apdcat
Autoritat Catalana de Protecció de Dades

Dictamen en relació amb la consulta formulada per l'Oficina del Delegat de Protecció de Dades de Salut a l'Autoritat Catalana de Protecció de Dades sobre la signatura de documents en format electrònic

Antecedents

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta formulada en els termes següents:

> "El Departament de Salut i la xarxa d'entitats públiques que articulen la provisió de serveis de salut necessiten incorporar la digitalització als seus processos i procediments sobre la base dels principis que apliquen a l'organització sanitària, entre d'altres, de racionalització, eficàcia, simplificació i eficiència. La implantació de la signatura electrònica s'alinea amb aquests principis i constitueix una mesura útil i necessària per a la seva materialització, amb eficàcia jurídica i que incorpora les garanties i mesures de seguretat adients per a la protecció dels drets i llibertats de les persones usuàries de la sanitat pública, especialment des de la vessant del compliment de la normativa de protecció de dades.
> En aquests moments es planteja en diversos àmbits del sistema públic de salut implantar la signatura electrònica per als següents casos d'ús:
>
> - Signatura electrònica en el context de l'aplicació "La Meva Salut" (LMS).
> - Signatura electrònica presencial (SMCE) per a la signatura del consentiment informat (CI) dels usuaris pacients del sistema públic de salut.
> - Signatura electrònica presencial (SMCE) per a la signatura del consentiment informat dels usuaris donants de sang i teixits.
> - Signatura electrònica remota per a la signatura de contractes laborals."

La consulta incorpora igualment una primera valoració jurídica dels aspectes indicats, amb exposició concreta dels casos d'ús. Finalment, delimita les qüestions sobre les quals interessa el pronunciament de l'APDCAT:

> "Exposats els supòsits d'utilització de la SMCE presencial i signatura electrònica remota, s'interessa pronunciament d'aquesta Autoritat sobre els següents aspectes:
>
> a) En relació amb la signatura mitjançant LMS del document de CI (punt 2.1) es realitzen les següents qüestions:
>
> - Tenint en compte que l'usuari podria signar el document de CI, seria suficient l'autenticació mitjançant usuari/contrasenya o caldria augmentar el nivell

mitjançant altres mecanismes de autenticació com els serveis intermediats per VALID?
- Tenint en compte la resposta del punt anterior, seria suficient la signatura mitjançant mecanisme de codi d'un sol ús?

b) En relació amb el supòsit de signatura de CI de pacients mitjançant SMCE (punt 2.2) presencial amb tauleta:

En relació amb la signatura del CI de pacients, es considera conforme a la normativa de protecció de dades personals el consentiment del pacient com a base legal per al tractament de les seves dades biomètriques quan s'utilitza la SMCE presencial –mitjançant tauleta i punter digital- si se li ofereix aquesta modalitat digital com a opció alternativa a la manuscrita tradicional en format paper?

Quines garanties caldria preveure des del punt de vista de la normativa de protecció de dades addicionalment junt amb el consentiment al que es refereix l'anterior punt 3.2.1 i, en concret, la transparència de la informació, l'adopció de mesures de seguretat i la realització d'AIPD?

c) En relació amb el supòsit de signatura de CI de donants de sang i teixits mitjançant SMCE (punt 2.3) presencial amb tauleta:

Es formulen les mateixes preguntes que en l'anterior apartat però en relació amb els donants de sang i teixits.

d) En relació amb el supòsit de signatura de contractes laborals mitjançant signatura digital remota (punt 2.4):

Es pot considerar dada biomètrica la obtinguda mitjançant signatura amb el dit sobre la pantalla del dispositiu utilitzat per l'usuari?

En cas de que es consideri dada biomètrica, s'adequaria a la normativa de protecció de dades personals el consentiment de la persona interessada com a base legal per al tractament de les seves dades personals, inclòs el paràmetre biomètric, implicades en el procés d'utilització de la signatura electrònica remota per a la signatura de contracte laboral si s'ofereix aquesta modalitat electrònica com opció a la manuscrita tradicional en format de paper?

Quines garanties caldria preveure des del punt de vista de la normativa de protecció de dades addicionalment junt amb el consentiment al que es refereix l'anterior punt i, en concret, la transparència de la informació, l'adopció de mesures de seguretat i la realització d'AIPD?"

Fonaments jurídics

I

L'Autoritat Catalana de Protecció de Dades (APDCAT) és l'organisme independent que té per objecte garantir, en l'àmbit de les competències de la Generalitat, el dret a la protecció de dades personals i d'accés a la informació que hi està vinculada, d'acord amb l'article 1 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.

L'article 5 de la llei esmentada atribueix a l'APDCAT un seguit de funcions per assolir aquest objectiu. Una d'aquestes funcions és la de respondre les consultes que formulin les entitats del seu àmbit d'actuació sobre la protecció de dades personals en poder de les administracions públiques, així com col·laborar amb aquestes entitats en la difusió de les obligacions derivades de la legislació reguladora d'aquestes matèries.

En conseqüència, aquest informe s'emet d'acord amb les esmentades previsions dels articles 5 i 8 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades.

II

1. Incorporació dels mitjans electrònics en l'àmbit de les administracions públiques

La consulta que es formula sobre la viabilitat jurídica de la implementació de determinats tipus de signatura electrònica es fonamenta en la incorporació dels principis de racionalització, eficàcia, simplificació i eficiència en la provisió de serveis de salut, i indica que la digitalització de processos i procediments i, en concret, la implantació de la signatura electrònica, és una mesura útil i necessària.

Al marge de compartir aquesta afirmació, s'ha d'addicionar que el marc normatiu vigent no tan sols imposa la incorporació dels mitjans electrònics com a eina d'aplicació dels principis abans referits, sinó que també obliga a implementar de manera efectiva el dret subjectiu de les persones a relacionar-se amb l'Administració per mitjans electrònics (art. 13 Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques). En aquest sentit, la Llei 39/2015 representa un canvi substancial en la manera d'actuar de les administracions públiques.

Davant d'una Administració presencial, basada en el paper, la Llei 39/2015 culmina el procés que va iniciar la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics. Amb aquesta finalitat, impulsa significativament la tramitació electrònica, incrementa el nombre de subjectes obligats a relacionar-s'hi

electrònicament (art. 14.2), configura l'acte administratiu exclusivament en suport electrònic (art. 28 i 36) i estableix una sèrie d'eines que han de permetre complir tots i cadascun dels requeriments de la relació juridicoadministrativa, amb plena seguretat jurídica. Eines que han de permetre a les persones interessades accedir als tràmits i serveis administratius, però que també han de permetre la tramitació o producció interna dels actes administratius i, tal com hem indicat, amb plena seguretat jurídica.

Això ens porta a un dels pilars bàsics de la tramitació digital, configurat en l'establiment i/o regulació de mecanismes d'identificació i signatura, a emprar tant per les persones interessades com per les administracions públiques.

2. Establiment de sistemes de identificació i signatura electrònica

Amb caràcter previ, podem indicar que la determinació dels sistemes d'identificació i signatura a utilitzar en cadascun dels tràmits i serveis administratius correspon a cadascuna de les administracions públiques, en exercici de les seves competències autoorganitzatives, en el marc de la normativa aplicable.

Això obliga a analitzar l'establiment de mitjans de identificació i signatura des de dues perspectives diferents:

a) D'una banda, des del vessant de protecció de dades.

b) D'altra banda, des de l'anàlisi de la normativa del procediment administratiu i, en particular, els sistemes d'identificació i signatura electrònica admesos en el marc de la prestació de serveis de confiança.

2.1. Sistemes d'identificació i signatura des del vessant de protecció de dades

La utilització dels sistemes d'identificació i signatura en la tramitació administrativa comporta que els subjectes sotmesos a l'àmbit d'aplicació de la Llei 39/2015 tractin dades personals dels interessats que utilitzen aquests sistemes. D'acord amb l'article 4.1 del Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD), cal entendre com a dada personal "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 nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

L'article 5.1.*a* de l'RGPD estableix que les dades personals recollides han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat. Per tal que aquest tractament sigui lícit, cal que hi concorri alguna de les condicions previstes en

l'article 6.1 de l'RGPD i, si es tracta de categories especials de dades, cal tenir en compte també les previsions de l'article 9 de l'RGPD.

Amb caràcter general, el tractament de les dades personals que efectuen les administracions públiques en el procediment administratiu, ja sigui presencial o per mitjans electrònics, pot trobar la base jurídica a l'article 6.1.*e* de l'RGPD, segons el qual hi ha habilitació legal per tractar dades personals quan "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 com es desprèn de l'article 6.3 de l'RGPD i recull expressament l'article 8 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPGDD), el tractament de dades només pot considerar-se fonamentat en la base jurídica de l'article 6.1.*e* de l'RGPD quan així ho estableixi una norma amb rang de llei.

Per tant, la base habilitadora del tractament ha de ser una norma amb rang de llei, que en el cas que ens ocupa és la Llei 39/2015, de l'1 d'octubre, de procediment administratiu comú de les administracions públiques. Això, sense perjudici que hi pugui haver normes de caràcter reglamentari que, sense poder configurar-se com a habilitadores de nous tractaments, puguin concretar les condicions en què es duen a terme tractaments que ja estan previstos en normes amb rang de llei reguladores del procediment administratiu.

2.2. El marc normatiu general de la identificació i signatura electrònica en el procediment administratiu

Abans d'analitzar la identificació i la signatura, és important fer referència al Reglament (UE) 910/2014, de 23 de juliol de 2014, relatiu a la identificació electrònica i als serveis de confiança per les transaccions electròniques en el mercat anterior i pel qual es deroga la Directiva 1999/93/CE (d'ara endavant, ReIDAS).

L'elecció del legislador europeu d'un reglament com a instrument legislatiu, d'aplicació directa als estats membres, va ser motivada per la necessitat de reforçar la seguretat jurídica al si de la Unió; i, també, per acabar amb la dispersió normativa provocada per les transposicions de l'esmentada Directiva en els ordenaments jurídics interns mitjançant lleis nacionals, que havia provocat una important fragmentació i la impossibilitat de prestar serveis transfronterers al mercat interior, agreujada per les diferències en els sistemes de supervisió aplicats en cada Estat membre.

Així, mitjançant el ReIDAS es volen regular dues realitats en un mateix instrument normatiu d'aplicació directa als estats membres: la identificació i els serveis de confiança electrònics en sentit ampli, harmonitzant i facilitant l'ús transfronterer dels serveis en línia, públics i privats; i el comerç electrònic a la UE, per contribuir al desenvolupament del mercat únic digital.

Cal tenir present igualment la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, la qual deroga la Llei 59/2003, de signatura electrònica. Aquests prestadors de serveis de confiança són essencials per garantir la seguretat jurídica de les transaccions realitzades per mitjans electrònics. Dins de les seves funcions, s'ha de destacar la creació, verificació i validació de signatures electròniques, segells electrònics, segells de temps electrònics, serveis de lliurament electrònic certificat i certificats relatius a aquests serveis.

Finalment, el marc normatiu de caràcter bàsic el trobarem essencialment en la Llei 39/2015, sens perjudici que cada administració pública té la facultat de determinar quins són els sistemes de signatura electrònica que reconeixerà a les persones interessades, dins de l'admissibilitat general del DNI electrònic, regulada en la disposició addicional tercera de la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

No podem concloure aquesta aproximació normativa sense diferenciar igualment el vessant extern i intern de l'actuació administrativa. Mentre que la Llei 39/2015, als articles 9 a 12, regula la identificació i la signatura de les persones interessades, la regulació de la identificació i la signatura de les administracions públiques i dels empleats públics està regulada en la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, als articles 38 i següents, sota la rúbrica "Funcionament electrònic del servei públic".

2.3. La identificació i signatura en la normativa de procediment administratiu. Aspectes bàsics aplicables a la consulta

2.3.1. Rellevància de la diferenciació entre identificació i signatura

Tal com passa a la tramitació presencial, en la tramitació electrònica s'han de diferenciar la identificació i la signatura de l'interessat, aspecte que és rellevant a l'efecte de resoldre les consultes plantejades.

La consulta plantejada per l'Oficina del Delegat de Protecció de Dades de Salut es refereix essencialment a la signatura de determinats documents en l'àmbit dels serveis de salut en diferents supòsits, si bé parteix de la identificació prèvia del pacient, ja sigui a l'aplicació específica de "La meva salut" (supòsit 2.1.) o presencialment, davant del metge com a usuari del sistema de salut o donant de sang i teixits (supòsits 2.2. i 2.3). Tan sols al supòsit 2.4 (Utilització de la signatura remota per a la signatura de contractes laborals) no s'efectua aquesta diferenciació.

Per aquesta raó, hem de diferenciar ambdós conceptes, ja que quan partim d'una anàlisi separada de tots dos les conclusions jurídiques són diferents, especialment pel que fa a les dades biomètriques com a instrument de signatura i la base jurídica habilitadora per tractar-les.

2.3.2. Sistemes d'identificació i signatura a la Llei 39/2015

La diferenciació entre identificació i signatura deriva del ReIDAS. Cal recordar que, en la seva relació amb l'Administració, tal com passa presencialment, hi ha ocasions en què una persona es limita a identificar-se, mentre que hi ha d'altres casos en què la persona interessada signa una sol·licitud, escrit o comunicació.

La Llei 39/2015 dona resposta jurídica a aquesta diferenciació. Així, a l'article 9 parla dels sistemes d'identificació de les persones interessades en el procediment, mentre que a l'article 10 es refereix als sistemes de signatura admesos per les administracions públiques.

Com a regla general per tramitar, la Llei 39/2015 estableix l'exigència de la identificació, quan a l'article 11.1 indica que "per efectuar qualsevol actuació que estableix el procediment administratiu, n'hi ha prou que les persones interessades n'acreditin prèviament la identitat", i reserva la signatura per als actes més qualificats enumerats a l'article 11.2.

Però, pel que fa a les consultes formulades, ens trobem davant de casos en què cal exigir la signatura de documents (determinats contractes o el document de consentiment informat, d'ara endavant, CI), cosa que passa necessàriament per determinar els sistemes de signatura vàlids per a aquests documents.

Partint d'aquesta diferenciació i de l'anàlisi del llistat de sistemes enumerats als articles 9 i 10 de la Llei 39/2015, veiem que els requeriments tecnològics o sistemes de signatura són més alts en el cas de les actuacions que requereixen signatura, que no pas en els casos en què es requereix la identificació.

Per exemple, la lletra *c* de l'article 9.2 parla de sistemes de clau concertada (que serien els ja coneguts, usuari i contrasenya), mentre que l'article 10.1, quan parla de la signatura, indica que "les persones interessades poden signar a través de qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i inalterabilitat del document", sense incloure en l'enumeració de l'apartat 2 cap referència a un sistema de clau concertada com a mecanisme de signatura.

A més, quan es parla de signatura, s'addiciona la garantia de l'autenticitat de la voluntat o consentiment, així com la integritat i inalterabilitat del document signat.

Aquestes previsions han estat desplegades per l'article 15 del Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics:

> "Artículo 15. Sistemas de identificación, firma y verificación
>
> 1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica y resulten adecuados para

> garantizar la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos.
>
> (...)
>
> 3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:
>
> a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.
>
> b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.
>
> c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.
>
> 4. La Administración no será responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo que concurran los requisitos establecidos en el artículo 32 de la Ley 40/2015, de 1 de octubre, para la exigencia de responsabilidad patrimonial".

L'article 10.2 de la Llei 39/2015 estableix quins són els sistemes de firma admesos per les administracions públiques, que són els que es consideren vàlids a l'efecte de signatura en el procediment. A diferència de la identificació, són sistemes més exigents des del punt de vista de la seguretat atès que, com hem dit, ja no es tracta exclusivament d'identificar-se i autenticar-se, sinó d'acreditar una voluntat, que aquesta voluntat és autèntica i que el contingut és íntegre o inalterable (i que qualsevol modificació pot ser detectada).

A més, la lletra *c* de l'article 10.2 parla de "Qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i condicions que s'estableixi (...)"," amb els requeriments que s'indiquen en el mateix apartat i que evidentment ha de complir qualsevol prestador de serveis de confiança que implementi el sistema de signatura a utilitzar per les administracions públiques.

2.3.3. Els tràmits objecte de consulta requereixen signatura

Des del punt de vista gramatical, per "signatura" entenem el nom i cognoms escrits per una persona de la seva pròpia mà en un document, amb rúbrica o sense, per donar-li autenticitat o mostrar l'aprovació del contingut. Al contrari, definim "signatura digital" com la informació xifrada que identifica l'autor d'un document electrònic.

En qualsevol cas, la signatura determina una declaració de voluntat. L'autenticació en un procediment presencial es fa, generalment, mitjançant la plasmació de la firma manuscrita. Això no obstant, l'article 10.1 de la Llei 39/2015 determina que les persones interessades poden signar amb qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i la inalterabilitat del document.

Com s'ha indicat, quan se signa, a més de la certesa de la identitat de la persona, s'ha de garantir la inalterabilitat o la integritat d'allò que se signa. Per contra, quan es tracta d'identificació, en principi no cal garantir la integritat de l'acte administratiu concret de què es tracti.

En els casos objecte de consulta, la plasmació de la voluntat pel que fa al consentiment informat i la signatura de determinats contractes suposa que s'han d'aplicar els requeriments tècnics i jurídics corresponents a la signatura.

El consentiment informat està regulat per la Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica (articles 6 i 7 del capítol IV). També hi resulten aplicables les previsions de la Llei 41/2002, de 14 de novembre, bàsica reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica (articles 8, 9 i 10 del capítol IV).

Concretament, l'article 6 de la Llei 21/2000 especifica el següent en relació amb el consentiment informat:

> "1. Qualsevol intervenció en l'àmbit de la salut requereix que la persona afectada hi hagi donat el seu consentiment específic i lliure i n'hagi estat informada prèviament, d'acord amb el que estableix l'article 2.
> 2. Aquest consentiment s'ha de fer per escrit en els casos d'intervencions quirúrgiques, procediments diagnòstics invasius i, en general, quan es duen a terme procediments que comporten riscos i inconvenients notoris i previsibles, susceptibles de repercutir en la salut del pacient.
> 3. El document de consentiment ha d'ésser específic per a cada supòsit, sens perjudici que s'hi puguin adjuntar fulls i altres mitjans informatius de caràcter general. Aquest document ha de contenir informació suficient sobre el procediment de què es tracta i sobre els seus riscos.
> 4. En qualsevol moment la persona afectada pot revocar lliurement el seu consentiment."

L'article 2 de la Llei 21/2000 estableix que:

> "1. En qualsevol intervenció assistencial, els pacients tenen dret a conèixer tota la informació obtinguda sobre la pròpia salut. Això no obstant, cal respectar la voluntat d'una persona de no ésser informada.
>
> 2. La informació ha de formar part de totes les actuacions assistencials, ha d'ésser verídica, i s'ha de donar de manera comprensible i adequada a les necessitats i els requeriments del pacient, per a ajudar-lo a prendre decisions d'una manera autònoma.
>
> 3. Correspon al metge responsable del pacient garantir el compliment del dret a la informació. També han d'assumir responsabilitat en el procés d'informació els professionals assistencials que l'atenen o li apliquen una tècnica o un procediment concrets."

Finalment, com indica la consulta formulada, l'article 12.3 indica que "en el procés de translació de la informació de la història clínica, des del suport original a un altre suport, tant si és digital com d'una altra naturalesa, s'ha de garantir la inalterabilitat, l'autenticitat i la perdurabilitat de la informació assistencial, i també la confidencialitat de les dades i de la informació que contenen. Les mesures tècniques i organitzatives de seguretat que s'adoptin a aquest efecte han d'ésser recollides per protocols interns aprovats per la direcció del centre sanitari, que s'han de basar en els criteris aprovats per la comissió tècnica a què fa referència la disposició final primera."

Igualment, la Llei 41/2002, de 14 de novembre, bàsica reguladora de la autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica, indica el següent a l'article 8:

> "1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso.
>
> 2. El consentimiento será verbal por regla general.
>
> Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente.
>
> 3. El consentimiento escrito del paciente será necesario para cada una de las actuaciones especificadas en el punto anterior de este artículo, dejando a salvo la posibilidad de incorporar anejos y otros datos de carácter general, y tendrá información suficiente sobre el procedimiento de aplicación y sobre sus riesgos.
>
> 4. Todo paciente o usuario tiene derecho a ser advertido sobre la posibilidad de utilizar los procedimientos de pronóstico, diagnóstico y terapéuticos que se le

apliquen en un proyecto docente o de investigación, que en ningún caso podrá comportar riesgo adicional para su salud.

5. El paciente puede revocar libremente por escrito su consentimiento en cualquier momento."

Pel que fa als contractes de treball, l'article 8 del Reial decret legislatiu 2/2015, de 23 d'octubre, por el que s'aprova el text refós de l'Estatut dels treballadors, preveu:

"Artículo 8. Forma del contrato.

1. El contrato de trabajo se podrá celebrar por escrito o de palabra. Se presumirá existente entre todo el que presta un servicio por cuenta y dentro del ámbito de organización y dirección de otro y el que lo recibe a cambio de una retribución a aquel.

2. Deberán constar por escrito los contratos de trabajo cuando así lo exija una disposición legal y, en todo caso, los de prácticas y para la formación y el aprendizaje, los contratos a tiempo parcial, fijos-discontinuos y de relevo y los contratos para la realización de una obra o servicio determinado; también constarán por escrito los contratos por tiempo determinado cuya duración sea superior a cuatro semanas.

Deberán constar igualmente por escrito los contratos de trabajo de los pescadores, de los trabajadores que trabajen a distancia y de los trabajadores contratados en España al servicio de empresas españolas en el extranjero.

De no observarse la exigencia de forma escrita, el contrato de trabajo se presumirá celebrado por tiempo indefinido y a jornada completa, salvo prueba en contrario que acredite su naturaleza temporal o el carácter a tiempo parcial de los servicios.

Cualquiera de las partes podrá exigir que el contrato se formalice por escrito, incluso durante el transcurso de la relación laboral."

Si bé en l'àmbit laboral és possible la contractació verbal, a l'administració pública la forma escrita és la manera ordinària de signar els contractes, i tan sols en determinats supòsits no s'aplicaria aquesta previsió (com ara la contractació verbal, en casos d'emergència). En definitiva, d'acord amb la doctrina de la vinculació positiva, la signatura escrita dels contractes de treball és la forma d'actuar imposada a les administracions públiques.

Igualment cal indicar que, en el dret d'obligacions, l'acceptació i la forma com aquesta acceptació es manifesta són determinants per a la validesa de la manifestació de la voluntat en un document privat; per això, té especial rellevància quan aquesta manifestació s'acredita amb una signatura electrònica. L'article 1262 del Codi civil espanyol estableix el següent:

> "El consentiment es manifesta pel concurs de l'oferta i de l'acceptació sobre la cosa i la causa que han de constituir el contracte
>
> Trobant-se en llocs diferents el que va fer l'oferta i el que la va acceptar, hi ha consentiment des que l'oferent coneix l'acceptació o des que, havent-la-hi remès l'acceptant, no pugui ignorar-la sense faltar a la bona fe. El contracte, en tal cas, es presumeix subscrit al lloc en què es va fer l'oferta
>
> Als contractes celebrats mitjançant dispositius automàtics hi ha consentiment des que es manifesta l'acceptació."

En resum, tant el CI com els contractes laborals objecte de consulta són documents que han de ser necessàriament signats.

2.3.4. La determinació dels tipus de signatura és competència de cada administració pública

Abans hem indicat que correspon a cada administració pública determinar el tipus de signatura a emprar en cada tràmit i servei, entre els sistemes legalment admesos.

De la mateixa manera, cal aclarir que no correspon a aquesta Autoritat definir els mitjans a través dels quals s'efectuï la identificació i/o signatura dels ciutadans per mitjans electrònics en la tramitació administrativa, ja que això correspon a les administracions públiques, si escau, amb les corresponents autoritzacions establertes per la normativa de procediment administratiu. Així mateix, tampoc li correspon determinar si un sistema d'identificació i/o signatura "pot garantir fefaentment la identitat de la persona sol·licitant."

Ara bé, sí que correspon a aquesta Autoritat vetllar perquè aquests sistemes d'identificació i/o signatura s'ajustin al que preveu la normativa de protecció de dades personals i, també, determinar els riscos que la seva utilització pot comportar en el dret fonamental a la protecció de dades personals

Actualment, hi ha molts sistemes d'identificació i de signatura que poden ser utilitzats pels ciutadans i per les empreses (persones globalment considerades), sistemes que són proveïts pels prestadors de serveis de confiança (abans del ReIDAS, prestadors de serveis de certificació).

Al mateix temps, cal recordar que la definició de la política de signatura electrònica és competència de cada administració pública, sens perjudici del compliment dels requeriments de interoperabilitat. Per aquesta raó, l'article 18 del Reial decret 4/2010, pel qual es regula l'Esquema Nacional de Interoperabilitat, disposa el següent:

> "1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad

para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas. […]

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales. Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital."

2.3.5. Determinació del tipus de signatura en funció del nivell de seguretat i tipus de signatura

2.3.5.1. Nivells de seguretat pel que fa al risc de suplantació de la persona

Quan parlem de sistemes d'identificació i de signatura, hem de tenir present que poden ser utilitzats per a diferents tràmits que efectuïn les persones interessades amb l'Administració, i la tipologia de sistema d'identificació i/o signatura que s'admeti es determina d'acord amb el grau de seguretat en la identificació que es vulgui assolir. Així, per raó del grau de seguretat, els sistemes d'identificació es poden classificar en nivells de seguretat baix, substancial o alt.

El ReIDAS els regula a l'article 8 i diferencia:

- Nivell de seguretat baix, amb l'objectiu de reduir el risc d'ús indegut o alteració de la identitat presentada.

- Nivell de seguretat substancial, amb l'objectiu de reduir substancialment el risc d'ús indegut o alteració de la identitat.

- Nivell de seguretat alt, amb l'objectiu d'evitar l'ús indegut o l'alteració de la identitat.

Tot i que l'àmbit d'aplicació del ReIDAS es limita a la identificació electrònica en l'accés transfronterer als serveis públics, aquests criteris de seguretat són igualment considerats a l'hora de determinar els sistemes de signatura a admetre.

Per aquesta raó, els objectius de reduir, reduir substancialment o evitar el risc de suplantació d'una persona interessada en una relació juridicoadministrativa són els que porten cada Administració a determinar quins tipus de signatura es pot exigir en un determinat procediment o tràmit, d'acord amb el principi de proporcionalitat o l'anàlisi de riscos.

2.3.5.2. Tipus de signatura legalment admeses

Aquesta determinació no és aleatòria, sinó que es relaciona amb la tipologia de signatura legalment admesa, que es pot diferenciar igualment en tres grans tipus: signatura electrònica reconeguda o qualificada, signatura avançada i signatura ordinària.

Cadascun d'aquests tipus de signatura incorpora uns requeriments tecnològics que permeten atribuir més o menys valor jurídic a l'actuació administrativa concreta. També ens permet determinar que tan sols la signatura electrònica reconeguda o qualificada s'equipara a la signatura manuscrita (art. 25.2 ReIDAS).

La signatura electrònica són “los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.” Aquesta seria la que anteriorment s'anomenava "signatura electrònica ordinària", que és qualsevol altra signatura que no sigui avançada o qualificada.

D’altra banda, la signatura electrònica avançada es defineix com “la firma electrónica que cumple los requisitos contemplados en el artículo 26”, sobre la qual es disposa el següent: “Una firma electrónica avanzada cumplirá los requisitos siguientes: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.”

Finalment, la signatura electrònica qualificada (en l’ordenament jurídic espanyol s’utilitza com a concepte equiparat al de signatura electrònica reconeguda) és “una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.”

Si tornem a l'enumeració de sistemes de signatura electrònica que fa l’article 10.2 de la Llei 39/2015, podem diferenciar:

"a) Sistemes de signatura electrònica reconeguda o qualificada i avançada basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos en la llista de confiança de prestadors de serveis de certificació. A aquest efecte, entre els esmentats certificats electrònics reconeguts o qualificats s'hi comprenen els de persona jurídica i els d'entitat sense personalitat jurídica.

b) Sistemes de segell electrònic reconegut o qualificat i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats de segell electrònic inclosos en la llista de confiança de prestadors de serveis de certificació.

c) Qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i les condicions que s'estableixi (...)"

Per completar la matèria, cal afegir l'anàlisi del concepte del segell electrònic, el qual es defineix com a "datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos."

Podem veure que el segell té per objecte garantir la integritat d'allò que se signa. Això suposa afegir un altre sistema per signar documents, que actuaria com a complementari d'una identificació prèvia de la persona interessada (tal com habilita l'article 10.4 de la Llei 39/2015).

La determinació del sistema es fa d'acord amb especificacions tècniques mínimes, normes i procediments que permetin determinar la fiabilitat o la qualitat de determinats elements, com són: la inscripció o el registre, la gestió dels mitjans d'identificació, el mecanisme d'autenticació utilitzat per confirmar la identitat i la gestió i l'organització del sistema (com ara les característiques i el disseny del mitjà, o l'expedició, el lliurament i l'activació d'aquest mitjà). A títol d'exemple, pot ser un factor d'autenticació basat en la possessió d'aquest, un factor d'autenticació basat en el coneixement, en què el subjecte ha de demostrar que el coneix, o un factor d'autenticació inherent, basat en un atribut físic que el subjecte està obligat a demostrar que posseeix.

Correspon a cada administració decidir quins sistemes d'identificació i de signatura requerirà a les persones interessades que s'hi relacionin, i aquesta decisió l'ha de prendre fent una anàlisi de proporcionalitat o de riscos, d'acord amb els paràmetres indicats més amunt. La tendència actual en el funcionament de les administracions públiques és requerir sistemes d'identificació o de signatura almenys substancials per a la majoria dels tràmits i, al mateix temps, permetre que les actuacions menys rellevants des del vessant jurídic es puguin fer amb sistemes considerats de nivell de seguretat baix.

Però aquest marc legal no és complet sense fer referència a les disposicions del Reglament d'execució (UE) 2015/1502 de la Comissió de 8 de setembre de 2015 sobre la fixació d'especificacions i de procediments tècnics mínims per als nivells de seguretat dels mitjans d'identificació electrònica (aplicable en tots els estats membres, atesa la seva naturalesa de reglament comunitari), que a l'annex en regula les especificacions i els requeriments; segons si es compleixen o no, un sistema d'identificació concret es pot qualificar de nivell baix, substancial o alt.

A l'esmentat reglament s'estableixen els requisits que inclouen els tres possibles factors d'autenticació necessaris per a cada nivell:

1. Factor d'autenticació basat en la possessió, en el qual el subjecte està obligat a demostrar possessió del mateix.

2. Factor d'autenticació basat en el coneixement, en el qual el subjecte està obligat a demostrar coneixement del mateix.

3. Factor d'autenticació inherent, que es basa en un atribut físic d'una persona física que el subjecte està obligat a demostrar la seva possessió.

Així, per exemple, en aplicació dels criteris de determinació a valorar, es pot configurar com a alt el sistema que, a més de complir els requeriments del nivell substancial, inclou proves d'identificació fotogràfiques o biomètriques.

En resum, com ja hem dit, amb aquests requeriments es busca tenir la certesa, amb un grau prou alt, que la persona que està actuant davant de l'Administració pública és qui diu que és.

Finalment, cal tenir present que la determinació del sistema d'identificació i/o signatura a emprar ha de tenir en compte igualment les condicions de seguretat establertes en l'Esquema Nacional de Seguretat (ENS), regulat pel Reial decret 311/2022, de 3 de maig. L'ENS permet definir el nivell de seguretat de l'autenticació per a les aplicacions o els sistemes per a la tramitació electrònica sobre la base de la naturalesa de les dades que es tractin i la classificació de seguretat, d'acord amb les recomanacions del mateix ENS.

2.3.6. Disposicions específiques en l'àmbit de l'Administració de la Generalitat

En el cas de l'Administració de la Generalitat, cal ajustar-se a les previsions del Decret 76/2020, de 4 d'agost, d'administració digital, que a l'article 58 fa referència al Catàleg i Guia dels sistemes d'identificació i signatura electrònica, en els termes següents:

> "1. Correspon a la persona titular del departament competent en matèria de polítiques digitals aprovar, mitjançant una ordre, el Catàleg de sistemes d'identificació i signatura electrònica admesos per efectuar els tràmits i procediments de les persones interessades amb l'Administració de la

> Generalitat. El Catàleg s'actualitza amb l'admissió de nous sistemes d'identificació i signatura electrònica i es publica a la Seu electrònica de l'Administració de la Generalitat.
>
> 2. Correspon a la persona titular del departament competent en matèria d'administració digital aprovar, mitjançant una ordre, una guia d'ús dels sistemes d'identificació i signatura electrònica que reculli els aspectes tècnics i organitzatius necessaris per implantar els sistemes d'identificació i signatura electrònica per a cada tràmit o servei digital a l'Administració de la Generalitat. Per a l'elaboració de la Guia i les actualitzacions posteriors, es requereix l'informe previ de l'òrgan encarregat de la ciberseguretat de la Generalitat de Catalunya i dels ens competents en la provisió dels sistemes d'identificació i signatura electrònica de l'Administració de la Generalitat."

En desenvolupament d'aquestes previsions, s'han aprovat respectivament l'Ordre VPD/93/2022, de 28 d'abril, per la qual s'aprova el Catàleg de sistemes d'identificació i signatura electrònica, i l'Ordre PRE/158/2022, de 30 de juny, per la qual s'aprova la Guia d'ús dels sistemes d'identificació i signatura electrònica en l'àmbit de l'Administració de la Generalitat.

Respecte de la primera (Catàleg de sistemes d'identificació i signatura electrònica), al web de l'APDCAT es pot consultar el dictamen PD 1/2022, emès per aquesta Autoritat en relació amb la proposta d'Ordre.

L'article 3 de l'Ordre VPD/93/2022 conté la següent redacció:

> "Sistemes d'identificació i signatura de les persones que es relacionen amb l'Administració.
> Els sistemes d'identificació i signatura electrònica per acreditar la identitat d'usuaris i signataris per mitjans electrònics es determinen en funció del subjecte, el grau de seguretat que requereixi el tràmit i el resultat del judici de proporcionalitat del sistema des del punt de vista de la normativa de protecció de dades."

Pel que fa a la Guia d'ús dels sistemes d'identificació i signatura electrònica, estableix els criteris que han de seguir les entitats incloses en el seu àmbit d'aplicació, a l'hora d'implementar els sistemes d'identificació i signatura.

Aquests són els paràmetres que s'han de valorar a l'efecte de determinar el sistema de signatura electrònica a emprar en un determinat servei; això suposa, d'una banda, la utilització d'algun dels sistemes de signatura legalment admesos en el marc de l'article 10.2 de la Llei 39/2015, i, d'altra banda, que el sistema de signatura escollit compleixi igualment la normativa de protecció de dades.

2.3.7. En particular: la signatura electrònica digital o biomètrica

A la consulta es planteja, en particular, la possibilitat d'utilitzar la signatura digital electrònica com a signatura biomètrica, cosa que ens obliga a definir aquest concepte.

La biometria és l'estudi per al reconeixement inequívoc de persones basat en un o més trets conductuals o físics intrínsecs. Així, la signatura electrònica manuscrita o biomètrica o dinàmica és el conjunt de dades biomètriques associades a la grafia d'un signant, capturades amb una tauleta digitalitzadora o mòbil, que poden assegurar el vincle entre el document i la identitat del signant si, a més, es dota de determinades mesures de seguretat que la configurin com una evidència electrònica de la firma que permeti que en el futur se'n verifiqui la certesa. La signatura representa la vinculació del signant amb el document firmat.

El Grup de treball de protecció de dades de l'article 29 (Dictamen 3/2012 sobre l'evolució de les tecnologies biomètriques, adoptat el 27 d'abril de 2012 i que en substitueix un d'anterior de l'any 2003), sobre aquesta qüestió va assenyalar que:

> "La firma biométrica puede considerarse un ejemplo de nuevo uso de las tecnologías biométricas tradicionales. La firma biométrica es una técnica biométrica basada en el comportamiento, que mide la conducta de una persona según lo expresado por la dinámica de su firma manuscrita. Mientras que el reconocimiento de firma tradicional se basa en el análisis de características fijas o geométricas de la imagen visual de la firma (aspecto de la firma), la firma biométrica, en cambio, hace referencia al análisis de las características dinámicas de la firma (cómo se hizo la firma) y esto hace que estas técnicas se denominen «firma dinámica».
>
> Las características dinámicas típicas medidas por un sistema de firma biométrica (como un tablero digitalizador) son la presión, el ángulo de escritura, la velocidad y aceleración del bolígrafo, la formación de las letras, la dirección de los rasgos de la firma y otras características dinámicas únicas. Estas características varían en uso e importancia entre los distintos proveedores y normalmente se recogen utilizando dispositivos de contacto sensibles".

Característiques dinàmiques com la pressió, l'angle d'escriptura, la velocitat i acceleració del bolígraf, la formació de les lletres i la direcció dels trets de la firma són dades biomètriques. Així, l'RGPD indica que les dades biomètriques són les "dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permetin o confirmin la identificació única de l'esmentada persona, com imatges facials o dades dactiloscòpiques." Les característiques dinàmiques que mesuren aquests sistemes de firma biomètrica varien en ús i importància entre els diferents proveïdors i, normalment, es recullen utilitzant dispositius de contacte sensibles.

En qualsevol cas, la signatura electrònica digital no deixa de ser una signatura manuscrita en què només canvia el suport en el qual es produeix i que, per tant, els

mitjans de prova han de ser similars a la firma tradicional (pericial tècnica i cal·ligràfica).

A títol d'exemple envers aquesta equiparació, en l'àmbit de la pericial cal·ligràfica sobre signatures manuscrites, sense perjudici que la jurisprudència del Tribunal Suprem reconeix una força probatòria superior a la feta sobre documents originals (ja que un dels aspectes que valora el pèrit, a l'hora de emetre el seu dictamen, és la pressió que es fa a l'hora de signar), no exclou la força probatòria de la pericial cal·ligràfica sobre fotocòpia.

Això, sense perjudici que la signatura electrònica digital pugui utilitzar-se com a mecanisme d'identificació i autenticació, mitjançant el tractament tecnològic de la signatura emesa i la seva verificació amb una plantilla prèviament registrada (cosa que no es produeix en els supòsits objecte de consulta).

D'acord amb l'exposat, sense perjudici de la força probatòria que se li pugui atribuir, una signatura biomètrica tan sols es podria equiparar a la signatura manuscrita quan així es prevegi normativament, com a conseqüència de l'anàlisi o compliment de determinats requeriments tecnològics; i, a hores d'ara, no es considera signatura electrònica reconeguda o qualificada.

No entrarem a valorar quins han de ser els condicionants jurídics i tècnics que ha de tenir una signatura electrònica digital o biomètrica, per complir els requeriments de captura d'elements biomètrics, vinculació d'aquests elements amb el document, integritat i autenticitat del document, confidencialitat de les dades i perdurabilitat en el temps (per citar els més rellevants). Tampoc ens correspon determinar o qualificar el sistema de signatura que implicaria, en termes de seguretat, ja que això, entre d'altres aspectes, dependrà de condicionants tecnològics en el cas en concret i del seu encaix en alguns dels sistemes de signatura regulats a l'article 10.2 de la Llei 39/2015.

Simplement recordar que, per dotar de les màximes garanties legals una signatura electrònica digital, s'ha de produir la intervenció d'un prestador de serveis de confiança de signatura electrònica que, de la mateixa manera que proveeix el signant d'un sistema de signatura, ha de complir els requeriments legals i tècnics per donar a la signatura la seguretat jurídica necessària -com ara la norma ISO/IEC 19794- i, en cas de discrepància, garantir-ne l'emissió (així com garantir el compliment de condicions de perdurabilitat en el temps).

La intervenció del prestador de confiança és assegurar que el document firmat amb la signatura electrònica compleix les propietats d'autenticitat i integritat del document i, per tant, constitueix un mitjà de prova en judici (i que sigui el més robust possible); és a dir, que s'atorgui a l'esmentat document ple valor probatori i, per descomptat, que en última instància se'n pugui determinar l'autoria pericialment.

El ReIDAS no regula la firma biomètrica, però sí que preveu la biometria com a factor d'autenticació electrònica. Així, ja hem indicat que l'article 8 diferencia els nivells baix, substancial i alt que cal especificar en els sistemes d'identificació electrònica dels Estats membres. I quan el Reglament d'execució (UE) 2015/1502 fa referència als tres possibles factors d'autenticació, necessaris per a cada nivell, la signatura biomètrica quedaria inclosa dins del tercer factor (factor d'autenticació inherent, que es basa en un atribut físic d'una persona física que el subjecte està obligat a demostrar que posseeix).

També ha d'indicar-se que, en la regulació europea de les signatures electròniques en les quals el signant utilitza certificats electrònics, en concret en l'article 24.1.*b* del ReIDAS, es preveu també la biometria entre els requisits per verificar la identitat "a distància" per expedir certificats qualificats. I es preveu, a més, que, en les normes que estableixi la Comissió Europea per a la creació de signatures electròniques avançades i qualificades "a distància", s'exigeixi un mitjà d'autenticació electrònic de l'usuari amb nivell de seguretat substancial o alt; això requerirà, almenys, que hi concorrin dos factors d'autenticació de diferents categories (de les tres possibles, basat en la possessió, basat en el coneixement i inherent).

2.4. Validesa legal de la signatura electrònica

A l'efecte d'avaluar jurídicament la signatura electrònica digital, a l'article 3 del ReIDAS es defineixen la signatura electrònica, la signatura electrònica avançada i la qualificada (o reconeguda).

Pel que fa als efectes jurídics, l'article 25 del ReIDAS indica:

> "Art. 25 Efectos jurídicos de las firmas electrónicas
>
> 1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.
>
> 2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.
>
> 3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será recono cida como una firma electrónica cualificada en todos los demás Estados miembros."

L'article 26 indica els requisits per a les signatures electròniques avançades, mentre que l'article 46, titulat "Efectes jurídics dels documents electrònics", article únic del capítol IV sobre els documents electrònics, estableix el següent:

> "Art. 46. Efectos jurídicos de los documentos electrónicos

> No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en formato electrónico."

D'acord amb aquestes previsions, i tal com s'exposa a l'apartat 3 subsegüent, tots els documents electrònics, sigui quina sigui la signatura que incorporin, fan o poden fer prova en cas de discrepància (sense perjudici que, òbviament, la força probatòria no serà la mateixa, sinó que dependrà del sistema de signatura emprat).

A l'ordenament jurídic estatal, la disposició final segona de la Llei 40/2015 modificava la Llei 59/2003 incloent un nou apartat 11 a l'article 3:

> "11. Tots els sistemes d'identificació i signatura electrònica establerts en la Llei de procediment administratiu comú de les administracions públiques i en la Llei de règim jurídic del sector públic, tenen plens efectes jurídics."

Com ja hem indicat, la Llei 59/2003 ha estat derogada per la Llei 6/2020, però la disposició addicional segona manté la mateixa determinació ("Efectos jurídicos de los sistemas utilizados en las Administraciones públicas"): "Tots els sistemes d'identificació, signatura i segell electrònic establerts en la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i en la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, tenen plens efectes jurídics."

D'acord amb això, correspon a cadascuna de les administracions públiques determinar quins tràmits o documents, per raó de la rellevància en el procediment, han de desplegar força probatòria indiscutible i, per això, han d'incorporar el sistema de signatura electrònica reconeguda o qualificada. O bé, per contra, poden admetre altres sistemes de signatura, que incorporin igualment la integritat o garantia de no alteració del document firmat.

En resum, la implementació electrònica del procediment requereix que s'adoptin decisions relatives al sistema de signatura electrònica a exigir als interessats, i aquestes decisions tenen un cert grau de discrecionalitat, en la mesura que poden haver-hi diversos sistemes. Això sens perjudici que, en tots els casos, ha de quedar garantida la integritat d'allò que s'hagi firmat i, igualment, s'han de complir els requeriments d'interoperabilitat i de seguretat. Finalment, cal atenir-se a l'eficàcia probatòria que es deriva de cada sistema de signatura utilitzat, i que s'ha de tenir en compte a l'hora de decidir la manera de plasmar electrònicament el tràmit o acte que, fins no fa gaire, es verificava presencialment i mitjançant firma manuscrita, com a regla general.

En resum, la signatura electrònica digital produeix efectes jurídics, si bé, en funció del tipus de signatura electrònica a la qual s'equipari i les condicions concretes del seu ús, caldrà ajustar-se a la prova corresponent.

3. La prova de la signatura electrònica

La força probatòria de la signatura electrònica està regulada a la Llei d'enjudiciament civil (LEC). Això no obstant, les previsions legals aplicables a l'àmbit processal són plenament traslladables a l'àmbit del procediment administratiu, ja que en última instància, en cas de manca de conformitat en el sí del procediment administratiu, sempre hi haurà la possibilitat del control judicial posterior; i, en aquests casos, les previsions de la LEC en matèria de prova són aplicables supletòriament en l'àmbit del procediment contenciós administratiu.

L'article 326 de la LEC disposa:

> "1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.
> 2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.
> Si del cotejo o de otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.
> 3. Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.
> 4. Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados.
> Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación. Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros."

S'ha d'indicar que l'apartat 4 ha estat afegit per la Llei 6/2020 i que l'apartat 3 ha estat objecte d'una nova redacció.

Aquesta previsió legal complementa i és coherent amb l'article 25 del ReIDAS. En resum, en cas de discrepància, cal atenir-se a les circumstàncies del cas en concret i als elements fàctics i tecnològics de què es disposi.

D'acord amb aquest marc, si ens trobem amb una signatura electrònica reconeguda o qualificada, la prova és molt més simple (mitjançant la intervenció del prestador de serveis de confiança corresponent). Però, en la resta de tipus de signatura, l'article 326.2 acaba indicant que "el tribunal lo valorará conforme a las reglas de la sana crítica."

Això suposa la lliure apreciació de la prova per part del jutge i, tractant-se d'una signatura electrònica manuscrita, la intervenció del prestador de serveis de confiança, les condicions d'emissió de la signatura i l'entorn en què es produeixi i es conservi seran rellevants a l'efecte de valoració de la prova, que no deixarà de ser una prova per indicis. Aspectes tots aquests traslladables a la prova en el procediment administratiu, tal com disposa l'article 77 de la Llei 39/2015:

> "Article 77. Mitjans i període de prova.
>
> 1. Els fets rellevants per a la decisió d'un procediment es poden acreditar per qualsevol mitjà de prova admissible en dret, la valoració de la qual s'ha de fer d'acord amb els criteris que estableix la Llei 1/2000, de 7 de gener, d'enjudiciament civil".

4. La utilització de sistemes de signatura biomètrics des del punt de vista de la protecció de dades

4.1. El tractament de dades biomètriques com a categories especials de dades

Tal com es va exposar al dictamen PD 1/2022, els sistemes d'identificació i signatura poden comportar el tractament de dades biomètriques dels interessats en el moment de la provisió del sistema a l'interessat (per exemple, si s'utilitzen dades biomètriques per identificar l'interessat per emetre un certificat o un sistema d'identificació); això no obstant, la utilització posterior d'aquest mecanisme no comporta el tractament d'aquestes dades biomètriques. També poden haver-hi altres sistemes en què les dades biomètriques, a més del moment de la provisió, es tracten cada vegada que l'interessat utilitza el sistema d'identificació i signatura (per exemple, un sistema basat en el reconeixement de la signatura en una tauleta per verificació dinàmica amb registre previ de la signatura, o un sistema basat en reconeixement facial automatitzat).

Cal recordar que a la consulta plantejada no s'articula la signatura biomètrica com a mecanisme d'identificació, sinó exclusivament de signatura.

D'acord amb l'article 4.14 de l'RGPD, les dades biomètriques són "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 confirmen

la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."

L'RGPD inclou les dades biomètriques dins la categoria de dades que han de ser objecte d'especial protecció. En concret, l'article 9.1 de l'RGPD estableix que: "1. Quedan prohibidos el tratamiento de datos personales que revelen 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 manera 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 considerant 51 de l'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 com ja vam exposar en el dictamen CNS 21/2020, que es pot consultar al web d'aquesta Autoritat, de la lectura conjunta d'aquestes previsions es desprèn que l'element clau a l'hora de considerar les dades relatives a les característiques físiques, fisiològiques o conductuals d'una persona física com a dades biomètriques és que aquestes dades es tractin amb mitjans tècnics específics amb la finalitat d'identificar o d'autenticar, de manera unívoca, la seva identitat. Quan això succeeix, ens trobem davant un tractament de categories especials de dades personals.

La prohibició del tractament de categories especials de dades de l'article 9.1 de l'RGPD pot ser objecte d'excepció quan, si a més d'una base jurídica prevista a l'article 6.1 de l'RGPD, es dona també alguna de les excepcions establertes a l'article 9.2 de l'RGPD, entre les quals: "(...) a) el interesado dio su consentimiento explícito para el tratamiento de dichos 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, sobre la base del 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; (...)."

Es pot descartar d'entrada que el tractament de les dades biomètriques dels interessats amb finalitat d'identificació o de signatura en la tramitació administrativa es pugui fonamentar en l'excepció prevista a l'article 9.2.*g* de l'RGPD, en la mesura que no sembla que el tractament es pugui fonamentar en l'existència d'un "interès públic essencial sobre la base del dret de la Unió o dels Estats membres" aplicable de manera generalitzada a qualsevol tipus de procediment. I, en qualsevol cas, requeria que estigués previst en el dret de la Unió Europea o en una norma amb rang de llei.

A manca d'altra excepció de les previstes a l'article 9.2 de l'RGPD, el consentiment dels interessats podria ser una base legítima que habilités els responsables del tractament que empri sistemes d'identificació i/o signatura electrònica que es basin en la utilització de dades biomètriques, sempre que aquest consentiment s'adeqüi als requisits establerts per la normativa de protecció de dades.

D'acord amb l'RGPD, el consentiment de l'interessat és: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, (...), el tratamiento de datos personales que le conciernen"(art. 4.11 RGPD).

Alhora, cal tenir en compte que, en la mesura que el tractament pretès comporta tractar categories especials de dades, el consentiment ha de ser explícit (art. 9.2.*a* RGPD). En relació amb aquest requisit, cal tenir en compte les Directrius 5/2020 sobre el consentiment, en el sentit del Reglament (UE) 2016/679 del Comitè Europeu de Protecció de Dades (CEPD):

> "93. El término explícito se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento. Una manera evidente de garantizar que el consentimiento es explícito sería confirmar de manera expresa dicho consentimiento en una declaración escrita. Cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, con el fin de eliminar cualquier posible duda o falta de prueba en el futuro. […]".
> Pel que fa al requisit que el consentiment sigui lliure, el considerant 43 de l'RGPD exposa el següent:
> "[…] el consentimiento […] no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular."
>
> "13. El término «libre» implica elección y control reales por parte de los interesados. […] si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido. […] La noción de desequilibrio entre el responsable del tratamiento y el interesado también se tiene en cuenta en el RGPD.
> 14. A la hora de valorar si el consentimiento se ha dado libremente, deben considerarse también las situaciones concretas en las que el consentimiento se supedita a la ejecución de contratos o a la prestación de un servicio […]. En términos generales, el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distintas) que impida que este ejerza su libre voluntad.
> […]

> 16. El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable.
> El CEPD considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.
> 17. Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD."
> […]

Atès el context de la relació desigual que es produeix entre l'administració pública i els ciutadans, amb caràcter general el consentiment dels interessats en el procediment administratiu no es pot considerar vàlidament atorgat.

Sobre la base del que s'ha exposat, i altres qüestions que també queden recollides a les Directrius 5/2020 del CEPD, a les quals ens remetem, tan sols podria considerar-se que hi ha consentiment lliure si l'interessat disposa d'una alternativa, i és aquest qui escull i presta el seu consentiment al tractament de les seves dades biomètriques per a la signatura del CI.

Únicament quan es garanteixi que la negativa a donar el consentiment no comporta al ciutadà algun tipus de conseqüència adversa o discriminatòria, per exemple si disposa d'alternatives fàcilment accessibles, es podria considerar vàlidament atorgat.

En conseqüència, per tal que el consentiment dels interessats es consideri vàlid per tractar les seves dades biomètriques, en la implementació de sistemes d'identificació i signatura electrònica que es basin en la utilització d'aquestes dades els responsables del tractament han de garantir que el sistema sigui voluntari per a l'interessat, i que se li ofereixen altres mecanismes d'identificació i signatura per fer els tràmits que siguin igualment accessibles (algun altre dels sistemes d'identificació per mitjans electrònics legalment previstos), de manera que la denegació del consentiment no li produeix perjudicis o situacions discriminatòries.

En el cas objecte de consulta, no tan sols l'alternativa presencial existeix sinó que, com veurem, la identificació i autenticació de la persona és presencial, mentre que la utilització de la signatura electrònica digital ho és exclusivament en la signatura del document de CI.

A aquest efecte, cal tenir en consideració que, d'acord amb el principi de responsabilitat proactiva (art. 5.2 RGPD), el responsable del tractament ha de ser capaç de demostrar que el consentiment és vàlid i que el tractament és lícit.

A més del principi de licitud, qualsevol tractament de dades s'ha d'adequar a la resta de principis que estableix l'RGPD. Entre aquests, els principis de finalitat i de minimització de dades, segons els quals les dades personals s'han de recollir per a finalitats determinades, explícites i legítimes (art. 5.1.*b* RGPD), i han de ser adequades pertinents i limitades a allò necessari en relació amb les finalitats per a les quals són tractades (art. 5.1.*c*).

Com ha posat de manifest el TC en reiterada jurisprudència, per totes la sentència 39/2016, de 3 de març, "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 con 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, por 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) [SSTC 66/1995, de 8 de 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]." (FD.5)

Quan parlem de signatura biomètrica, semblaria que utilitzar-la per signar el CI superaria el judici de proporcionalitat. No tan sols perquè resulta idònia, sinó també perquè resulta necessària, ja que la signatura del CI no tan sols ve imposada per l'actuació mèdica corresponent, sinó especialment perquè no hi hauria una mesura més moderada.

Cal tenir present que estem parlant de sistemes de signatura legalment admesos en el marc de l'article 10.2 de la Llei 39/2015. En aquest sentit, correspon a l'Administració dotar de sistemes de signatura electrònica els interessats, per complir el dret de les persones que es relacionen amb l'Administració recollit a l'article 13.*g* de la mateixa llei. Per aquesta raó, tal com exposarem posteriorment, la signatura biomètrica del CI, sense practicar cap actuació d'identificació simultània de la persona que signa, semblaria neutra per a l'interessat pel que fa al tractament de la seva signatura.

Finalment, la ponderació en sentit estricte també resultaria adequada ja que, a efectes de prova i en cas de discrepància, la signatura biomètrica tindria una força probatòria superior a altres sistemes, cosa que és tan beneficiós per a l'interessat com per a l'Administració.

L'aplicació del principi de minimització de dades i el judici de proporcionalitat que comporta ha de tenir en consideració, en cada cas, el tràmit concret en el qual es vulgui implementar el sistema. Per tant, els responsables del tractament que vulguin

utilitzar la signatura biomètrica per la signatura del CI hauran d'analitzar-ne la proporcionalitat, per determinar-ne l'adequació al principi de minimització de dades.

Tal com s'ha indicat amb anterioritat, la determinació dels sistemes d'identificació i signatura s'ha d'efectuar en funció del subjecte i del grau de seguretat que requereix el tràmit corresponent. Però, a més, especialment en el cas que incorpori categories especials de dades, caldrà tenir en compte la proporcionalitat de la informació tractada.

Per altra banda, pel que fa a la recollida, emmagatzemament, tractament i gestió de les dades biomètriques, el responsable del tractament també ha de tenir en consideració l'obligació de complir el que estableix l'apartat 3 dels articles 9 i 10 de la Llei 39/2015, que preveu expressament que els recursos tècnics necessaris per recollir, emmagatzemar, tractar i gestionar categories especials de dades en els termes de l'RGPD han d'estar situats en territori espanyol; i que només es poden transferir a un tercer país o organització internacional quan hagin estat objecte d'una decisió d'adequació de la Comissió Europea, o quan ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya.

El considerant 52 de l'RPGD indica:

> "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. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial."

Aquests considerants guarden relació amb el principi de licitud (art. 5.1.*a* RGPD), a partir del qual qualsevol tractament de dades personals ha de ser lícit i requereix que hi concorri alguna de les bases jurídiques establertes a l'article 6.1 de l'RGPD. I, en la mesura que es tractin categories especials de dades personals, com en el cas que ens ocupa, hi ha de concórrer també alguna de les excepcions previstes a l'article 9.2 de l'RGPD.

Pel que fa a l'habilitació continguda al dret dels estats membres, el considerant 41 de l'RGPD disposa 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", però afegeix que això s'ha d'entendre "sin perjuicio de los requisitos de conformidad con el ordenamiento constitucional del Estado miembro de que se trate". En el cas de l'Estat espanyol, d'acord amb les exigències constitucionals, en tractar-se del desenvolupament d'un dret fonamental la norma que ho prevegi ha de tenir rang de llei (article 53 de la Constitució espanyola, CE).

En relació amb el principi de reserva de llei i concreció de la norma, cal tenir en compte la sentència del Tribunal Constitucional 76/2019, de 22 de maig. En aquesta sentència, el tribunal recorda que la ingerència estatal en l'àmbit dels drets fonamentals i les llibertats públiques requereix una norma amb rang de llei, i precisa els requisits indispensables que ha de reunir aquesta norma com a garantia de la seguretat jurídica:

> "[…] Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4). En otras palabras, "no sólo excluye apoderamientos a favor de las normes
>
> [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites" (STC 292/2000, FJ 15).
> La segunda exigencia mencionada constituye la dimensión cualitativa de la reserva de ley, y se concreta en las exigencias de previsibilidad y certeza de las medidas restrictivas en el ámbito de los derechos fundamentales**.** En la STC 292/2000, FJ 15, señalamos que, aun teniendo un fundamento constitucional, las limitaciones del derecho fundamental establecidas por una ley "pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación", pues "la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción"; "al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla". En la misma Sentencia y fundamento jurídico precisamos también el tipo de vulneración que acarrea la falta de certeza y previsibilidad en los propios límites: "no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, FJ 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado

> que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, FJ 15; 142/1993, de 22 de abril (RTC 1993, 142) , FJ 4, y 341/1993, de 18 de noviembre (RTC 1993, 341) , FJ 7)".

Així, la norma habilitadora ha de tenir un grau de concreció suficient i ha de ser previsible per al destinatari. En el cas objecte de consulta, pel que fa a la possibilitat d'utilitzar dades biomètriques amb la finalitat de recavar la signatura de l'usuari del servei de salut del seu CI, aquesta concreció es podria emparar en el dret de l'interessat a utilitzar sistemes de signatura electrònica legalment admesos, recollida legalment en el marc de la Llei 39/2015, dins de les previsions d'aquesta normativa, complint els requeriments de la mateixa.

A més, a la sentència també es determina que la norma ha d'establir garanties adequades, especialment quan es tractin categories especials de dades. En particular, el Tribunal manifesta el següent:

> "La exigencia de especial protección de esta categoría de datos está prevista en el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (RCL 1985, 2704) , de 28 de enero de 1981 (instrumento de ratificación publicado en el Boletín Oficial del Estado núm. 274, de 15 de noviembre de 1985), cuyo artículo 6 establece lo siguiente: "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las
> convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. [...]." […]
> Las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención. La naturaleza y el alcance de las garantías que resulten constitucionalmente exigibles en cada caso dependerán de tres factores esencialmente: el tipo de tratamiento de datos que se pretende llevar a cabo; la naturaleza de los datos; y la probabilidad y la gravedad de los riesgos de abuso y de utilización ilícita que, a su vez, están vinculadas al tipo
> de tratamiento y a la categoría de datos de que se trate. Así, no plantean los mismos problemas una recogida de datos con fines estadísticos que una recogida de datos con un fin concreto. Tampoco supone el mismo grado de injerencia la recopilación y el procesamiento de datos anónimos que la recopilación y el procesamiento de datos personales que se toman individualmente y no se anonimizan, como no es lo mismo el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la

> salud, la vida sexual o la orientación sexual de una persona física, que el tratamiento de otro tipo de datos.
> El nivel y la naturaleza de las garantías adecuadas no se pueden determinar de una vez para todas, pues, por un lado, deben revisarse y actualizarse cuando sea necesario y, por otro lado, el principio de proporcionalidad obliga a verificar si, con el desarrollo de la tecnología, aparecen posibilidades de tratamiento que resultan menos intrusivas o potencialmente menos peligrosas para los derechos fundamentales."

En la mesura que les categories especials de dades tenen especial protecció, superior a altres dades personals, "una protección adecuada y específica frente a su tratamiento constituye, en suma, una exigencia constitucional, sin perjuicio de que, como se ha visto, también represente una exigencia derivada del Derecho de la Unión Europea. Por tanto, el legislador está constitucionalmente obligado a adecuar la protección que dispensa a dichos datos personales, en su caso, imponiendo mayores exigencias a fin de que puedan ser objeto de tratamiento y previendo garantías específicas en su tratamiento, además de las que puedan ser comunes o generales."

En relació amb aquest punt, pel que fa al supòsit d'utilització de la signatura biomètrica, els termes de la consulta indiquen que s'empraria exclusivament a efectes de signatura, i no d'identificació del signant en el moment de la seva emissió; això determina que els riscos del tractament semblaria que són inferiors, en termes de seguretat.

4.2. Adequació al principi de minimització en el cas concret

Al marge del principi de licitud, qualsevol tractament ha de complir també la resta dels principis i obligacions derivats de la normativa de protecció de dades, com ara el principi de minimització (art. 5.1.*c* RGPD).

En aquest sentit, el Dictamen 3/2012 del Grup de treball de l'article 29 sobre l'evolució de les tecnologies biomètriques, afirmava el següent en relació amb l'anàlisi del compliment del principi de minimització:

> "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. 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."

Pel que fa a la signatura del CI, aquesta proporcionalitat podria complir aquests requeriments, per les raons següents:

- La identificació i autenticació de l'usuari de salut es fa presencialment, i simplement es tracta de recollir la seva signatura en el document de CI.

- La signatura electrònica digital, sense que sigui equiparable a la signatura manuscrita, tindria una força probatòria superior per a l'interessat davant d'altres tipus de signatura més simples, sempre que garanteixi la integritat i conservació.

- Tot i que es pot entendre que hi ha pèrdua de privacitat, ho és exclusivament quant a la realització de la signatura del document, i és una obligació legal de l'usuari del servei de salut prestar el seu consentiment, en relació amb el qual es manté la possibilitat de fer-ho manuscritament.

Les exigències derivades de la protecció de dades en el disseny (art. 25.1 RGPD) i, en especial, del principi de minimització, obliguen a escollir la tecnologia que resulti menys intrusiva des del punt de vista de la protecció de dades. El principi de minimització no es manifesta només a l'hora d'optar per alternatives que no impliquin el tractament de dades personals, o de tractar-les de manera que s'emprin les dades mínimes indispensables. També ha de comportar que, si es pot assolir una determinada finalitat sense haver de tractar dades de categories especials, aquesta opció ha de prevaldre davant altres opcions que sí que impliquin el tractament d'aquests tipus de dades.

Cal tenir en compte que les dades biomètriques, atès el seu caràcter personal i únic, constitueixen un mitjà fiable d'identificació (tot i que en determinades dades biomètriques pot haver-hi un risc de no identificabilitat). Però la fiabilitat com a sistema d'identificació està condicionada també per l'amplitud amb què es puguin utilitzar aquests sistemes d'identificació. Com més gran sigui el nombre de sistemes d'identificació que es basen en unes dades biomètriques o en una plantilla obtinguda a partir de dades biomètriques, major és el risc que aquesta dada pugui acabar essent utilitzada de manera inadequada i donant lloc a un risc d'usurpació o suplantació d'identitat. Aquest risc es pot incrementar, clarament, en funció de quina sigui la tecnologia emprada i del tractament que es doni a les dades biomètriques en brut o originals.

Per una banda, en funció de la tecnologia utilitzada una pèrdua de confidencialitat d'aquestes dades podria permetre la suplantació. Però és que, a més, aquestes dades no són modificables. És a dir, a diferència d'una contrasenya, en cas de pèrdua no es poden canviar.

Per altra banda, també hi ha riscos evidents, si la tecnologia emprada no garanteix de manera suficient que la plantilla obtinguda a partir de les dades biomètriques no coincidirà amb l'emprada en altres sistemes similars.
A l'efecte de determinar els riscos existents i les mesures per mitigar-los, poden ser d'ajuda les Directrius 3/2019 sobre el tractament de dades personals mitjançant dispositius de vídeo del CEPD; en particular l'apartat 5.2, relatiu a les mesures suggerides per minimitzar els riscos a l'hora de tractar dades biomètriques.

De la lectura conjunta d'aquestes previsions se'n desprèn que l'element clau a l'hora de considerar les dades relatives a les característiques físiques, fisiològiques o conductuals d'una persona física com a dades biomètriques és que aquestes dades es tractin amb mitjans tècnics específics, amb la finalitat d'identificar o d'autenticar de manera unívoca la seva identitat. Quan això succeeix, ens trobarem davant un tractament de categories especials de dades personals.

Per contra, quan les dades biomètriques no es tracten a efectes d'identificar i autenticar la persona, els efectes jurídics i els condicionants per a què la seva implementació sigui vàlida es poden modular, tal com s'exposa a la consideració jurídica subsegüent.

4.3. En el cas plantejat, la signatura biomètrica del CI no genera cap plantilla biomètrica, ni serveix per identificació i autenticació simultàniament a la seva emissió

A més, en els termes plantejats a la consulta, s'ha de tenir present que la signatura biomètrica no s'utilitza com a sistema d'identificació i autenticació, sinó exclusivament als efectes de signar el CI i garantir-ne la integritat i conservació. En aquest sentit, s'indica que "el metge identificaria presencialment al pacient com usuari del sistema públic de salut", davant del qual es fa la signatura electrònica presencial (SMCE) del consentiment informat (CI), i es manté l'alternativa en paper.

Com indica la Guia de l'AEPD sobre tractaments de control de presència mitjançant sistemes biomètrics, de novembre de 2023, "un dato biométrico contenido en un sistema se almacena en forma de una plantilla o patrón biométrico. Una plantilla biométrica es una forma de escritura de una característica biométrica humana, como un rostro o una huella dactilar, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados. La plantilla biométrica no está orientada a ser interpretada por una persona, como una fotografía, sino que está orientada a ser tratada en un proceso automatizado, es decir, ser eficiente y eficazmente interpretable por una máquina. Esta forma de almacenamiento permitiría singularizar a un individuo y ejecutar acciones de forma automática, perfilar o inferir información sobre un sujeto como actitudes o patrones de comportamiento, etc."

En el mateix sentit, el Grup de treball de l'article 29 defineix els sistemes biomètrics com a: "aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes."

El tractament de les dades biomètriques en un sistema biomètric sol constar de diferents processos que inclouen: el registre, l'emmagatzematge i la correspondència. I aquestes operacions suposen la generació prèvia d'una plantilla (com és el cas de l'empremta digital o el reconeixement facial).

Per contra, en el cas objecte de consulta, la signatura del CI mitjançant signatura electrònica digital no suposa l'articulació d'una plantilla, ni realitzar cap operació de identificació i autenticació, ja que la identificació presencial prèvia es manté i no es veu alterada com a conseqüència de la signatura biomètrica, ni es verifica automàticament la signatura emesa amb una plantilla biomètrica prèviament registrada.

En aquest sentit, les Directrius 05/2022 del Comitè Europeu de Protecció de Dades (CEPD) sobre l'ús del reconeixement facial en l'àmbit de les forces de l'ordre públic (versió 2.0, de 26 d'abril de 2023), determina a l'apartat 12 que el concepte de dada biomètrica abasta l'autenticació i la identificació, i en tots dos procediments es tracten dades dirigides a identificar una persona física, com a conseqüència de la qual és aplicable la prohibició de l'article 9.1 de l'RGPD. Això s'ha d'aplicar "no sólo a los tratamientos dirigidos a la identificación sino también a los supuestos de tratamientos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma."

Així ho indica l'AEPD en la Guia indicada, si bé cal tenir present que no ens trobem amb un sistema d'identificació i/o autenticació, ja que aquesta s'ha fet prèviament amb caràcter presencial. El que es fa és incorporar una signatura biomètrica a un document, sense verificar la identitat del signatari (identificació que, si escau, tan sols es realitzarà posteriorment, en cas de discrepància). Aquest punt és rellevant envers entendre que hi ha una base jurídica habilitadora del seu tractament, en els dos moments en el qual aquest es produeix.

5. Avaluació d'impacte de protecció de dades

Finalment, recordar que, abans de decidir posar en marxa d'un sistema d'aquest tipus, cal tenir en compte que l'article 35 de l'RGPD preveu la necessitat de fer una avaluació de l'impacte relativa a la protecció de dades (AIPD) en el tractaments, especialment si empren noves tecnologies que comportin un alt risc per als drets i llibertats de les persones. A aquests efectes, i d'acord amb l'article 35.4 de l'RGPD, aquesta Autoritat ha publicat una llista de tipus de tractaments de dades que requereixen avaluació d'impacte relativa a la protecció de dades (https://apdcat.gencat.cat/web/.content/02-

drets_i_obligacions/obligacions/documents/Lista-DPIA-CAT.pdf), en la qual es determina que cal fer-la en la majoria dels casos en què el tractament compleixi dos o més criteris de la llista. Entre aquests criteris, en el cas que s'analitza hi poden concórrer els següents:

> "[...]
> 5. Tractaments que impliquin l'ús de dades biomètriques amb el propòsit d'identificar de manera única a una persona física.
> [...]
> 10. Tractaments que impliquin la utilització de noves tecnologies o un ús innovador de tecnologies consolidades, incloent la utilització de tecnologies a una nova escala, amb un nou objectiu o combinades amb altres, de manera que suposi noves formes de recollida i utilització de dades amb risc pels drets i llibertats de les persones.[...]"

En conseqüència, és necessari fer una avaluació de l'impacte relativa a la protecció de dades, en la qual cal avaluar tant la legitimitat del tractament i la seva proporcionalitat, com la determinació dels riscos existents i les mesures per mitigar-los (art. 35 RGPD).

6. Tractaments objecte d'anàlisi

Abans de resoldre en concret les consultes plantejades, s'han de diferenciar els dos tractaments de dades objecte d'anàlisi ja que, en el marc de l'article 9.2 de l'RGPD, les bases jurídiques legitimadores són diferents:

a) Un primer tractament seria el derivat de la recollida de la signatura, en el moment de signar el document corresponent.

   És important tenir present que, en aquests casos, en els termes en els quals està plantejada la consulta, no es realitza un control d'autenticació de la persona que signa, sinó que simplement s'incorporaria aquesta signatura al document signat i es conservaria per a un moment posterior.

   Tal com ja es va indicar al dictamen 21/2020, "la signatura biomètrica obtinguda sobre una tauleta, mesurant la formació de les lletres, la direcció dels trets, pressió i altres característiques dinàmiques úniques, també s'ha de considerar dada de categoria especial, en la mesura que se sotmeti a un tractament tècnic específic amb la finalitat de confirmar-ne l'autoria."

   A sensu contrario, si en el moment de recollir aquesta signatura biomètrica no es contrasta l'autoria del document, estem davant d'una finalitat de tractament exclusivament limitada a recollir aquesta signatura, en el marc d'un procediment administratiu.

Per aquesta raó, si és una signatura legalment admesa en el marc de la Llei 39/2015, la signatura biomètrica s'adequaria a la normativa de procediment i, tal com indiquem posteriorment, també a la normativa de protecció de dades.

b) Un segon tractament, en cas de discrepància. És a dir, si la persona que ha signat el CI nega haver produït aquesta signatura, suposaria la pràctica d'una eventual pericial tecnològica contradictòria, per a la lliure apreciació de la prova.

En aquest cas, l'anàlisi de la signatura biomètrica comportaria un tractament de categories especials de dades amb la finalitat d'identificar la persona. Això requeriria una base legitimadora específica de les citades en l'article 9.2, que podem avançar que seria la recollida a la lletra *f*, quan el tractament és necessari per la formulació, l'exercici o la defensa de reclamacions.

A més, cal tenir present que no es tractaria necessàriament de contrastar la signatura biomètrica emesa amb altres d'anteriors (cap de les quals és pròpiament una plantilla), sinó que es podria procedir a generar noves signatures biomètriques, a l'efecte de fer l'anàlisi pericial corresponent.

7. Compliment del principi de transparència amb independència del sistema de signatura a utilitzar

Amb caràcter general, de la mateixa manera en què l'interessat no pot tenir una pèrdua de garanties com a conseqüència de la tramitació digital, qualsevol sistema de signatura electrònica ha de garantir el compliment del principi de transparència.

En aquest cas, el supòsit de fet plantejat indica que, al marge de mantenir en tot cas com a opció alternativa la signatura manuscrita del CI en suport paper, el document de CI inclouria totes les dades que s'han d'incorporar al CI, la informació exigida per la normativa de protecció de dades i "permetria al pacient llegir prèviament el document de CI en format electrònic (amb previsió de facilitar-li un temps de reflexió, cas de ser necessari)...".

En els termes plantejats, es compliria el principi de transparència.

També en el supòsit de la signatura mitjançant LMS, s'indica que "el ciutadà té penjada tota la informació necessària amb el format i contingut vàlid per prendre la decisió de signar."

A la Guia d'usuaris de salut redactada per l'APDCAT, es tractava aquesta qüestió a les FAQ, en els termes següents:

> "He anat a una mútua a fer-me la revisió mèdica de l'empresa, i em demanen que signi a la pantalla d'un dispositiu electrònic per informar-me de com tractaran les meves dades. M'expliquen que puc llegir-ho en un full en paper que em

> mostren i que més endavant m'enviaran la clàusula informativa per correu electrònic. És correcte?
>
> No. Demanar una signatura a un pacient sense haver-lo informat prèviament de quines dades es recolliran, per a quin motiu, a qui es comunicaran, etc., i sense que hagi pogut aclarir els seus dubtes, no és correcte".

D'acord amb l'exposat, cal facilitar la informació que exigeix la llei de manera que en quedi constància, i el pacient l'ha de poder entendre. Mai no s'hauria de signar en blanc, si no se sap a què s'associa la signatura. El pacient té dret a obtenir una còpia de qualsevol document que hagi signat.

En aquest sentit, s'ha de garantir que aquesta informació sigui accessible però, al mateix temps, articular mecanismes que permetin acreditar que l'interessat va llegir o va tenir la possibilitat de llegir-ne el redactat.

No ens pertoca determinar quins han de ser aquests mecanismes però, per exemple, la utilització de tècniques de *scroll (*que garanteixin que l'interessat ha recorregut visualment tot el document) o similars es podrien considerar adequades.

III

Analitzats els aspectes jurídics rellevants quant a la consulta formulada, cal procedir a respondre-la d'acord amb els arguments prèviament desenvolupats.

Exposats els supòsits d'utilització de la SMCE presencial i signatura electrònica remota, s'interessa el pronunciament d'aquesta Autoritat sobre els aspectes següents:

a) En relació amb la signatura mitjançant LMS del document de CI (punt 2.1) es realitzen les següents qüestions:
 Tenint en compte que l'usuari podria signar el document de CI, seria suficient l'autenticació mitjançant usuari/contrasenya o caldria augmentar el nivell mitjançant altres mecanismes de autenticació com els serveis intermediats per VALID?

Tal com s'ha indicat prèviament, la determinació dels sistemes d'identificació i signatura corresponen a cada Administració. L'accés a LMS amb un usuari i contrasenya és plenament vàlid, si bé un usuari i contrasenya no serveix per signar.

En aquest punt, convé recordar que el dictamen CNS 2/2017, en relació amb la consulta formulada en relació amb l'obtenció del codi i contrasenya d'accés al portal "CatSalut – La meva Salut" en línia, ja indicava que:

> "El procés de registre, identificació i autenticació de les persones físiques per tal que es puguin relacionar amb les Administracions publiques, amb vistes a exercir drets o realitzar diferents tràmits, és una fase especialment crítica, ja que

> és en aquest moment que l'Administració s'ha d'assegurar que es tracta efectivament de la persona física que pot exercir un determinat dret o realitzar determinat tràmit, i no d'una altra persona que es registra en nom seu.
>
> Per tant, en aquesta primera fase cal aplicar les mesures adequades per tal de garantir que la persona física afectada és identificada adequadament i que és aquesta la que podrà exercir un determinat dret, o podrà accedir i tractar determinada informació personal. Als efectes que ens ocupen, una mesura clau es refereix, precisament, a l'elecció del sistema adequat de registre i identificació.
>
> Així, des de la perspectiva de la protecció de dades cal implementar mecanismes i procediments prou segurs a l'hora d'identificar i autenticar les persones usuàries d'un servei, per tal d'evitar la suplantació de la persona usuària o l'accés a informació personal per part de terceres persones no autoritzades, entre d'altres. Si aquesta primera fase de registre no compta amb suficients garanties, la resta del procediment (l'exercici de drets, la realització de determinats tràmits, l'accés a informació personal, etc), no poden considerar-se segures."

I afegia:

> "Per tant, des de la perspectiva de la protecció de dades personals, sembla clar que el sistema de registre de persones usuàries del portal "CatSalut – La meva Salut", hauria d'evitar la suplantació o "alteració de la identitat" de les persones afectades (en els termes de l'art. 8.2.c) RUE 910/2014), és a dir, hauria d'oferir un nivell alt de seguretat, i evitar l'accés indegut a la informació personal de "La meva Salut" per part de terceres persones no autoritzades, que seria contrari a la normativa de protecció de dades personals (LOPD i RGPD) i a la normativa sectorial (Legislació d'autonomia del pacient)."

Si a LMS ens trobem en un entorn d'identificació i autenticació alt, la signatura de documents en aquest entorn ha de garantir la integritat i conservació d'allò que se signi. Això suposa que, en el moment de la signatura del CI, serà necessari un sistema de signatura fort jurídicament i tècnicament (dins dels admesos com a sistemes de signatura de la llista de prestadors de serveis de confiança, en el marc de l'article 10 de la Llei 39/2015).

Així mateix, cal tenir present la previsió de l'article 10.4 de la Llei 39/2015, que admet que els sistemes d'identificació serveixen com a sistema de signatura, quan permeten acreditar l'autenticitat de l'expressió de la voluntat i consentiment de l'interessat (com podria ser la incorporació d'un segell electrònic).

En qualsevol cas, l'autenticació de la declaració de voluntat que suposa el CI i la seva integritat és un acte que ha de ser realitzat o signat de manera singularitzada a LMS; es a dir, s'ha de produir un acte formal de signatura.

De la mateixa manera, l'articulació del tràmit de signatura del CI s'ha de fer d'una manera que permeti acreditar que el ciutadà té penjada tota la informació, i que hi ha accedit de manera efectiva. Com seria amb l'articulació d'un sistema que no permeti signar sense haver obert els documents i haver-los recorregut visualment -*scroll*- (addicionalment al segell de temps que s'indica al supòsit de fet).

- Tenint en compte la resposta del punt anterior, seria suficient la signatura mitjançant mecanisme de codi d'un sol ús?

En principi, la signatura digital amb un codi d'un sol us (OTP) és un mitjà legalment admès per signar que, en funció de les condicions establertes (per exemple, el temps de validesa del codi o l'establiment de requeriments de seguretat addicionals) pot arribar a tenir un nivell de seguretat substancial que, tal com indica l'article 8 del ReIDAS, redueix substancialment el risc de suplantació de la persona.

En qualsevol cas, ja hem indicat que correspon a cada Administració, en funció del tràmit o servei, i en el marc de la normativa de signatura electrònica, fer l'anàlisi de riscos i determinar si admet o no aquest tipus de signatura que, en tot cas, com ja hem indicat, ha de tenir implementats igualment mecanismes addicionals que permetin acreditar la integritat d'allò que se signa.

A partir d'aquesta prèvia determinació, no es negaran efectes jurídics a les signatures emeses i caldrà a les circumstàncies específiques del cas en concret, en cas de discrepància.

b) En relació amb el supòsit de signatura de CI de pacients mitjançant SMCE (punt 2.2) presencial amb tauleta:

En relació amb la signatura del CI de pacients, es considera conforme a la normativa de protecció de dades personals el consentiment del pacient com a base legal per al tractament de les seves dades biomètriques quan s'utilitza la SMCE presencial –mitjançant tauleta i punter digital- si se li ofereix aquesta modalitat digital com a opció alternativa a la manuscrita tradicional en format paper?.

La qüestió relativa a la signatura biomètrica és la més complexa de les consultes formulades, des del punt de vista de la protecció de dades.

En tractar-se de la signatura biomètrica de dades especialment protegides, el tractament tan sols és possible en el marc dels supòsits de l'article 9.2 de l'RGPD.

No obstant això, tal com s'ha indicat, en aquest supòsit la identificació i autenticació de l'usuari del servei de salut s'ha fet presencialment amb caràcter previ, i la signatura biomètrica es fa exclusivament a l'efecte d'incorporar la signatura electrònica al CI. No hi ha, però, una plantilla biomètrica de signatura prèviament registrada, sinó que -en els termes plantejats al supòsit- el CI signat biomètricament es desaria de manera segura per al cas de discrepància en el futur. A més, en tot cas es dona l'alternativa manuscrita.

Aquesta diferenciació és rellevant, ja que es produeixen dos tractaments de dades, amb bases legitimadores diferenciades:

a) Un primer tractament, el derivat de la recollida de la signatura, ho és exclusivament a aquest efecte, ja que la identificació i autenticació s'ha fet presencialment, es manté presencialment i el CI simplement se signaria per un sistema de signatura que hauria de trobar-se en el marc de l'article 10.2 de la Llei 39/2015, i per part d'un prestador de serveis de confiança reconegut legalment.

   Aquest punt és important, ja que la manca de base jurídica en determinats tractaments de categories especials de dades en quan a les dades biomètriques ho és, en el termes actualment debatuts, en quan a la seva utilització com a sistema de identificació i autenticació i la manca de proporcionalitat que es donaria en aquest cas. . Però no seria el cas de la consulta plantejada, en què la dada biomètrica s'incorpora exclusivament al document del CI sense verificar la identitat del signatari.

   Així, la base jurídica pel tractament de la signatura biomètrica la trobaríem, d'una banda, en el consentiment de l'interessat (l'alternativa de la signatura manuscrita s'ha d'oferir sempre) i en el fet que, en tractar-se exclusivament de la recollida i dipòsit de la signatura biomètrica, sense verificar-ne l'autoria, es conservaria de manera segura de cara al futur, per al cas d'una eventual discrepància. D'acord amb l'exposat, semblaria que aquest tractament superaria el test de proporcionalitat.

   Al mateix temps, d'acord amb la lletra *h* de l'article 9.2 de l'RGPD, la signatura del CI és necessària per prestar l'assistència.

   En definitiva, l'element diferenciador d'altres supòsits (com el control horari amb empremta digital) és que ens trobem amb una signatura biomètrica que, en el moment de recollir-la, no s'utilitza per identificar i autenticar, sinó que serveix exclusivament per signar. Una vegada emesa tampoc no es valida amb una plantilla biomètrica, cosa que determina que no s'utilitza per identificar i autenticar la persona, que és on hi ha problemes de base jurídica en termes de protecció de dades.

b) En cas de discrepància es donaria un segon tractament, que seria una eventual pericial tecnològica contradictòria en què la persona que negués la signatura del CI hauria de signar novament, i es procediria a la comparativa pericial (com hem dit, no hi ha plantilla prèvia). En aquest cas, la base legitimadora seria la lletra *f* de l'article 9.2 de l'RGPD (el tractament és necessari per la formulació, l'exercici o la defensa de reclamacions).

Quines garanties caldria preveure des del punt de vista de la normativa de protecció de dades addicionalment, juntament amb el consentiment al que es refereix l'anterior punt 3.2.1 i, en concret, la transparència de la informació, l'adopció de mesures de seguretat i l'execució d'AIPD?

Tal com s'ha indicat, tots tres aspectes són necessaris per emprar les dades biomètriques, si bé el primer -la transparència de la informació- és aplicable a la signatura del CI per qualsevol tipus de signatura. El supòsit de fet plantejat així ho preveu, en referir-se a les condicions prèvies i posteriors a la signatura del CI.

Pel que fa a les mesures de seguretat, només recordar les obligacions del responsable del tractament, d'acord amb l'article 32 de l'RGPD, que són aplicables amb caràcter general.

c) En relació amb el supòsit de signatura de CI de donants de sang i teixits mitjançant SMCE (punt 2.3) presencial amb tauleta:

Es formulen les mateixes preguntes que en l'anterior apartat, però en relació amb els donants de sang i teixits.

La consulta indica que es tracta d'un supòsit molt similar a l'anterior i, en aquest punt, coincidim que la resposta és i ha de ser la mateixa, ja que la concurrència del component de voluntarietat que presideix l'actuació de les persones donants de sang i teixits no altera l'anàlisi jurídica realitzada. Ans al contrari, aquesta voluntarietat reforçaria la base legitimadora del consentiment explícit.

d) En relació amb el supòsit de signatura de contractes laborals mitjançant signatura digital remota (punt 2.4).

- ¿Es pot considerar dada biomètrica l'obtinguda mitjançant signatura amb el dit sobre la pantalla del dispositiu utilitzat per l'usuari?

En els termes plantejats, si es tracta simplement de la pressió sobre la pantalla del dispositiu en el moment de signar no ens trobaríem amb una dada biomètrica, sinó exclusivament amb una condició necessària per signar digitalment que, en cap cas, suposa l'aplicació del règim de les categories especials de dades.

En aquest sentit, aquesta signatura no biomètrica podria ser vàlida jurídicament, sense perjudici que la seva força probatòria seria inferior a la d'altres sistemes de signatura que impliquin mesures de seguretat corresponents a un nivell superior. Però, com indica l'article 25 del ReiDAS, se li han de reconèixer efectes jurídics, en funció del cas en concret.

- En cas que es consideri dada biomètrica, s'adequaria a la normativa de protecció de dades personals el consentiment de la persona interessada com a base legal per tractar les seves dades personals, inclòs el paràmetre biomètric, implicades en el procés d'utilització de la signatura electrònica remota per signar un contracte laboral, si s'ofereix aquesta modalitat electrònica com a opció a la manuscrita tradicional en format de paper?

Tal com s'ha indicat, no ens trobem amb el tractament de dades biomètriques.

- Quines garanties caldria preveure des del punt de vista de la normativa de protecció de dades addicionalment, juntament amb el consentiment al que es refereix l'anterior punt i, en concret, la transparència de la informació, l'adopció de mesures de seguretat i la realització d'AIPD?

Si no ens trobem davant de categories especials de dades (al menys així es derivaria dels termes de la consulta en aquest supòsit en concret) no caldria fer una AIPD.

Per contra, sí que caldria complir els requeriments de transparència de la informació i adoptar l es mesures de seguretat adequades al tràmit corresponent.

En definitiva, es tracta d'un sistema de signatura que s'hauria de resoldre d'acord amb els principis i condicionats del primer dels apartats objecte de consulta.

Signat per:
Meritxell Borràs Solé
Directora de l'Autoritat Catalana de Protecció de Dades
Autoritat Catalana de Protecció de Dades

2024.01.22 12:30:41 +01'00'

Meritxell Borràs i Solé
Directora