CNS 22/2009

Dictamen en relación con una consulta sobre el sistema de control horario del personal de una Diputación Provincial, mediante la huella dactilar.

Con fecha del 7 de mayo de 2009, se presenta ante la Agencia Catalana de Protección de Datos un escrito de una Diputación Provincial, en el que se solicita la opinión de la Agencia en relación con las implicaciones jurídicas que puede suponer la instalación de un sistema de control horario de sus empleados mediante el tratamiento de la huella dactilar y su adecuación a la legislación vigente en materia de protección de datos personales.

Analizada la consulta, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente:

I

[...]

II

La Diputación Provincial (en adelante, Diputación) planea llevar a cabo la instalación de un sistema de control horario de su personal, basado en el uso de la huella dactilar, en todos los puntos de entrada del edificio, y a fin de delimitar los extremos que sean necesarios para cumplir lo previsto en la normativa en materia de protección de datos personales, plantea las cuestiones siguientes:

a) Implicaciones jurídicas que puede suponer el sistema de control horario, el cual implica el tratamiento del dato personal de los empleados relativo a la huella dactilar, así como su adecuación a la finalidad del tratamiento planteado.

b) Delimitación de las actuaciones necesarias para adecuar el tratamiento pretendido a la normativa aplicable sobre protección de datos personales.

Ambas consultas se tratan en los fundamentos jurídicos siguientes.

III

En primer lugar, hay que analizar si el tratamiento de la huella dactilar de los empleados de la Diputación, como sistema de control horario, es conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y a la demás normativa aplicable.

El artículo 3 a) de la LOPD define como dato personal cualquier información referente a personas físicas identificadas o identificables. Asimismo, el artículo 5.1 f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante, RLOPD), define dato de carácter personal como cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Los datos de huellas dactilares son datos biométricos. El término «biometría» se refiere a aquellos sistemas que utilizan características físicas o fisiológicas o elementos de conducta personal medibles, con la finalidad de determinar la identidad o verificar la supuesta identidad de una persona. La huella dactilar forma parte de los datos conocidos como «datos biométricos fisiológicos», que se entiende que están

basados en datos derivados de la medición de una parte de la anatomía de una persona.

Así pues, la huella dactilar, como dato biométrico, tendrá la consideración de dato de carácter personal, por lo que se deberá tener en cuenta la aplicación de los principios y obligaciones de la normativa sobre protección de datos personales.

Conviene aclarar, aunque resulte obvio, que aquellas huellas que no permitan la identificación de una persona física, o aquel sistema de almacenamiento que no permita que se pueda identificar sin esfuerzos desproporcionados al interesado, quedan fuera del ámbito de aplicación de la normativa sobre protección de datos personales (Documento de trabajo sobre biometría, adoptado por el Grupo de Trabajo sobre el artículo 29, el 1 de agosto de 2003). Otra cosa es que el dato biométrico se almacene de una manera no identificable, pero que, relacionado con otros datos identificativos, como pueden ser el nombre y los apellidos del titular, permita la identificación de una persona sin tener que realizar esfuerzos desproporcionados (artículo 5.1 o) del RLOPD). En este caso, el tratamiento de los datos biométricos sí que entrará dentro del ámbito de aplicación de la normativa sobre protección de datos.

Asimismo, no hay que confundir la singularidad de estos datos con el carácter de datos sensibles o datos especialmente protegidos a los que hace referencia el artículo 7 de la LOPD. Los datos biométricos sólo tendrán la consideración de datos sensibles cuando revelen la ideología, la afiliación sindical, la religión o las creencias, o hagan referencia al origen racial, la salud o a la vida sexual de los interesados.

IV

Una vez establecido que la instalación de un sistema de control horario basado en la recogida y el tratamiento de huellas dactilares comportará el tratamiento de datos personales de los empleados de la Diputación, hay que tener en cuenta que este tipo de tratamiento puede afectar al derecho fundamental de los empleados a la protección de sus datos personales (artículo 18.4 de la Constitución Española).

Por lo tanto, hay que determinar si este tipo de tratamiento de datos personales biométricos por parte de la Diputación puede resultar proporcionado y legítimo de acuerdo con lo establecido en la normativa sobre protección de datos personales.

El artículo 4.1 de la LOPD, relativo al principio de calidad de los datos, dispone que los datos de carácter personal sólo se pueden recoger para ser tratados, así como someterlos a tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se obtuvieron.

A fin de determinar si el tratamiento de la huella dactilar de los empleados por parte de la Diputación, como sistema de control horario, cumple con este principio de calidad de los datos, resultan ilustrativas, por enjuiciar un supuesto parecido al planteado en esta consulta, como bien menciona la institución competente en materia de derechos de los ciudadanos, la Sentencia del Tribunal Superior de Justicia de Cantabria, de 21 de febrero de 2003, y la Sentencia del Tribunal Supremo, de 2 de julio de 2007, así como la Sentencia Interlocutoria del Tribunal Constitucional, de 26 de febrero de 2007, en especial en cuanto a los argumentos referidos a la doctrina de la proporcionalidad.

De acuerdo con dicha doctrina, para comprobar si una medida restrictiva de un derecho fundamental respeta el principio de proporcionalidad, se tendrá que verificar que cumpla tres requisitos: que sea necesaria, en el sentido de que no exista otra más

moderada para la consecución de aquel propósito con la misma eficacia (juicio de necesidad); que sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad); y, finalmente, que de ella se deriven más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Sobre la base de estos argumentos, hay que entender que la instalación de un sistema de control horario mediante huellas dactilares:

- Puede ser una medida de control horario necesaria, dada la incorporación a la Administración pública de las nuevas tecnologías como método de control, debido, tal como manifiesta la Diputación, al notorio carácter de imperfectos de los sistemas de control usados más habitualmente (sistema de marcación a través de una ficha), que no ofrecen suficientes garantías.

- Es una medida de control horario que resulta idónea para conseguir el objetivo propuesto, que no es otro que el de lograr un mayor nivel de eficacia en la Administración pública, lo que pasa por un control efectivo del cumplimiento de sus obligaciones por parte de los empleados públicos; obligaciones que se inician en el momento en que acceden puntualmente a sus puestos de trabajo y en una estricta observancia de la jornada laboral.

- Y que la implantación de estos sistemas puede reportar beneficios o ventajas para el interés general. La relación entre la Administración pública y sus empleados, si bien está inspirada en deberes especiales de buena fe o lealtad del empleado (el funcionario) hacia el empleador (el servicio público), no puede comportar la privación al empleado de sus derechos fundamentales y libertades públicas, ni siquiera de una manera transitoria o provisional, ni tampoco desembocar en un deber de sujeción extremo o genérico. Ahora bien, el carácter especial de la relación entre la Administración y sus empleados justifica una especial exigencia en el cumplimiento de sus obligaciones, ya que esto repercute en una mayor eficacia de la Administración en la consecución de los intereses generales (STC 85/1983, de 25 de octubre).

De acuerdo con todas estas consideraciones, se puede llegar a admitir la recogida de datos biométricos, como las huellas dactilares, del personal de la Diputación como medida de control horario. Este tratamiento cumplirá con el principio de calidad regulado en el artículo 4 de la LOPD, por tratarse de un dato adecuado, pertinente y no excesivo en relación con su finalidad de controlar el cumplimiento horario de los empleados citados, siempre que, como veremos, se adopten las garantías necesarias.

Por otro lado, también se tendrá que analizar si la Diputación necesita el consentimiento de los empleados para la recogida y el tratamiento de sus huellas dactilares. En este sentido, el artículo 6 de la LOPD señala que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. Sin embargo, el apartado segundo de ese mismo artículo establece que no será necesario el consentimiento cuando los datos personales se refieran a las partes de un contrato o precontrato de una relación de negocio, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

Dado que la recogida de datos personales de los empleados se realiza dentro de una relación jurídica laboral o administrativa y tiene como finalidad el control, precisamente, de su cumplimiento, la Diputación podrá recoger y tratar datos biométricos consistentes en la huella dactilar de sus empleados sin necesidad de requerir su consentimiento.

Sin embargo, aunque la Agencia admite que el uso de estos sistemas de control del horario mediante huellas dactilares no es contrario a la normativa sobre protección de datos personales, de acuerdo con la doctrina expuesta, sí que recomienda, en la medida en que sea posible, evitar su uso de manera generalizada. Los sistemas de control basados en estos tipos de datos biométricos se configuraron principalmente como mecanismos para controlar el acceso de personas a determinados lugares o servicios en los que se requería un grado de seguridad mayor debido al tipo de información tratada o al tipo de actividad realizada. Si el uso de estos sistemas de control se amplía a otros ámbitos de actuación cotidianos o corrientes, se corre el riesgo de perder su valor como medida de seguridad más fiable. Por lo tanto, dentro de la legitimidad que tiene la Diputación para elegir el medio de control horario que considere más adecuado, se recomienda valorar la posibilidad de optar por un sistema menos restrictivo.

V

Entrando en el análisis de la segunda cuestión planteada por la Diputación, se recuerda que, sin perjuicio de las consideraciones anteriores, en caso de que se proceda a la instalación del sistema de control horario basado en las huellas dactilares de los empleados, la Diputación está obligada a cumplir los demás principios y obligaciones que establece la normativa en protección de datos personales, como, entre otros:

1.- Será necesario cumplir con el principio de información establecido en el artículo 5.1 de la LOPD, según el cual, al solicitar datos personales, «los interesados […] deberán ser informados de modo expreso, preciso e inequívoco*:*

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.»

2.- Con carácter previo a la recogida de los datos personales, se deberá crear, y notificarlo al Registro de Protección de Datos de Cataluña, el correspondiente fichero de datos personales, entendido como «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso» (artículo 3 b) de la LOPD*).*

En este sentido, la Diputación manifiesta que utilizará los datos personales de los empleados que ya figuran en su fichero de «personal».

Se ha constatado que dicho fichero se creó mediante un acuerdo del Pleno de la Diputación con fecha del 17 de junio de 2005. En este sentido, se recuerda que el artículo 20.1 de la LOPD establece que la creación, modificación o supresión de los

ficheros de las Administraciones públicas sólo se podrán efectuar mediante disposición de carácter general publicada en el Boletín Oficial del Estado o en el diario oficial correspondiente. Aunque el artículo 52.1 del RLOPD permita la creación, modificación o supresión de ficheros mediante acuerdo, se recuerda que en este caso, dado que la Diputación disfruta de potestad reglamentaria en sentido propio, esta disposición no le será aplicable, y será necesario crear, modificar o suprimir sus ficheros mediante una ordenanza o cualquier otra disposición de carácter general, de acuerdo con lo dispuesto en el artículo 20.1 de la LOPD.

Dicho fichero de «personal» incluye los apartados exigidos por el artículo 20.2 de la LOPD en relación con la finalidad del fichero y los usos previstos; las personas o colectivos sobre los que se obtienen los datos; el procedimiento de recogida de los datos; la estructura básica del fichero y la descripción de los tipos de datos personales que se incluyen; las cesiones y, en su caso, las transferencias de datos a países terceros; los órganos responsables del fichero; los servicios o unidades ante los que se pueden ejercer los correspondientes derechos y, finalmente, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

Sin embargo, para que este fichero legitime el tratamiento de las huellas dactilares de los empleados por parte de la Diputación, deberá ser objeto de modificación necesariamente antes de la puesta en marcha del sistema de control horario o del inicio de la recogida de los datos personales, salvo que se opte por crear otro nuevo. Concretamente:

- Respecto al apartado «finalidad y usos del fichero» (artículo 20.2 a) de la LOPD), se deberá especificar lo relativo al control horario de los empleados.

- Respecto al apartado «procedimiento de recogida de los datos» (artículo 20.2 c) de la LOPD), se deberá incluir también el sistema empleado para recoger las huellas dactilares.

- Respecto al apartado «estructura básica del fichero y tipo de datos personales incluidos» (artículo 20.2 d) de la LOPD), se deberá incluir, dentro de los datos identificativos, los datos relativos a las huellas dactilares de los empleados.

Por otro lado, hay que tener en cuenta que el RLOPD, en relación con el contenido del acuerdo de creación de ficheros, ha concretado o añadido (artículo 54.1) varias cuestiones en relación con lo que dispone el artículo 20.2 de la LOPD, y que, por tanto, será necesario consignar cuando se modifique el fichero de «personal» de la Diputación (o bien cuando se cree un fichero específico para este tratamiento). Concretamente:

- Respecto a la estructura básica del fichero, hay que indicar el sistema de tratamiento utilizado en la organización (apartado 54.1 c). En este sentido, aunque en el fichero se especifica su carácter «informatizado y manual», se debería emplear la terminología prevista en el RLOPD y señalar que el sistema de tratamiento utilizado será «parcialmente automatizado».

- Respecto a las transferencias internacionales de datos (apartado 54.1 e), hay que tener en cuenta que si bien el artículo 20.2 de la LOPD engloba en un mismo apartado la información referente a las cesiones o comunicaciones de datos personales y a las transferencias internacionales de datos personales, el artículo

54.1 del RLOPD ha diferenciado en dos apartados distintos cada uno de estos conceptos: el apartado d) del artículo 54.1 en lo que se refiere a las comunicaciones de datos, indicando, en su caso, los destinatarios o categorías de destinatarios; y el apartado e) del mismo artículo en lo que se refiere a las transferencias internacionales de datos previstas a terceros países, con indicación también, en su caso, de los destinatarios o categorías de destinatarios. Por lo tanto, se recomienda incluir en este fichero un apartado específico para las transferencias internacionales de datos previstas a terceros países, indicando, en su caso, que no se harán transferencias internacionales de datos.

Asimismo, se recomienda aprovechar la oportunidad para modificar los demás ficheros creados mediante el acuerdo del Pleno de la Diputación con fecha del 17 de junio de 2005, a fin de adecuar su contenido a las exigencias del artículo 54.1 del RLOPD.

3.- Igualmente, será necesario cumplir estrictamente con el principio de seguridad de los datos, especialmente velando por evitar errores en la confección de las plantillas relacionadas con cada huella dactilar.

En este sentido, el RLOPD dispone que las medidas de seguridad correspondientes a cada fichero con datos de carácter personal se establecerán de acuerdo con la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información, y con independencia de cuál sea el sistema de tratamiento empleado.

El fichero de «personal» contempla, en el apartado relativo a las medidas de seguridad, la aplicación de un nivel alto (artículo 81.3 del RLOPD) en atención a las diversas tipologías de datos personales tratados: datos identificativos, datos de características personales, datos académicos y profesionales, datos de ocupación laboral y datos económico-financieros. Este nivel de seguridad se considera conforme con la normativa en materia de protección de datos, y la inclusión del tratamiento de las huellas dactilares de los empleados en dicho fichero no alterará este nivel asignado inicialmente.

En caso de que la Diputación opte por crear un nuevo fichero, se recuerda que, de acuerdo con la naturaleza de los datos personales que se tratarán, en principio, datos identificativos (huellas dactilares, números identificadores de los empleados, acrónimos, etc.), podría ser suficiente la aplicación del nivel de seguridad básico, de acuerdo con lo dispuesto en el artículo 81.1 del RLOPD. Sin embargo, en la medida en que el lapso temporal de almacenamiento de los datos pueda permitir hacer una avaluación de determinados aspectos de los comportamientos de los empleados (puntualidad, ausencias, períodos de vacaciones, personas con las que se entra o sale del centro de trabajo, etc.), serían también exigibles medidas de nivel medio.

En este sentido, hay que destacar que mientras que el artículo 4.4 del Reglamento de Medidas de Seguridad aprobado por el Real Decreto 994/1999, de 11 de junio, establecía el nivel medio cuando la información permita «la evaluación de la personalidad del individuo», el artículo 81.2 f) del nuevo RLOPD exige este nivel cuando la información permita evaluar «determinados aspectos de la personalidad o el comportamiento» de las personas.

Por otro lado, se recuerda que, en atención a las particulares circunstancias que comporta el tratamiento de datos biométricos y a los riesgos que se pueden derivar del mismo, es recomendable adoptar determinadas medidas de seguridad de nivel superior para evitar la pérdida accidental, la alteración, la difusión o el acceso no autorizado a tales datos biométricos. Y es que hay que poner de manifiesto la

importancia de tener en cuenta el problema de seguridad que puede ocasionar la pérdida de este tipo de información para la Diputación.

En particular, a fin de garantizar la integridad y la confidencialidad de los datos biométricos tratados, es recomendable mantener un registro de accesos (artículo 103 del RLOPD), y, especialmente, para el caso de un tratamiento de datos biométricos que incluya su transmisión dentro de una red (intranet, extranet o Internet) o mediante redes inalámbricas de comunicaciones electrónicas, es recomendable codificar los datos o bien emplear cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (artículo 104 del RLOPD). En cualquier caso, se trata de una recomendación para mejorar la seguridad, tanto de la propia organización como de las otras organizaciones que utilicen un sistema de identificación basado en la misma huella dactilar.

En caso de que se modifique el fichero de «personal» existente actualmente, serían exigibles todas las medidas de seguridad de nivel alto.

Conclusiones

Los datos biométricos, como la huella dactilar, son equiparables a los rasgos fisiológicos o de comportamiento de una persona, por lo que tienen la consideración de datos de carácter personal, en los términos establecidos por los artículos 3 a) de la LOPD y 5.1 f) del RLOPD.

El uso de sistemas de control horario mediante la huella dactilar de los empleados de la Diputación Provincial se considera conforme a los principios de proporcionalidad y calidad de los datos (artículo 4 de la LOPD), dado que el tratamiento de las huellas dactilares se considera adecuado, pertinente y no excesivo en relación con la finalidad de controlar el cumplimiento horario de los empleados.

No es necesario requerir el consentimiento de sus empleados para el tratamiento de sus huellas dactilares, de acuerdo con lo que establece el artículo 6.2 de la LOPD.

El tratamiento de los datos personales biométricos referidos a las huellas dactilares obliga a la Diputación Provincial a cumplir con los demás principios y obligaciones de la LOPD, especialmente, el deber de informar a los afectados (artículo 5.1 de la LOPD), la modificación del fichero de «personal» creado mediante acuerdo del Pleno del 17 de junio de 2005, o bien la creación e inscripción de un fichero específico para este tratamiento (artículo 20 de la LOPD) y la adopción de las medidas de seguridad exigibles de acuerdo con lo expuesto, así como la conveniencia de la aplicación de las medidas adicionales a las que se ha hecho referencia, en atención a la naturaleza de la información tratada y los riesgos previsibles.