CNS 63/2018

Dictamen en relación con la consulta formulada por un colegio profesional sobre la utilización de sistemas de control basados en la huella dactilar

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de un colegio profesional en lo que se pide que la Autoridad emita un dictamen para valorar si la utilización de sistemas de control basados en la huella dactilar puede suponer una vulneración de la legislación sobre protección de datos.

En concreto, la consulta se refiere a dos situaciones: por una parte, la utilización de sistemas de fichaje mediante huella dactilar con finalidad de control horario de los trabajadores; por otra parte, también se plantea en relación con el acceso a determinadas instalaciones que la consulta identifica como instalaciones de seguridad del Colegio (centros de procesamiento de datos y archivo).

Analizada la consulta, que no se acompaña de ninguna otra documentación, y de acuerdo con el informe de la Asesoría Jurídica, emito el siguiente dictamen:

I

(...)

II

En relación con la primera de las cuestiones planteadas, la instalación de un sistema de control de acceso y horario basado en la recogida y tratamiento de un patrón de la huella dactilar de los empleados implica el tratamiento de sus datos personales, ya que por dato personal hay que entender *"toda información sobre una persona física identificada o identificable («el interesado»)* (art. 4.1 del Reglamento 2016/679, del Parlamento y del Consejo, de 27 de abril, general de protección de datos (en adelante, RGPD)).

En lo concerniente a la huella dactilar o al patrón de la huella dactilar se trata, además, de datos que deben ser calificados como datos biométricos, ya que de acuerdo con el artículo 4.14 del RGPD tienen esta consideración cuando han sido *"obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*";

Esto hace que, de acuerdo con el artículo 9.1 del RGPD, a los datos relativos a las huellas dactilares se les deba aplicar el régimen específico previsto para las categorías especiales de datos previsto tanto en el artículo 9 como en otros artículos del RGPD.

En este sentido, el considerando 51 del RGPD pone de manifiesto el carácter restrictivo con el que se puede admitir el tratamiento de estos datos:

> *"(51) (...) Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.*
>
> *(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. (...)"*

De acuerdo con estas consideraciones, el tratamiento de datos biométricos requerirá no solo la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD, sino que también deberá concurrir alguna de las excepciones previstas en el artículo 9.2 del RGPD.

Esta Autoridad ya ha analizado, en dictámenes anteriores (por ejemplo, CNS 9/2009, CNS 22/2009 o 22/2011), la adecuación a la normativa en materia de protección de datos personales de los sistemas de control de acceso y horario de los empleados de las administraciones públicas mediante datos biométricos (como la huella digital o un patrón biométrico). Estos dictámenes, y otros, pueden ser consultados en la página web www.apd.cat.

De conformidad con el artículo 6.2 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y con el principio de calidad de los datos (artículo 4 de la LOPD), aplicables por razones temporales a los supuestos que se analizaban en aquellos dictámenes, la Autoridad consideró, en supuestos similares a los que se examinan en este dictamen, que, en la medida en que la recogida de datos personales de los trabajadores públicos se realizaba dentro de una relación jurídica laboral o administrativa y tenía como finalidad el control, precisamente, de su cumplimiento al amparo de lo establecido en el artículo 20.3 del Estatuto de los trabajadores (TE), el responsable podía tratar y recoger los datos

biométricos consistentes en la huella digital o el patrón biométrico de sus trabajadores sin necesidad de requerir su consentimiento.

En este sentido, se pronunciaba la Sentencia del Tribunal Supremo de 2 de julio de 2007, fundamento séptimo, recalcando que la finalidad perseguida con este sistema *"es plenamente legítima: el control del cumplimiento del horario de trabajo al que viene obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Además, no parece que la toma en las condiciones expuestas, de una imagen de la mano, incumpla las exigencias del artículo 4.1. Por el contrario, puede considerarse adecuada, pertinente y no excesiva*", a la que se remiten otras sentencias que enjuician supuestos similares, como por ejemplo la Sentencia del Tribunal Superior de Justicia de la Región de Murcia de 25 de enero de 2010 o la Sentencia de la Audiencia Nacional de 4 de marzo de 2010. En el mismo sentido se señalaba el Auto del Tribunal Constitucional de 26 de febrero de 2007, en especial con respecto a los argumentos referidos a la doctrina de la proporcionalidad.

Sin embargo, la aprobación y la plena aplicabilidad del RGPD han introducido algunos elementos adicionales que afectan al análisis que se puede hacer de la utilización de datos biométricos en el entorno laboral.

III

Con la aprobación del RGPD, y desde el punto de vista de la base jurídica del tratamiento, no solo es posible acudir a la base jurídica prevista en el artículo 6.1.*b* del RGPD (que el tratamiento sea necesario para la ejecución de un contrato en el que la persona interesada es parte), sino que también es posible, en el caso de sujetos a los que sea aplicable, acudir a la base jurídica establecida en el artículo 6.1.*f* (que el tratamiento sea necesario para satisfacer el interés legítimo del empleador en la correcta ejecución de las prestaciones derivadas del contrato de trabajo), tal como había reconocido el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de las tecnologías biométricas. Sea como sea, el elemento clave será la determinación de la necesidad del tratamiento. No ya de la necesidad de hacer algún tipo de control, sino de hacerlo a través de la técnica propuesta, eso es el uso de sistemas de identificación basados en datos biométricos.

Por otra parte, y tal como pone de relieve el considerando 51 del mismo RGPD, en la medida en que los datos biométricos han pasado a ser considerados como una categoría especial de datos (art. 9.1 RGPD), será necesario que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD que permiten levantar la prohibición general del tratamiento de estos tipos de datos establecida en el artículo 9.1.

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será de aplicación cuando "*el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados*

miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".

Por lo tanto, para poder aplicar esta excepción será necesaria la concurrencia de dos condiciones:

a) Que el tratamiento sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos específicos del empleador o de la persona interesada en el ámbito del derecho laboral o de la seguridad y protección social.

b) Que lo autorice el derecho de la Unión o de los Estados miembros o un convenio colectivo, que establezca garantías adecuadas del respeto de los derechos fundamentales y los intereses de las personas afectadas.

En lo concerniente a la posibilidad de que el derecho de los Estados miembros lo autorice, el considerando 41 del RGPD dispone que *"cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento",* pero añade que ello se debe entender *"sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate".* En el caso del Estado español, de acuerdo con las exigencias constitucionales, la norma que lo prevea, por tratarse del desarrollo de un derecho fundamental, deberá tener rango de ley (artículo 53 CE).

En este sentido, el artículo 88 del RGPD ha establecido que los Estados miembros pueden, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y las libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular, entre otros, a efectos del cumplimiento de las obligaciones que establece la ley o el convenio colectivo, la gestión, planificación y organización del trabajo. Estas normas deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, en particular, en relación con, entre otros, los sistemas de supervisión en el puesto de trabajo.

Cada Estado miembro debe notificar a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1.

En el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores, pero no se refiere en ningún momento a una autorización para la utilización de categorías especiales de datos o, en concreto, de datos biométricas, con esta finalidad:

> "*3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad*".

Los artículos 87, 89 y 90 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), sí que han previsto y han regulado las condiciones y garantías con las que puede hacerse el control de los trabajadores por parte del empresario con respecto a la utilización de los dispositivos digitales puestos a su disposición por parte del empresario, la utilización de sistemas de videovigilancia en el puesto de trabajo o la utilización de sistemas de geolocalización en el ámbito laboral, pero no contienen ninguna referencia a la posibilidad de utilización de datos biométricas en sistemas de control en el ámbito laboral, como sería el caso del control horario.

Esta autorización para implantar sistemas de control sería aún más necesaria en el caso de sistemas basados en datos biométricos, teniendo en cuenta la condición de categoría especial de estos datos y los términos poco precisos con que se pronuncia el actual artículo 20.3 del ET. La falta de previsión expresa de una autorización en el derecho laboral, que ahora requiere el artículo 9.2.b) del RGPD hace que puedan surgir dudas respecto a la admisibilidad de este tipo de sistemas de control horario en el ámbito laboral.

Por otra parte, y al margen de esta cuestión relacionada con la exigencia de que la utilización de los datos biométricos esté autorizada por una norma con rango de ley, hay que tener en cuenta que en cualquier caso el tratamiento debe cumplir con el resto de los principios y obligaciones derivados de la normativa de protección de datos, en especial, del principio de minimización (art. 5.1.c) RGPD).

Así se desprende tanto de la misma redacción del artículo 9.2.b) del RGPD, que exige que el tratamiento sea "necesario", como de la Recomendación CM/Rec(2015) 5 del Consejo de Ministros del Consejo de Europa a los Estados miembros sobre el tratamiento de datos personales en el contexto laboral. En concreto, el principio 18 de esta Recomendación establece lo siguiente:

> *"18.1. La recopilación y posterior procesamiento de los datos biométricos solo se deberían emprender cuando hay que proteger los intereses legítimos de empresarios, empleados o terceros, solo si no hay otros medios menos intrusivos disponibles y solo si se acompaña de las garantías adecuadas previstas en el principio 21.*
>
> *18.2. El tratamiento de los datos biométricos se debe basar en métodos científicamente reconocidos y debe estar sujeto a los requisitos de estricta seguridad y proporcionalidad".*

En este sentido, el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de las tecnologías biométricas afirmaba lo siguiente en relación con el análisis del cumplimiento de este principio:

> *"Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar[1]. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro,*

entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".

Parece clara la necesidad de admitir la instalación de sistemas de control del cumplimiento horario por parte de los trabajadores, tal como había reconocido reiteradamente esta Autoridad, de acuerdo con las decisiones judiciales que se han mencionado más arriba. Ahora bien, una vez que los datos biométricos hayan pasado a ser considerados como datos especialmente protegidas, no parece tan claro que el uso de sistemas de control horario basados en este tipo de datos deba ser admitido como medio preferente para llevar a cabo el control. Más bien al contrario. Dada la especial naturaleza de estos datos, parece que se deberá optar en primer lugar por otros sistemas de control que, sin utilizar categorías de datos especialmente protegidos, puedan permitir alcanzar la misma finalidad.

Las exigencias derivadas de la protección de datos en el diseño (art. 25.1 RGPD) y, en especial, del principio de minimización, obligan a escoger aquella tecnología que resulte menos intrusiva desde el punto de vista de la protección de datos. El principio de minimización no se manifiesta solo a la hora de optar por alternativas que no impliquen el tratamiento de datos personales, o de llevar a cabo el tratamiento de datos de manera que se utilicen los datos mínimos indispensables, sino que también debe conllevar que, si se puede alcanzar una determinada finalidad sin tener que tratar datos de categorías especiales, esta opción debe prevalecer ante otras opciones que sí que impliquen el tratamiento de estos tipos de datos.

Hay que tener en cuenta que los datos biométricos, dado su carácter personal y único, constituyen un medio fiable de identificación (aunque en determinados datos biométricos pueda existir un riesgo de no identificabilidad). Sin embargo, la fiabilidad como sistema de identificación está condicionada también por la amplitud con la que se puedan utilizar estos sistemas de identificación. Cuanto mayor sea el número de sistemas de identificación que se basan en unos datos biométricos o en una plantilla obtenida a partir de datos biométricos, mayor es el riesgo de que estos datos puedan acabar siendo utilizados de manera inadecuada y dando lugar a un riesgo de usurpación o suplantación de identidad. Este riesgo se puede incrementar claramente en función de cuál sea la tecnología utilizada y del tratamiento que se dé a los datos biométricos en bruto u originales.

Por una parte, una pérdida de confidencialidad de estos datos podría permitir, en función de la tecnología utilizada, la suplantación. Pero es que, además, estos datos no son modificables. Es decir, a diferencia de una contraseña, en caso de pérdida no se pueden cambiar.

Por otra parte, también existen riesgos evidentes si la tecnología utilizada no garantiza de manera suficiente que la plantilla obtenida a partir de los datos biométricos no coincidirá con la utilizada en otros sistemas similares.

Es innegable que la utilización de sistemas basados en datos biométricos para llevar a cabo el control horario evita el riesgo de suplantación que se puede producir en algún caso. Ahora bien, no parece que sea el único sistema que permita garantizarlo. Por ejemplo, a efectos del control horario, el uso de tarjetas personales u otros tipos de objetos (*tokens*) en un sistema de marcaje, la utilización de códigos personales, la visualización directa del punto de marcaje o el uso de sistemas de videovigilancia donde quede constancia de la hora de entrada o salida

pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas eficaces para llevar a cabo el control.

En virtud de estas consideraciones, algunas autoridades de control en materia de protección de datos no han admitido la utilización de sistemas de control basados en datos biométricos como sistema generalizado de control horario de los trabajadores por parte del empresario. Sería el caso de la Commission Nationale de l'Informatique et des Libertés (CNIL) de Francia o Garante per la protezione dei dati personali de Italia.

En la consulta formulada se hace referencia a la información que se ofrece en el apartado de preguntas frecuentes de la AEPD y a la resolución de la Agencia Vasca de Protección de Datos¸ de 19 de diciembre de 2016, en la que se admitía la utilización de un sistema descentralizado de control basado en datos biométricos. Sin embargo, cabe decir que, si bien se hace referencia a la aprobación del RGPD, en ambos casos hay una remisión a la jurisprudencia anterior a la RGPD, la cual había admitido, tal como también había hecho esta Autoridad en los dictámenes mencionados al principio, la utilización de datos biométricos para sistemas de control horario en el ámbito laboral.

Más allá de ello, en la consulta no se expone cuáles son las circunstancias que justificarían este tipo de control ni tampoco qué motivos impedirían utilizar otros sistemas de control que no impliquen el tratamiento de categorías especiales de datos y que, por lo tanto, sean menos intrusivos en relación con el derecho a la protección de datos de las personas afectadas.

Dadas estas circunstancias, no parece que se pueda concluir la proporcionalidad de la utilización de la huella dactilar para establecer un sistema de control horario en el caso descrito en la consulta.

En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo, teniendo en cuenta las implicaciones tecnológicas de la tecnología utilizada, la observación sistemática de los hábitos de los trabajadores y el tratamiento de datos de una categoría especial (biométricos), sería preciso llevar a cabo una evaluación del impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos (art. 35 RGPD).

IV

En la consulta se plantea todavía otro supuesto, consistente en la utilización de la huella dactilar para controlar el acceso a determinadas dependencias que requieran una mayor seguridad. En la consulta se identifican como tales los centros de procesamiento de datos o los archivos.

A diferencia del caso anterior, aquí, si se accede a las dependencias de que se trate, el posible daño que se produzca, la destrucción, alteración, sustracción o el acceso indebido a la información o a los sistemas de información contenidos en estas dependencias será difícil de reparar. No se trataría solo de tener constancia de quien accede a estas dependencias, sino también de evitar que personas no autorizadas puedan acceder a ellas. Siendo así, sistemas como la instalación de cámaras de videovigilancia no serían sistemas eficaces, pero en cambio

sí que puede haber otros sistemas (claves, código personal, token) que sí que pueden resultar eficaces.

Como en el caso anterior resulta esencial que se cumpla el principio de proporcionalidad o de minimización de los datos personales a la hora de determinar cuál es el sistema de control que se aplica.

De entrada parece plausible que la necesidad de aplicar sistemas de control de acceso más robustos para el acceso a determinadas dependencias que pueden contener información sensible pueda parecer más justificada que en el caso de la finalidad de control horario. No obstante, tampoco parece que se pueda concluir de manera automática la justificación de la medida.

De acuerdo con el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29, sobre la evolución de las tecnologías biométricas, "*como norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable. Para ello, el responsable del tratamiento deberá probar que determinadas circunstancias plantean un riesgo considerable específico, que deberá evaluar con especial cuidado. Con el fin de cumplir con el principio de proporcionalidad, el responsable del tratamiento, ante estas situaciones de alto riesgo, deberá verificar si posibles medidas alternativas podrían ser igualmente eficaces pero menos intrusivas en relación con los objetivos perseguidos, y optar por tales alternativas. La existencia de las circunstancias en cuestión también deberá revisarse periódicamente. Sobre la base de esta revisión, las operaciones de tratamiento de datos que no se justifiquen deberán concluirse o suspenderse".*

Por lo tanto, habrá que ver, en atención a la naturaleza de la información custodiada y las repercusiones que podría tener un acceso indebido a estas dependencias, cuáles son los riesgos que hay que afrontar, así como cuáles son las posibles alternativas. Más allá de identificar el tipo de dependencias (centros de procesamiento y archivo), en la consulta no se ofrece ninguna otra información que permita evaluar los riesgos ni analizar las posibles alternativas.

En cualquier caso, y para el supuesto de que, después de realizar la evaluación de impacto a la que nos hemos referido en el fundamento jurídico anterior, se pueda concluir que la medida resulta proporcionada, de acuerdo con el Dictamen 3/2012 del Grupo de Trabajo del Artículo 29 sobre la evolución de las tecnologías biométricas y sin perjuicio de lo que resulte del análisis de riesgos que se lleve a cabo, conviene tener en cuenta algunas medidas técnicas para minimizar los riesgos:

a) Conviene evitar el almacenamiento de datos biométricos en bruto, y conservar solo las plantillas obtenidas a partir de estos datos.
b) La plantilla se debe extraer de manera que se pueda prever que no podrá ser utilizada por otros responsables del tratamiento para fines similares.

c) Se debe dar preferencia a los sistemas de almacenamiento descentralizados, evitando la creación de bases de datos centralizadas con estos tipos de datos. De acuerdo con el modelo descentralizado que se propone, las plantillas biométricas se conservarían exclusivamente en poder de las personas interesadas mediante una tarjeta o dispositivo, de manera que la pérdida de las mismas tendría unos efectos limitados.
d) Los datos se deben conservar cifrados.

Todo ello aparte de la necesidad de facilitar información transparente a las personas afectadas sobre el tratamiento que se pretende llevar a cabo de manera que puedan comprender el alcance y las consecuencias que podría tener este tratamiento.

De acuerdo con las consideraciones hechas en estos fundamentos jurídicos en relación con la consulta planteada en relación con la utilización de sistemas de control basados en la huella dactilar, se extraen las siguientes

Conclusiones

La inclusión de los datos biométricos, entre ellos los de la huella dactilar, entre las categorías especiales de datos previstas por el RGPD no permite concluir de manera automática que la implantación de un sistema de control horario basado en la recogida de este tipo de datos pueda considerarse proporcionada y, por lo tanto, conforme con el principio de minimización. Hay que hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en las que se lleve a cabo el tratamiento para determinar su legitimidad y proporcionalidad, incluido el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas.

En el caso del control de acceso a dependencias o zonas que requieran unas condiciones de seguridad reforzadas, el uso de este tipo de sistemas puede resultar justificado en determinados casos, si bien también resulta necesario llevar a cabo con carácter previo la evaluación del impacto en la protección de datos.

Barcelona,14 de febrero de 2019