de datos, o de consentimiento…

La promoción de una cultura de la confidencialidad está unida a esos esfuerzos, pues sin perjuicio de la concienciación de los usuarios, no se puede pretender que quede en sus manos la primera respuesta y/o decisión sobre cuestiones como las repetidamente apuntadas (acceso, consentimiento etc.), que pueden resultar complejas en su respuesta.

A modo de ejemplo, pensamos en las situaciones a las que se refiere la Ley Orgánica 15/1999, en su artículo 6.4, relativo al consentimiento del ciudadano. La interpretación o aplicación de este artículo plantea muchas interrogantes -sobre todo en un ámbito como el sanitario, en el que, en principio, no es necesario el consentimiento-, y su alcance debería estudiarse en cada ámbito, en tanto puede ser argumentado por el ciudadano para oponerse a un tratamiento de sus datos personales.

De nuevo tenemos que decir que la efectividad de las facultades que integran el derecho a proteger sus datos dependerá de que se prevean criterios que ayuden a determinar los supuestos enunciados de modo genérico en la ley.

Además de tratarse de problemas cuyo estudio necesita de conocimientos técnico-jurídicos, quizás distintos de los requeridos al usuario para desempeñar su puesto de trabajo, las respuestas deben ser homogéneas, tomando como base criterios objetivos previamente establecidos por el titular del fichero. A este respecto, aunque el usuario

respete impecablemente la confidencialidad de los datos, puede desconocer la respuesta a cuestiones sobre el ejercicio de facultades del paciente respecto de sus datos, y no siempre será fácil o cómodo, ni tampoco debe ser siempre necesario, remitir todas las preguntas al titular del fichero para su respuesta.

La competencia para resolver estas cuestiones corresponde al titular del fichero, que deberá resolver motivadamente, por lo que, en principio, el usuario –en el ámbito sanitario, principalmente el médico– que recibe del ciudadano unos datos que después serán automatizados, no es estrictamente el obligado a pronunciarse sobre las cuestiones o problemas que sobre ese tratamiento pueda plantearle el ciudadano. Pero también es cierto que el usuario/facultativo, aunque sea en el grado que le corresponda, puede ser una fuente de información y, por tanto, ser importante para que el paciente pueda ejercer correctamente su derecho de protección de datos.

Junto con los empleados que son usuarios de los datos personales, las administraciones titulares de los ficheros constituyen una pieza esencial en esta cultura de la confidencialidad.

Pero el papel de las administraciones no es sólo trascendente en la adopción de medidas directas sobre su propio sistema de información, en función del nivel de seguridad que el ordenamiento establece según el tipo de datos contenidos en sus ficheros, o de control de sus usuarios. Su papel también es esencial porque son las administraciones las que, con relación a determinados servicios, deciden sacar al exterior el tratamiento de datos personales recabados de los ciudadanos.

La posibilidad de prestación de servicios de tratamiento de datos por cuenta de terceros, recogida por la LOPDP, en su artículo 12, puede añadir más riesgos, al intervenir terceros distintos a la administración titular del fichero.

En el ámbito de la Administración de la Comunidad Autónoma, la Orden de 11 de junio de 2002, de la Vicepresidencia del Gobierno y Consejera de Hacienda y Administración Pública, recuerda, en relación con el tratamiento de datos por terceros, la obligación de que los contratos que se suscriban con ellos incorporen en sus condiciones las que establece el art. 12 de la LOPDP.

Además de la cesión para el tratamiento de datos, en otras ocasiones se puede dar también una gestión indirecta de un servicio público.

La contratación de empresas privadas para gestionar servicios tales como la recaudación de ingresos, de gestión de tareas relacionadas con nóminas, o atención telefónica para situaciones de desbordamiento de llamadas, son opciones que pueden tener encaje en el ordenamiento, si se cumplen los requisitos para ello. A modo de ejemplo, en un ámbito como el de la recaudación, donde no ha sido extraña la contratación administrativa para la gestión de los ingresos, hemos de pensar que la administración titular del fichero encargará el tratamiento de los datos a la empresa con quien contrata aquella gestión de la recaudación.

No nos corresponde pronunciarnos sobre la conveniencia de acudir a la gestión indirecta de servicios que son titularidad de cada administración. Pero si debemos recordar que las garantías deben ser idénticas, y que los requisitos que se deben cumplir no se refieren únicamente al ámbito de la contratación administrativa.

Aunque estos contratos no conlleven una renuncia en el ejercicio de autoridad por parte de las administraciones contratantes, suponen una cesión de los datos de carácter personal. Por ello, por los riesgos que pueden acarrear para la seguridad la contrata-

ción externa, añadidos a los inherentes al propio tratamiento automatizado, es imprescindible que las condiciones del contrato prevean la vinculación a los preceptos referidos a la protección de datos personales, y se establezcan mecanismos que permitan auditar su cumplimiento, y, en su caso, la devolución de los datos.

Comenzábamos estas reflexiones señalando que el nivel de concienciación sobre la confidencialidad de los datos quizás sea inferior al que debiera. Pero es posible que en algunos ámbitos (por ejemplo, los que tienen alcance económico), por la tangibilidad que atribuimos a su utilización indebida, el ciudadano tenga una mayor conciencia y, de modo correlativo, también la tengan el usuario y el titular del fichero.

Por el mismo motivo, por su tangibilidad, manifestada en el estigma social que existe aún, podemos decir que sobre determinadas enfermedades (por ejemplo, VIH o SIDA), hay una concienciación del derecho a la confidencialidad del paciente que no es equivalente a la de otros con enfermedades diferentes que no sufren el mismo estigma.

Sin pretender obviar las diferencias entre situaciones que no son iguales, y las especialidades que pueden presentar unas respecto de otras, el hilo conductor de las medidas a adoptar por los titulares de ficheros y la conducta de sus usuarios debe ser la de la utilización de los datos exclusivamente para el fin con que se crea el fichero. No hay razones para rebajar el grado de confidencialidad en el acceso y utilización de los datos personales que, en palabras de la Ley Orgánica, son *"cualquier información concerniente a personas físicas identificadas o identificables"*.

Nos hemos referido a algún ámbito de actuación administrativa concreto, para ilustrar las facetas que presenta el derecho a la intimidad de los ciudadanos, en su vertiente de protección de datos de carácter personal. La institución del Ararteko trasladó a la administración afectada las concretas conclusiones y sugerencias que el estudio de las quejas nos merecieron.

Las reflexiones que aquí hemos hecho, de alcance general, han pretendido recordar la necesidad de promover la protección de todos los datos de carácter personal que existan en los ficheros, en nuestro caso, de titularidad de las administraciones públicas de nuestra Comunidad Autónoma.

Dando por sentadas cuáles son las obligaciones impuestas a las administraciones públicas, consustanciales al cumplimiento de los fines de interés general que tienen encomendado, hemos querido referirnos a esta manifestación del derecho fundamental a la intimidad como es la protección de datos, por entender que su percepción no tiene la entidad que debería, y que, en consecuencia, los agentes afectados –los titulares de los ficheros, los usuarios, y los ciudadanos–, adolecemos en ocasiones de una insuficiente cultura de la confidencialidad.

En el marco de esa cultura, podemos pensar que existirán medios que permitan un ejercicio efectivo de las facultades de los ciudadanos para proteger sus datos, un mejor conocimiento de su alcance por parte de los usuarios, y que la confidencialidad tenga el protagonismo que debe.

Esta concienciación tendrá diversas manifestaciones, como pueden ser, la continuidad en la implantación de los sistemas de seguridad, la vigilancia del cumplimiento del artículo 12 de la LOPDP a las empresas adjudicatarias en los casos de contratos de tratamiento de datos, o de cesión de estos para la gestión indirecta de un servicio, la instrucción a los usuarios en sus obligaciones sobre la utilización de los datos, o el

establecimiento de criterios que ayuden a que las facultades de acceso, consentimiento, cancelación, se puedan ejercer adecuadamente.

Situados en este contexto, donde hemos tratado de los aspectos sobre los que se debe trabajar para garantizar este derecho, es difícil obviar la importancia que un órgano especializado tiene para el control efectivo de los límites impuestos al uso de la informática, sin perjuicio de las competencias atribuidas a la institución del Ararteko por la Ley 3/1985, de 27 de febrero.

De ahí que no nos puedan pasar desapercibidas las funciones previstas para la Agencia de Protección de Datos, ni la contribución que para esta protección supondrá la creación de una Agencia Vasca de Protección de Datos, en relación con los ficheros de datos de carácter personal creados o gestionados por la Administración de nuestra Comunidad Autónoma, órganos forales de los territorios históricos y por la Administración local.

Por ello, terminamos estas reflexiones recordando la importancia que para un control más efectivo del uso de los datos personales tiene la aprobación y dotación de los medios que permitan la puesta en funcionamiento de la Agencia de Protección de Datos de la Comunidad Autónoma del País Vasco.