

Dictamen en relación con una consulta sobre el sistema de control horario del personal adscrito a un Departamento de la Administración de la Generalitat de Cataluña, mediante la huella dactilar.

Se presenta ante la Agencia Catalana de Protección de Datos un escrito de una institución competente en materia de derechos de los ciudadanos, en el que se solicita la opinión de la Agencia en relación con la adecuación de la instalación de un sistema de control horario del personal de un Departamento de la Administración de la Generalitat de Cataluña, mediante la huella dactilar, 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 consulta planteada por una institución competente en materia de derechos de los ciudadanos hace necesario analizar si el tratamiento de la huella dactilar de los empleados de un Departamento de la Administración de la Generalitat (en adelante, el Departamento), 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.

III

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 del Departamento, 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 del Departamento 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 del Departamento, 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, habrá 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 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 funcionario 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), especialmente si se trata de algún Departamento que, por las competencias que tiene atribuidas, requiere la adopción de medidas de seguridad especiales.

De acuerdo con todas estas consideraciones, se puede llegar a admitir la recogida de datos biométricos, como las huellas dactilares, del personal de la Administración de la Generalitat como medida de control horario por parte del Departamento. 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 el Departamento 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, el Departamento 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 se 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 el Departamento para elegir el medio de control horario que

considere más adecuado, se recomienda valorar la posibilidad de optar por un sistema menos restrictivo.

IV

Sin perjuicio de las consideraciones anteriores, en caso de que el Departamento proceda a la instalación del sistema de control horario basado en las huellas dactilares de sus empleados, se recuerda que está obligado a cumplir los demás principios y obligaciones establecidos por la normativa de protección de datos personales. Entre otras cosas:

- Será necesario cumplir con el principio de información establecido en el artículo 5.1 de la LOPD, según el cual:

«Los interesados a los que se soliciten datos personales deberán ser previamente 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.»

- Con carácter previo a la recogida de los datos personales, el Departamento deberá crear, declarar e inscribir en el 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).

Este fichero de datos personales se tendrá que crear necesariamente antes de la puesta en marcha del sistema de control horario o del inicio de la recogida de los datos personales, a fin de legitimar el tratamiento de dichos datos por parte del responsable, el Departamento, conforme a lo dispuesto en la normativa de protección de datos.

Concretamente, el artículo 20.1 de la LOPD dispone que la creación de los ficheros de las Administraciones públicas sólo se puede efectuar mediante una disposición de carácter general publicada en el boletín oficial correspondiente, que deberá especificar el contenido de todos los elementos incluidos en el apartado 2 del mismo artículo.

El apartado 2 del artículo 20 de la LOPD establece, taxativamente, los apartados que deberán incluir las disposiciones de creación de ficheros, concretamente: la finalidad del fichero y los usos previstos; las personas o los colectivos sobre los que se obtengan 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 incluyan; 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 ejercitar los correspondientes derechos; y, finalmente, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible.

Asimismo, hay que tener en cuenta que el RLOPD, en relación con el contenido de la disposición de creación de ficheros, ha concretado o añadido (artículo 54.1) varias cuestiones en relación con lo establecido en el artículo 20.2 de la LOPD, y que, por tanto, se deberán consignar cuando se cree el fichero de datos correspondiente. En concreto, respecto a los datos de carácter personal tratados, no sólo hay que especificar el procedimiento de recogida de los datos, sino también su procedencia (apartado b); respecto a la estructura básica del fichero, hay que hacer una descripción detallada de los datos identificativos (entre ellos, las huellas dactilares) y, en su caso, de los datos especialmente protegidos, así como de las demás categorías de datos personales que se incluirán, y habrá que indicar el sistema de tratamiento utilizado en la organización (apartado c); y, respecto a las transferencias internacionales de datos, hay que indicar, en su caso, los países de destino de los datos (apartado e).

En este sentido, la disposición adicional tercera de la Ley 5/2002, de 19 de abril, habilita a los consejeros y consejeras de la Generalitat, dentro del ámbito de las competencias respectivas, para la creación, la modificación y la supresión, mediante orden, de los ficheros que sean pertinentes.

- 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 del sistema de tratamiento empleado.

De acuerdo con la naturaleza de los datos personales que serán tratados (en principio, datos identificativos), podría ser suficiente la aplicación del nivel de seguridad básico, de acuerdo con lo establecido 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 evaluación de determinados aspectos de los comportamientos de los empleados (puntualidad, ausencias, periodos 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 nivel medio cuando la información permitiera «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 el Departamento, así como para aquellas otras instituciones que también hayan optado por este tipo de sistema de control como mecanismo para asegurar el control en el acceso de personas a determinados lugares o servicios que requieren un grado de seguridad mayor.

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.

De acuerdo con las consideraciones efectuadas hasta ahora en relación con la consulta sobre el sistema de control horario, mediante la huella dactilar, del personal adscrito al Departamento, se formulan las siguientes

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 del Departamento 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 al Departamento 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 creación y la inscripción del correspondiente fichero de datos personales (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.