VIII

NUEVAS TECNOLOGÍAS Y PROPIEDAD INTELECTUAL

Reglamento sobre la Biometría en el centro de trabajo

03 de abril de 2019

La reciente obligación de registro de jornada de trabajo, recogida en el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, que entrará en vigor el próximo 12 de mayo de 2019, servirá para controlar que no se excedan las jornadas laborales máximas exigidas en el Estatuto de los Trabajadores y que, en su caso, las horas extras sean retribuidas a los empleados. Sin embargo, la normativa no concreta la forma de realizar dicho registro, razón por la que muchas compañías han optado por hacer uso de datos biométricos para cumplir con la reciente disposición.

Ante este creciente y cada vez mayor uso de datos biométricos, calificados como datos sensibles por el Reglamento General de Protección de datos y sujetos, por lo tanto, a una mayor protección, la Comisión Nacional de Informática y de las Libertades (en adelante, "CNIL") ha adoptado un Reglamento relativo a la **biometría en el lugar de trabajo**, que especifica las obligaciones de los empleadores que desean utilizar dispositivos biométricos para controlar el acceso a los espacios de trabajo con el fin de garantizar la máxima seguridad en el uso de los datos personales de los empleados. Estas directrices de carácter europeo servirán como guía para conocer el alcance y los límites del uso de datos biométricos en nuestro Ordenamiento Jurídico.

En este sentido, la **biometría** consiste en un proceso de verificación de la identidad y autenticación de un individuo mediante el uso de características inherentes a su persona, como la cara o la huella dactilar. Estos datos son calificados como **sensibles** porque a través de ellos los individuos son identificados por lo que son, y no por lo que se sabe (como una contraseña) ni por lo que se tiene (como un documento de identidad). Por esta razón, cualquier violación o uso indebido de estos datos da lugar a violaciones significativas de los derechos y libertades de las personas afectadas, ya que una violación de tales datos puede ser irreversible. Así, el tratamiento de datos biométricos está prohibido en principio, con algunas excepciones previstas en el texto.

Obligaciones

Este Reglamento se aplica a toda utilización de datos biométricos impuesta por un empleador en virtud del Derecho público o privado a su personal para controlar el acceso a los locales, las aplicaciones y los instrumentos profesionales. El Reglamento, además de proporcionar un marco para el uso de la biometría, establece las siguientes **obligaciones**:

- La compañía debe **justificar el uso** de la biometría, basándose, entre otras cuestiones, en el contexto o en las limitaciones técnicas y reglamentarias, que son detalladas de forma concreta para los tipos de biometría que presentan los mayores riesgos.

- La compañía debe **documentar** las diferentes opciones que se toman al implementar los dispositivos biométricos.

- La compañía debe cumplir con **medidas de seguridad** organizativas y técnicas.

- La compañía debe **cumplir con el Reglamento General de Protección de Datos**, en particular con la obligación de **informar** a las personas afectadas, así como exigir que los responsables del tratamiento lleven a cabo una **evaluación de impacto**.

Responsable del Tratamiento

El **Responsable del Tratamiento** es la persona, física o jurídica, que determina las finalidades y medios del mismo, es decir, el empleador. Con habitualidad, el diseño y la instalación del sistema de control de acceso biométrico se subcontrata a un proveedor externo, que será el **Encargado del Tratamiento**. El responsable deberá asegurarse de que el encargado ofrece garantías suficientes en materia de protección de datos.

Corresponderá a los responsables del tratamiento decidir y **justificar** la elección de las características biométricas requeridas, desde el análisis de características morfológicas (huella dactilar, forma de la mano, iris…) hasta características biológicas (saliva, sangre, ADN…) o conductuales. Los medios utilizados para garantizar dicho control deben respetar el **principio de proporcionalidad.** Por lo tanto, el empresario tendrá que justificar su necesidad de implantar un dispositivo biométrico, en comparación con otras soluciones de control menos intrusivas. Las **obligaciones del Responsable del Tratamiento** son las siguientes:

- Justificar los contextos que exijan un **alto nivel de protección**, como la manipulación de maquinaria o productos peligrosos, el acceso a fondos u objetos de valor, equipos o productos sujetos a una reglamentación específica (sustancias psicotrópicas, productos químicos, etc.).

- **Demostrar** la insuficiencia o inadecuación de **medios menos intrusivos**, como una tarjeta de identificación o un código de acceso.

Al registrar a un usuario en un dispositivo biométrico, el sistema toma una serie de medidas de las características morfológicas (huella dactilar, forma de la mano, iris…), biológicas (orina, sangre…) o conductuales de la persona afectada. Estas medidas almacenadas son las denominadas **"plantillas"**, que reflejan el nivel de control que tienen los interesados sobre la forma en que el responsable del tratamiento almacena sus datos biométricos.

Tipos de Dispositivos Biométricos

El Reglamento distingue tres tipos de **dispositivos biométricos**:

Tipo 1.

- La plantilla está bajo el **control de la persona interesada.**

- Los soportes de almacenamiento de las plantillas son individuales (un soporte sólo puede contener una plantilla) y están en posesión de cada empleado (sin que el

empleador o los proveedores conserven ninguna copia).

- Al no existir una base de datos centralizada de plantillas biométricas para todos los empleados, el **riesgo** de exposición de los datos ante cualquier vulneración en la seguridad es muy **bajo.**

Tipo 2.

- La plantilla está bajo **control compartido**, ya que existe una base de datos con los datos de todos los empleados.

- Los datos están **cifrados** por lo que no pueden leerse ni utilizarse sin la intervención de la persona interesada. Para ello, se asigna a cada persona un elemento personal (por ejemplo, un código) que debe presentarse al dispositivo en el momento de la autenticación.

- El **riesgo** de que se expongan los datos biométricos de los interesados es **bajo** porque los datos son ilegibles.

Tipo 3.

- La plantilla está bajo el **control del controlador**.

- Las plantillas de los empleados se almacenan en una base de datos centralizada. El empleado no tiene control sobre el medio de almacenamiento.

- La existencia de una base de datos centralizada permite que estos datos se filtren, lo que podría **exponer de forma irreversible los datos biométricos** de las personas afectadas.

El almacenamiento de Tipo 1 es el que mejor garantiza los derechos y libertades de las personas afectadas. La utilización de los métodos de almacenamiento Tipos 2 y 3 debe ser excepcional y estar justificada por consideraciones específicas, como entornos especialmente críticos en los que la pérdida de, por ejemplo, una tarjeta de identificación tendría consecuencias graves para el desarrollo de las operaciones.

Obligación Legal

La **obligación legal** o el **interés legítimo** son las bases jurídicas más idóneas para justificar el dispositivo biométrico elegido, a diferencia del consentimiento, que debido a la relación jerárquica entre el empresario y sus empleados crea un desequilibrio en las relaciones que puede afectar a la naturaleza libre del mismo. Por ello, el consentimiento sólo en muy raras ocasiones puede conservarse como base jurídica para el tratamiento de datos en el lugar de trabajo. Aun así, si el empleador desea contar con el consentimiento de los trabajadores debe asegurarse de que exista una verdadera libertad de elección de los empleados, ofreciendo a las personas una solución alternativa para que puedan elegir la opción que mejor se adapte a sus necesidades, sin que ninguna consecuencia influya en dicha elección.

La organización empleadora debe llevar a cabo un **análisis interno**, registrada **por escrito**, sobre la **necesidad** de establecer un tratamiento de datos biométricos y sobre la **proporcionalidad** de las modalidades de su aplicación. La elección de un tipo de dispositivo biométrico que exponga en mayor medida los datos personales deberá ser documentado con especial detalle. Esta documentación deberá poder presentarse en caso de control por parte de la CNIL.

También deberá documentarse la reflexión sobre los riesgos para los derechos e intereses de los interesados, así como las medidas adoptadas para limitar estos riesgos, es decir, realizar una **evaluación de impacto** antes de que se lleve a cabo la operación de tratamiento.

Estos documentos deben **actualizarse periódicamente**, y **al menos cada tres años**, en particular en lo referido a la evaluación de riesgos y a las medidas de seguridad.

Departamento: Tecnología y Propiedad Intelectual
Contacto: Joaquín Muñoz jmunoz@ontier.net