CNS 2/2017

Dictamen 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

Es presenta davant l'Autoritat Catalana de Protecció de Dades una consulta en què s'explica que el CatSalut està desenvolupant el portal *"CatSalut – La meva Salut"* com un espai digital online segur, personal i intransferible, que ha de permetre als ciutadans accedir a la seva informació i a determinats serveis.

La consulta explica que, actualment, el procediment d'assignació de codi i contrasenya per accedir al portal *"CatSalut – La meva Salut"* requereix la identificació presencial de la persona afectada en el CAP.

Es consulta sobre la possibilitat que els ciutadans puguin obtenir el codi i contrasenya d'accés a *"CatSalut – La meva Salut",* en línia, amb una identificació basada en l'aportació d'informació coneguda per la persona interessada i pel CatSalut, ateses les previsions de l'Ordre PRE/226/2016, de 29 d'agost, per la qual es regulen els aspectes tècnics i organitzatius del procés de registre previ en el fitxer Seu electrònica de l'Administració de la Generalitat de Catalunya necessari per als sistemes d'identificació i signatura basats en claus concertades.

Analitzada la petició, que no s'acompanya de cap altra documentació, vista la normativa vigent aplicable, i l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

La consulta explica que el CatSalut està desenvolupant el portal *"CatSalut – La meva Salut"* com un espai digital online segur, personal i intransferible, que ha de permetre als ciutadans accedir a la seva informació i a determinats serveis.

Mitjançant Ordre SLT/371/2015, de 23 de desembre, de modificació de l'Ordre SLT/25/2014, de 3 de febrer, per la qual s'actualitza la regulació dels fitxers que contenen dades de caràcter personal del Departament de Salut i de les entitats vinculades o que en depenen (DOGC núm. 7028, de 30.12.2015), es crea el fitxer *"Gestió de la identificació per a l'accés a sistemes d'informació de salut",* que té per finalitat i usos: *"possibilitar l'accés multicanal a sistemes d'informació de salut"* i *"facilitar mecanismes d'identificació per canal electrònic o mitjançant dispositius mòbils per accedir a informació personal de salut, fer ús dels serveis d'atenció no presencial i realitzar tràmits electrònics i recollir les dades identificatives i d'autorització d'accés a sistemes d'informació de salut, així com el manteniment dels mecanismes d'identificació."*

Segons la consulta, pel que fa a l'accés al portal *"Cat@Salut La Meva Salut",* actualment *"el procediment d'assignació de codi i contrasenya requereix la identificació presencial en el CAP".*

Atesa la informació disponible al web https://lameva salut.gencat.cat, per tal d'accedir al portal *"Cat@Salut La Meva Salut",* es sol·licita a la persona usuària que introdueixi el Codi d'Identificació Personal (CIP) que es troba a la targeta sanitària. A partir d'aquí, la persona afectada es pot autenticar a través d'un dels dos sistemes alternatius que indica el portal, o bé una contrasenya, o bé un certificat digital.

En el primer cas, per tal d'autenticar-se a través de contrasenya, la informació disponible al web explicita que: *"Cal que us adreceu al vostre centre d'atenció primària o centre dotat amb la finalitat d'assignar credencials, presenteu la vostra targeta sanitària, document identificatiu, verifiqueu/informeu les vostres dades personals i signeu la sol·licitud de consentiment amb l'objectiu de poder generar les vostres dades d'autoregistre. (...)."*

A banda d'aquesta possibilitat (identificació presencial en el CAP), en el moment d'emetre aquest dictamen també es troba operativa la possibilitat d'accedir al portal *"CatSalut – La meva Salut",* utilitzant un certificat electrònic reconegut, sense haver d'adreçar-se personalment al CAP corresponent, com es desprèn de la informació disponible al web citat.

En qualsevol cas, i a banda d'aquesta doble possibilitat, cal analitzar, des de la perspectiva de la protecció de dades, la possibilitat que els ciutadans puguin registrar-se per a accedir i utilitzar els serveis de *"CatSalut – La meva Salut"* en línia, sense personar-se al CAP ni utilitzar certificats electrònics reconeguts.

III

Pel que fa al marc normatiu en el que es situa la consulta, cal referir-se a l'article 9 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (LPAC), segons el qual:

> *"1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.*
>
> *2. Los interesados* ***podrán identificarse electrónicamente*** *ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad. En particular, serán admitidos, los sistemas siguientes:*
>
> *a) Sistemas basados en* ***certificados electrónicos reconocidos*** *o cualificados de firma electrónica (…).*
>
> *b) Sistemas basados en* ***certificados electrónicos reconocidos*** *o cualificados de sello electrónico (…).*
>
> *c)* ***Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido,*** *en los términos y condiciones que se establezcan.*
>
> ***Cada Administración Pública podrá determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos,*** *si bien la admisión de alguno de los sistemas de identificación previstos en la letra c) conllevará la admisión de todos los previstos en las letras a) y b) anteriores para ese trámite o procedimiento.*
>
> *3. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo*

prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo."

Segons es desprèn d'aquesta previsió, en principi els interessats poden identificar-se davant les Administracions públiques a través de sistemes basats en certificats electrònics (apartats a) i b) de l'art. 9.2 LPAC), i també a través de sistemes de "clau concertada", o d'altres sistemes que l'Administració corresponent pugui establir.

Segons l'article 9.2 LPAC, citat, cada Administració ha de determinar quins sistemes d'identificació resulten admissibles en relació amb els diferents tràmits o procediments que s'hagin de dur a terme.

Segons la disposició addicional setzena de la Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya (incorporada a través de la Llei 16/2015, del 21 de juliol, de simplificació de l'activitat administrativa de l'Administració de la Generalitat i dels governs locals de Catalunya i d'impuls de l'activitat econòmica):

1. Les administracions públiques de Catalunya, en el termini d'un any des de l'entrada en vigor d'aquesta llei, han d'establir una solució d'interoperabilitat o compatibilitat dels sistemes d'identificació, autenticació i signatura electrònica no avançada a partir de la utilització de claus concertades en un registre previ com a usuari, l'aportació d'informació coneguda per ambdues parts o altres sistemes no criptogràfics, en els termes i les condicions establerts per reglament.

2. Les claus concertades en un registre previ, la informació coneguda pels ciutadans i per les administracions públiques, i les dades i els codis alfanumèrics que figurin impresos en targetes identificadores o d'accés a serveis públics expedides per les administracions públiques, inclosa la targeta d'identificació sanitària, poden ésser emprats per a verificar la identificació i autenticació dels ciutadans i fer el registre electrònic de llur identitat sense certificat digital. En tot cas, la persona interessada ha d'ésser informada i requerida a consentir, pel mateix canal electrònic, que el procés de validació d'aquestes dades requereix la consulta de les seves dades en el fitxer corresponent.

3. El sistema d'identificació, autenticació i signatura electrònica no avançada és vàlid en l'àmbit de l'Administració de la Generalitat i aplicable en les seves relacions i actuacions amb els ciutadans, les entitats, fundacions i associacions inscrites en els registres públics, les empreses i altres organismes públics. Els termes, les condicions i els supòsits d'utilització d'aquest sistema de signatura electrònica i l'àmbit subjectiu d'aplicació han d'ésser determinats per ordre del conseller competent en matèria d'atenció ciutadana.

En desenvolupament d'aquestes previsions legislatives, el Decret 232/2013, de 15 d'octubre, pel qual es crea la Seu electrònica, disposa que l'Administració de la Generalitat ha de garantir la identificació de les persones físiques o jurídiques a través d'un sistema de signatura electrònica (art. 9.1). L'apartat 2 del mateix article 9, preveu que el sistema de signatura electrònica ha de basar-se en documents identificadors, certificats digitals, utilització de claus concertades prèviament en un registre, *"o qualsevol altre sistema establert per la regulació de cada procediment".*

L'article 3.e) del mateix Decret 232/2013, defineix les *"claus concertades"* com el *"sistema d'identificació alternatiu al certificat digital i que consisteix en l'ús d'una clau d'accés que proporciona l'Administració i que és confidencial i intransferible."*

És a dir, el marc normatiu estudiat estableix la possibilitat que les Administracions públiques seleccionin i articulin diferents sistemes d'identificació i autenticació dels ciutadans, per tal que aquests puguin relacionar-s'hi i dur a terme diferents tràmits.

En aquest context, l'Ordre PRE/226/2016, a la que es refereix la consulta, preveu el següent en l'exposició de motius:

"El sistema d'identitat electrònica de la Generalitat, més enllà d'admetre i regular l'ús i els casos d'aplicació dels sistemes criptogràfics tradicionals basats en certificats digitals, ***incorpora un sistema d'identificació*** *i signatura electrònica no criptogràfics* ***anomenat idCAT Mòbil*** *basat en la utilització de claus concertades prèviament en un registre i la tramesa d'un codi d'un sol ús al telèfon mòbil.* ***Aquest sistema exigeix com a requeriment previ el registre de la ciutadania en el fitxer anomenat Seu electrònica*** *de l'Administració de la Generalitat de Catalunya (en endavant fitxer Seu electrònica) que recull les dades de contacte de les persones, les quals constitueixen la informació coneguda per ambdues parts, ciutadania i Administració, i que permet fer les validacions corresponents prèvies a la tramesa del codi d'un sol ús al telèfon mòbil."*

L'Ordre PRE/226/2016 té per objecte *"regular els aspectes tècnics i organitzatius corresponents per a la implantació del procés de registre previ en el fitxer Seu electrònica necessari en els sistemes d'identificació i signatura basats en claus concertades"* (art. 1).

El fitxer *"Seu electrònica",* esmentat, creat per l'Ordre PRE/208/2015, de 8 de juliol, té per finalitat: *"Possibilitar la comunicació amb la ciutadania per qualsevol canal i facilitar la identificació i signatura per canal electrònic de les persones que accedeixin a la Seu electrònica de l'Administració de la Generalitat de Catalunya (...)."*

Aquest és un aspecte que cal fer notar ja d'entrada, atès que l'accés a *"CatSalut – La meva Salut"* no s'efectua a partir del fitxer *"Seu electrònica",* sinó del *fitxer "Gestió de la identificació per a l'accés a sistemes d'informació de salut",* al qual ens hem referit. No obstant això, analitzarem igualment la possibilitat d'emprar un mecanisme d'identificació equivalent als descrits en aquesta Ordre.

L'article 4 de l'Ordre PRE/226/2016, detalla com es duu a terme el registre al fitxer *"Seu electrònica",* i la identificació amb el sistema "idCAT Mòbil" (o sistema d'identificació electrònica "idCAT-SMS", segons l'Acord de Govern, GOV/92/2015, de 16 de juny, pel qual s'aprova el sistema d'identificació electrònica idCAT-SMS i l'ús del Validador de credencials d'identitat (VALid)), en els següents termes:

> *"**Per realitzar el registre de les dades de contacte en el fitxer Seu electrònica i per a la identificació i signatura mitjançant el mecanisme idCAT Mòbil cal verificar la identitat de les persones interessades** així com l'aportació d'unes dades mínimes i necessàries a l'efecte.*
>
> *4.1 Requisits per a la inscripció:*
> *a) Ser major de 16 anys.*
> *b) Acreditar la personalitat mitjançant un dels següents documents reconeguts: (...).*
> *c) Aportar un correu electrònic i un telèfon mòbil.*
>
> ***4.2 Modalitats de registre:***
> *a) Amb* ***identificació presencial*** *a les oficines de la Generalitat i altres entitats de registre habilitades a l'efecte.*
> *b) En línia, amb identificació mitjançant els* ***certificats*** *que s'esmenten en l'article 6.3.1 d'aquesta Ordre.*
> *c)* ***En línia,*** *amb identificació basada en l'aportació* ***d'informació coneguda*** *per la persona interessada i per l'Administració.*
>
> *(...)."*

En qualsevol cas, a partir del registre en el dit fitxer de les dades de contacte de les persones que es relacionen amb l'Administració de la Generalitat a través de les

distintes modalitats de l'article 4.2 de l'Ordre PRE/226/2016, que puguin correspondre en cada cas –com de fet estableix el propi article 9.2, darrer paràgraf, de la Llei 39/2015, citada-, les persones podran interactuar amb l'Administració de la Generalitat a través de la seva Seu electrònica, que és única per a tots els òrgans de l'Administració de la Generalitat (art. 4 Decret 232/2013).

Ara bé, sens perjudici d'aquestes previsions que, amb caràcter general, habiliten el registre de les persones usuàries afectades a través de diversos sistemes, cal determinar si la utilització d'un sistema en línia resulta adequat, específicament, per registrar-se i identificar-se al portal *"Cat Salut-La meva Salut",* en els termes que planteja la consulta.

IV

Cal analitzar quins són els sistemes de registre i identificació adequats, des de la perspectiva dels principis i garanties de la normativa de protecció de dades de caràcter personal.

Aquesta Autoritat ha analitzat en ocasions anteriors (entre d'altres, els Dictàmens CNS 3/2010, CNS 25/2016, o CNS 37/2016), les característiques dels processos d'identificació i autenticació de persones usuàries que permeten accedir a diferents serveis o prestacions que ofereixen les administracions públiques, i l'exercici de drets (com pot ser, entre d'altres, l'exercici del dret a vot, o la participació en consultes populars).

Com ha posat de manifest l'Autoritat, 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.

Amb més motiu, cal extremar les precaucions de seguretat i fiabilitat en el registre de les persones usuàries, quan la informació personal a la que es podrà accedir a partir d'aquest registre sigui informació personal mereixedora d'especial protecció.

La informació personal a la que es pot accedir a través del portal esmentat, és informació sobre els diferents processos assistencials del pacient, en definitiva, informació continguda en la història clínica de cada pacient, la qual es troba regulada i protegida per una regulació específica (Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació

clínica, i 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).

Cal tenir en compte doncs que a través de la utilització per part de l'usuari (persona física atesa pel sistema públic de salut) del portal *"CatSalut - La meva Salut",* es pot accedir i tractar informació personal, com són les dades de salut de la persona afectada (art. 7.3 Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), i arts. 4.15 i 9 Reglament general de protecció de dades (UE) 2016/679 (RGPD), que va entrar en vigor el 25 de maig de 2016, i que serà aplicable a partir del 25 de maig de 2018 (art. 99 RGPD)). No només això, sinó que es podran realitzar determinades accions (consulta i sol·licitud de visites, visualitzar resultats de proves mèdiques, etc...).

En aquest punt, cal tenir en compte que el Reglament (UE) nº 910/2014, de 23 de juliol de 2016, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior (en endavant, RUE 910/2014), estableix **diferents nivells de seguretat –baix, substancial i alt- per als sistemes d'identificació electrònica**, que el mateix RUE 910/2014 (art. 8.2) defineix en els següents termes:

> *"a) el nivel de seguridad bajo se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;*
> *b) el nivel de seguridad sustancial se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;*
> *c) el* ***nivel de seguridad alto se referirá a un medio de identificación electrónica****, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos,* ***cuyo objetivo es evitar el uso indebido o alteración de la identidad."***

L'article 8, apartat 3, del mateix RUE 910/2014, disposa que:

> *"(...) la Comisión establecerá, mediante actos de ejecución, las especificaciones técnicas mínimas, las normas y los procedimientos con referencia a los cuales se especificarán los niveles de seguridad bajo, sustancial y alto de los medios de identificación electrónica a efectos del apartado 1.*
>
> *Estas especificaciones técnicas mínimas, normas y procedimientos se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:*
>
> *a) el procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica;*
>
> *b) el procedimiento para expedir los medios de identificación electrónica solicitados;*
>
> *c) el mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria;*
>
> *d) la entidad que expide los medios de identificación electrónica;*
>
> *e) cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica, y*
>
> *f) las especificaciones técnicas y de seguridad de los medios de identificación electrónica.*

(...)."

L'article 9.2 del mateix RUE 910/2014, disposa que: *"Un año después de la fecha de aplicación de los actos de ejecución a que hacen referencia el artículo 8, apartado 3, y el artículo 12, apartado 8, la Comisión publicará en el Diario Oficial de la Unión Europea la lista de los sistemas de identificación electrónica notificados de conformidad con el apartado 1 del presente artículo y la información básica al respecto."*

En desenvolupament d'aquesta norma, s'ha dictat el Reglament d'execució (UE) 2015/1502 de la Comissió, de 8 de setembre de 2015, sobre la fixació d'especificacions i procediments tècnics mínims per als nivells de seguretat de mitjans d'identificació electrònica d'acord amb el que disposa l'article 8.3 del RUE 910/2014. Segons el Considerant 8 del dit Reglament d'execució: *"Los requisitos de prueba y verificación de la identidad deben tener en cuenta los distintos sistemas y prácticas, y garantizar al mismo tiempo una seguridad suficientemente alta con el fin de establecer la confianza necesaria. (...)".*

En qualsevol cas, sens perjudici de les previsions del Reglament d'execució esmentat (en concret, del seu annex, que detalla especificacions sobre els diferents apartats de l'article 8.3 del RUE 910/2014, citat), des de la perspectiva de la protecció de dades de caràcter personal cal fer avinent que les dades de salut requereixen una especial protecció i, en conseqüència, han de protegir-se amb mesures que podem qualificar com de "nivell alt" (tenint en compte els nivells de seguretat establerts en la normativa de protecció de dades –art. 81 i Títol VIII del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD (RLOPD)-, i en base a les previsions sobre mesures de seguretat aplicables que puguin derivar-se del RGPD, en relació amb dades especialment protegides, específicament, dades de salut).

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).

A això cal afegir que l'Ordre GRI/233/2015, de 20 de juliol, per la qual s'aprova el Protocol d'identificació i signatura electrònica (en endavant, Ordre PISE), recull les disposicions del RUE 910/2014, citat, i estableix que els mecanismes d'identificació i signatura electrònica per acreditar la identitat dels usuaris per mitjans electrònics **es determinen en funció del subjecte i el grau de seguretat del tràmit corresponent** (art. 6 Ordre PISE).

En concret, l'article 6.1.1 de l'Ordre PISE, inclou, com a mecanisme d'identificació per a persones físiques, el *"mecanisme idCAT-SMS, que és un mecanisme d'identificació i signatura electrònica dels ciutadans (persones físiques) no criptogràfic, basat en l'enviament de codis d'un sol ús a dispositius mòbils, gestionat pel Consorci AOC."*

En relació amb l'admissió de mecanismes d'identificació electrònica, l'article 7.1 de l'Ordre PISE, citada, estableix el següent:

> *"**Amb caràcter general**, els ciutadans i ciutadanes es poden identificar electrònicament davant de l'Administració de la Generalitat de Catalunya emprant qualsevol sistema d'identificació que compti amb un registre previ com a usuari que permeti garantir la seva identitat.*

L'admissió dels mecanismes d'identificació i signatura electrònica es du a terme conforme als nivells de seguretat requerits en ***l'Esquema Nacional de Seguretat.***

(...)

Quan en el context d'un servei electrònic de l'Administració de la Generalitat calgui ***garantir la protecció de la confidencialitat*** *de les dades implicades mitjançant mecanismes d'identificació electrònica, s'admetran els sistemes següents:*

7.1.1 ***Per als tràmits classificats amb categoria alta***

S'admeten els sistemes d'identificació electrònica de ***nivell de seguretat alt, que són els que fan un registre dels usuaris presencial i fiable*** *i proveeixen els usuaris d'un mitjà d'identificació electrònica de doble factor.*

S'admeten amb caràcter obligatori:

- Els certificats reconeguts o qualificats que s'emetin en un dispositiu qualificat de creació de signatura electrònica, d'entre els establerts en el punt 6 d'aquest Protocol, atenent a les tipologies de certificats i del col·lectiu específic.
- Qualsevol dels mitjans d'identificació que hagi estat classificat amb nivell de seguretat alt i s'inclogui en la llista que, conforme al que estableix el ReIDAS en el capítol 2, ***publicarà la Comissió Europea*** *per accedir als serveis prestats en línia per un organisme del sector públic en un estat membre, a l'efecte de l'autenticació transfronterera."*

Pel que fa a la referència a l'Esquema Nacional de Seguretat (art. 7.1 Ordre PISE), el Reial decret 3/2010, de 8 de gener, que regula l'ENS en l'àmbit de l'Administració electrònica, remet als nivells baix, substancial i alt del RUE 910/2014, citat.

Dit això, l'article 7.1.1 de l'Ordre PISE només admet, com a sistemes d'identificació electrònica per a tràmits de categoria alta, sistemes d'identificació electrònica basats en un registre presencial o sistemes que utilitzen certificats electrònics reconeguts, o un sistema equivalent.

Així, l'Acord de Govern GOV/92/2015, citat, preveu que: "*El sistema idCAT-SMS* ***té la consideració de nivell mitjà de seguretat****,* ***a l'efecte de la seva utilització amb caràcter obligatori*** *per a la realització de tràmits o l'accés a serveis que tinguin establert aquest nivell de seguretat."*

Tenint en compte aquestes previsions, el tràmit de registre inicial per accedir a la informació personal de *"La meva Salut"*, atesa la informació que es tracta (la història clínica del pacient), seria un tràmit de *"categoria alta"* (en els termes de l'article 7.1.1 Ordre PISE), i per això hauria de dur-se a terme necessàriament de forma *"presencial"*, o bé dur-se a terme amb certificats electrònics reconeguts (en definitiva, a través de les dues vies per les que es duu a terme el tràmit en el moment d'emetre aquest dictamen, segons la informació disponible).

En conseqüència, vista la normativa estudiada, des de la perspectiva de la protecció de dades, pel que fa a l'accés al portal i serveis de *"CatSalut – La meva Salut",* caldria descartar la possibilitat del registre en línia, amb identificació basada en l'aportació d'informació coneguda per la persona interessada i l'Administració (art. 4.2.c) Ordre PRE/226/2014). Per tant, les persones usuàries s'haurien de registrar en el portal *"CatSalut - La meva Salut",* de forma presencial (art. 4.2.a) Ordre PRE/226/2016) o bé utilitzant certificats electrònics reconeguts (art. 4.2.b) Ordre PRE/226/2014).

En definitiva, el sistema idCAT Mòbil, o un sistema equivalent, pot ser admès com a mecanisme d'identificació de les persones usuàries del servei *"CatSalut - La meva*

Salut", sempre que el tràmit de registre inicial es dugui a terme de forma presencial (art. 4.2.a) Ordre PRE/226/2014) o a través de certificats electrònics reconeguts (art. 4.2.b) Ordre PRE/226/2014).

Des de la perspectiva de la protecció de dades no hi hauria inconvenient, un cop completat el registre inicial de les persones usuàries del servei en els termes indicats, en articular els successius accessos al portal *"CatSalut - La meva Salut",* i a la informació personal que s'hi conté, a través de mecanismes en línia, com el sistema idCAT Mòbil o equivalent, que no requereixin certificats electrònics reconeguts.

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

Des de la perspectiva de la protecció de dades, atesa la normativa estudiada, i la informació personal objecte de tractament (art. 7.3 LOPD i art. 9 RGPD), pel que fa a l'accés al portal i serveis de *"CatSalut – La meva Salut",* caldria descartar la possibilitat del registre en línia, amb identificació basada en l'aportació d'informació coneguda per la persona interessada i l'Administració (art. 4.2.c) Ordre PRE/226/2014). Per tant, les persones usuàries s'haurien de registrar en el portal *"CatSalut - La meva Salut",* de forma presencial (art. 4.2.a) Ordre PRE/226/2016) o bé utilitzant certificats electrònics reconeguts (art. 4.2.b) Ordre PRE/226/2014).

Des de la perspectiva de la protecció de dades no hi hauria inconvenient, un cop completat el registre inicial de les persones usuàries del servei en els termes indicats, en articular els successius accessos al portal *"CatSalut - La meva Salut",* i a la informació personal que s'hi conté, a través de mecanismes en línia (sistema idCAT Mòbil o equivalent), que no requereixin certificats electrònics reconeguts.

Barcelona, 2 de febrer de 2017