

## **Informe en relación con el Proyecto de Orden por el que se aprueba el Catálogo de sistemas de identificación y firma electrónica**

Se presenta a la Autoridad Catalana de Protección de Datos el Proyecto de Orden por el que se aprueba el Catálogo de sistemas de identificación y firma electrónica.

El Proyecto de Orden se estructura en 5 artículos, una disposición derogatoria una disposición final y un anexo.

Analizado el Proyecto, que se acompaña de la memoria general de la disposición y teniendo en cuenta la normativa vigente aplicable, de acuerdo con el informe de la Asesoría Jurídica, emito el siguiente informe.

### **Fundamentos jurídicos**

y  
(...)

#### **II**

El Proyecto de orden tiene por objeto, de acuerdo con lo que prevé el artículo 1, "aprobar el Catálogo de sistemas de identificación y firma electrónica para efectuar los trámites y procedimientos de las personas interesadas con la Administración de la Generalidad".

El artículo 2 determina el ámbito subjetivo de la Orden, que se aplica a los departamentos de la Administración de la Generalidad de Cataluña, a los organismos públicos y entidades de derecho público vinculados o dependientes de la Administración de la Generalidad ya los consorcios adscritos a la Administración de la Generalidad.

Es necesario remarcar que la utilización de estos sistemas de identificación y firma en la tramitación administrativa comporta el tratamiento, por parte de los sujetos sometidos al ámbito de aplicación de la Orden, de datos personales de los interesados que utilizan estos sistemas de identificación y firma, entendiendo como dato personal, de acuerdo con el artículo 4.1 del RGPD, "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un número, un número de identificación, datos de localización, un identificador online o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

El artículo 5.1.a) del RGPD establece que los datos personales recogidos deben ser tratados de forma lícita, leal y transparente en relación con el interesado. Para que este tratamiento sea lícito es necesario que concurra alguna de las condiciones previstas en el artículo 6.1 RGPD y, en caso de que

se trate de categorías especiales de datos, es necesario tener en cuenta también las previsiones del artículo 9 RGPD.

Con carácter general, el tratamiento de los datos personales por las administraciones públicas en el procedimiento administrativo, ya sea presencial o por medios electrónicos, puede encontrar su base jurídica en el artículo 6.1.e) del RGPD, según el cual existe habilitación legal para el tratamiento de datos personales cuando "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

Tal y como se desprende del artículo 6.3 del RGPD y recoge expresamente el artículo 8 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante LOPGDD) el tratamiento de datos sólo puede considerarse fundamentado en la base jurídica del artículo 6.1.e) del RGPD cuando así lo establezca una norma con rango de ley.

Una primera consecuencia de ello es que la orden que se analiza (al igual que el Decreto 76/2020, de 4 de agosto, de Administración digital, que desarrolla) no constituye un instrumento apto para habilitar la existencia de nuevos tratamientos. Ahora bien, esta norma puede concretar las condiciones en las que se llevan a cabo tratamientos que ya están previstos con normas con rango de ley reguladoras del procedimiento administrativo, como pueden ser en caso de que nos ocupa las previsiones de los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).

### III

En la exposición de motivos del Proyecto de Orden se hace mención a que el "Decreto 76/2020, de 4 de agosto, despliega la potestad de las administraciones para la determinación de sistemas de identificación y firma propios, estableciendo, por un lado, principios para la creación de nuevos sistemas, basados en la simplicidad y facilidad de su uso, y por otro, el impulso de mecanismos basados en elementos biométricos o en un registro previo (...)" -

Si bien no parece que ninguno de los sistemas incluidos en el catálogo recogido en el anexo del Proyecto de Orden esté basado en "elementos biométricos", en la medida en que de acuerdo con el artículo 3.1.1.y 3.2.1 los sistemas reconocidos pueden ampliarse a cualquier otro sistema no criptográfico con registro previo, y que estos sistemas (de acuerdo con la voluntad manifestada en la exposición de motivos de impulso de mecanismos basados en elementos biométricos) podrían comportar el tratamiento de datos biométricos de los interesados, se considera oportuno efectuar consideraciones respecto al tratamiento de estos datos, que deben ser tenidas en cuenta tanto en lo referente al procedimiento de reconocimiento de estos sistemas como por las administraciones responsables del tratamiento de estos datos de los interesados.

Conviene puntualizar que los sistemas de identificación y firma pueden comportar el tratamiento de datos biométricos de los interesados en el momento de la provisión del sistema al interesado (por ejemplo si se utilizan datos biométricos para identificar al interesado para el emisión de un certificado o de un sistema de identificación) pero la utilización posterior de este mecanismo no comporta el tratamiento de estos datos biométricos. También pueden existir otros sistemas en los que el tratamiento de datos biométricos se efectúa, además de en el momento de la provisión, cada vez que el interesado utiliza el sistema de identificación y firma (por ejemplo un sistema basado en el reconocimiento de la firma en una tableta por verificación dinámica previo registro de la firma o un sistema basado en reconocimiento facial automatizado).

De acuerdo con el artículo 4.14 del RGPD los datos biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas

o conductuales de una persona física que permitan o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;”

El RGPD incluye los datos biométricos dentro de la categoría de datos que deben ser objeto de especial protección. En concreto, el artículo 9.1 del RGPD establece que:

“1. Quedan prohibidos el tratamiento de datos personales que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de forma unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.”

El considerante 51 del RGPD especifica que “el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.)”.

Tal y como ya expusimos en el dictamen [CNS 21/2020](#), que se puede consultar en la web de esta Autoridad, de la lectura conjunta de estas previsiones se desprende que el elemento clave a la hora de considerar los datos relativos a las características físicas, fisiológicas o conductuales de una persona física como datos biométricos es que estos datos se traten con medios técnicos específicos con el fin de identificar o autenticar de manera unívoca su identidad. Cuando esto sucede, estamos ante un tratamiento de categorías especiales de datos personales.

La prohibición del tratamiento de categorías especiales de datos del artículo 9.1 del RGPD, puede ser objeto de excepción cuando, si además de una base jurídica prevista en el artículo 6.1 del RGPD, se da también alguna de las excepciones establecidas en el artículo 9.2 del RGPD, entre las cuales:

“(…)

a) el interesado dio su consentimiento explícito para el tratamiento de dichas datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

(…)

g) el tratamiento es necesario por razones de un interés público esencial, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

(…)”

Puede descartarse de entrada que el tratamiento de los datos biométricos de los interesados con finalidad de identificación o de firma en la tramitación administrativa se pueda fundamentar en la excepción prevista en el artículo 9.2.g) del RGPD en la medida que no parece que el tratamiento pueda fundamentarse en la existencia de un “un interés público esencial sobre la base del derecho de la Unión o de los Estados miembros” aplicable de forma generalizada a cualquier tipo de procedimiento, y que, en cualquier caso, requería la existencia de una previsión al respecto en el derecho de la Unión Europea o en una norma con rango de ley.

A falta de otra excepción de las previstas en el artículo 9.2 RGPD, el consentimiento de los interesados podría ser una base legítima que habilitara a los responsables del tratamiento que utilice sistemas de identificación y/o firma electrónica que se basen en la utilización de datos biométricas,

siempre que este consentimiento se adecue a los requisitos establecidos por la normativa de protección de datos.

De acuerdo con el RGPD, el consentimiento del interesado es: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, (...), el tratamiento de datos personales que le conciernen;" (artículo 4.11 RGPD). En el caso de las categorías especiales de datos, además, el consentimiento debe ser explícito.

El considerante 42 del RGPD pone de manifiesto que "El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno". Y el considerante 43 añade: "Para garantizar que el consentimiento se haya dado libremente, éste no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.". En consecuencia, dado el contexto de la relación desigual que se produce entre la administración pública y los ciudadanos, el consentimiento de los interesados en el procedimiento administrativo no puede considerarse, a todos los efectos, válidamente otorgado.

Únicamente cuando se garantice que la negativa a dar el consentimiento no comporta al ciudadano algún tipo de consecuencia adversa o discriminatoria, por ejemplo si dispone de alternativas fácilmente accesibles, podría considerarse válidamente otorgado.

En consecuencia, para que se considere válido el consentimiento de los interesados para el tratamiento de sus datos biométricos, en la implementación de sistemas de identificación y firma electrónica que se basen en la utilización de estos datos, los responsables del tratamiento deben garantizar que el sistema sea voluntario para el interesado y que se le ofrecen otros mecanismos de identificación y firma para la realización de los trámites que sean igualmente accesibles (alguno de los sistemas de identificación por medios electrónicos previstos en el catálogo que no se base en la utilización de categorías especiales de datos) de tal modo que la denegación del consentimiento no le produce perjuicios o situaciones discriminatorias.

Además del principio de licitud, cualquier tratamiento de datos debe adecuarse al resto de principios establecidos por el RGPD. Entre ellos, los principios de finalidad y de minimización de datos según los cuales, los datos personales deben ser recogidos para finalidades determinadas, explícitas y legítimas (artículo 5.1.b) RGPD) y, deben ser adecuadas pertinentes y limitadas a ello necesario en relación con las finalidades para las que son tratadas (artículo 5.1.c))

Como ha puesto de manifiesto el TC en reiterada jurisprudencia, por todas la Sentencia 39/2016, de 3 de marzo, "la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta recordar que para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, puede derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (Juicio de proporcionalidad en sentido estricto) mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8]."

La aplicación del principio de minimización de datos y el juicio de proporcionalidad que comporta, deberá tener en consideración, en cada caso, el trámite concreto en el que el sistema quiera implementarse.

Por tanto los responsables del tratamiento, en este caso las administraciones sometidas al ámbito de aplicación del proyecto de orden que quieran implementar la utilización de alguno de los sistemas reconocidos en el catálogo que comporten el tratamiento de datos biométricos, deberán analizar su proporcionalidad para cada trámite concreto en el que se pretenda aplicar el sistema, para determinar su adecuación al principio de minimización de datos.

En este sentido, se valora positivamente la previsión del artículo 3 del Proyecto de Orden según la cual:

"Los sistemas de identificación y firma electrónica para acreditar la identidad de usuarios y signatarios por medios electrónicos se determinará en función del sujeto y el grado de seguridad del trámite correspondiente."

Sin embargo, la determinación de los sistemas de identificación y firma debe efectuarse en función del sujeto y del grado de seguridad que requiere el trámite correspondiente, pero además, especialmente en caso de que incorpore categorías especiales de datos, habrá que tener en cuenta la proporcionalidad de la información tratada.

Por este motivo se propone modificar la redacción de este artículo para recoger esta necesidad de tal forma que el artículo quedaría redactado como sigue:

"Los sistemas de identificación y firma electrónica para acreditar la identidad de usuarios y signatarios por medios electrónicos se determina en función del sujeto, el grado de seguridad que requiera el trámite y el resultado del juicio de proporcionalidad del sistema desde el punto de vista de la normativa de protección de datos. "

Es necesario recordar que, en función de los riesgos o la concurrencia de los requisitos previstos en el artículo 35 del RGPD que se puedan generar en función del trámite de que se trate (al respecto tener en cuenta [la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos](#) que ha publicado esta Autoridad al amparo del artículo 35.4 RGPD), puede ser necesario realizar una evaluación de impacto relativa a la protección de datos (art. 35 RGPD) y, en su caso, una consulta previa a la Autoridad (art. 36 RGPD).

Por otra parte, el responsable del tratamiento también debe tener en consideración, en lo que se refiere a la recogida, almacenamiento, tratamiento y gestión de los datos biométricos, la obligación de dar cumplimiento a lo establecido en el apartado 3 de los artículos 9 y 10 de la LPAC que prevé expresamente que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de categorías especiales de datos en los términos del RGPD deben estar situados en territorio español, y que sólo pueden transferirse a un tercero país u organización internacional cuando hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

Por todo esto se hacen las siguientes,

## **Conclusiones**

Examinado el Proyecto de Orden por el que se aprueba el Catálogo de sistemas de identificación y firma electrónica, se considera adecuado a las previsiones establecidas en la normativa sobre protección de datos personales, siempre que se tengan en cuenta las consideraciones hechas en este informe.

Barcelona, 3 de marzo de 2022

Traducción Automática