

**Dictamen en relació amb una consulta sobre diverses qüestions relacionades amb una aplicació informàtica d'entrada massiva de documents a un organisme tributari**

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit en el qual es demana que l'Autoritat emeti un dictamen sobre diverses qüestions relacionades amb una aplicació informàtica d'entrada massiva de documents a un organisme tributari (en endavant, l'organisme), des del punt de vista de la legislació sobre protecció de dades.

En concret, es plantegen dos aspectes clarament diferenciats:

1.- Adequació de la informació tributària que ha de rebre l'organisme als fitxers actualment existents de dades de caràcter personal.

2.- Adequació a la normativa sobre protecció de dades del sistema d'identificació i autenticació per relacionar-se electrònicament amb la Generalitat basat en la informació coneguda per ambdues parts. En concret es proposa un sistema basat en el NIF i el codi d'identificació personal de la targeta d'identificació sanitària (CIP-TIS) expedida per CatSalut.

Analitzada la consulta, que s'acompanya d'un informe de l'Assessoria Jurídica de l'organisme, i vist l'informe de l'Assessoria Jurídica emeto el següent dictamen:

I

(...)

II

Pel que fa a la primera qüestió plantejada, això és, l'adequació de la informació tributària que ha de rebre l'organisme als fitxers actualment existents de dades de caràcter personal, en la consulta s'exposa que s'està construint una aplicació informàtica –a la qual s'anomena “gestor d'entrades”- que ha de permetre recollir dos tipus d'informació:

- Declaracions de l'IRPF destinades per a ser utilitzades en la tramitació d'un determinat procediment de contractació administrativa o de concessió d'ajuts o subvencions. En aquest cas, es manifesta que l'organisme es limitarà a trametre les declaracions al departament al qual van adreçades, sense que es faci cap incorporació immediata de dades als sistemes d'informació de l'organisme, i sense perjudici que aquest organisme, posteriorment, en demani la cessió, a l'empara de l'article 94 de la Llei general tributaria.

- Dades fiscals vinculades a l'IRPF lliurades voluntàriament pels contribuents. Aquelles dades que puguin ser d'utilitat per a la gestió tributària que sigui competència de l'organisme (és a dir, la referida als anomenats tributs propis i totalment cedits) seran incorporades al seu sistema d'informació i degudament estructurades i tractades, a través dels fitxers regulats a (...) (fitxers "Gestió i recaptació tributària" i fitxer "Recaptació"). Segons es manifesta a la consulta, la informació es destinarà a tasques de:

- Gestió i liquidació tributària en relació als tributs estatals cedits i propis de la Generalitat de Catalunya.
- Recaptació de deutes en període voluntari o executiu.

Ara bé, en la consulta es manifesta que l'organisme "*haurà de dissociar aquelles dades subministrades pel contribuent que poden ser objecte de tractament per l'organisme d'aquelles altres que, per no ser útils ni necessàries per a l'exercici de les seves competències, no serien incorporades al fitxer*".

Atesa la dificultat de demanar als ciutadans que facin aquesta dissociació o separació en la consulta s'apunta a la creació d'un nou fitxer de nova creació al qual es destinarien les dades "*no útils*".

El que consulta el departament és, en concret, si les dades fiscals lliurades es poden escindir en dos fitxers diferents. I en el cas que això sigui possible, quin és el tractament que cal donar a les dades que no es puguin incorporar als fitxers existents fins que no se'n creï un de nou.

Cal dir però que els termes en què es formula la consulta resulten força ambigus. No queda clar a quins tipus d'informació s'està referint, ni la finalitat de la seva recollida, més enllà de les finalitats pròpies de gestió tributària que en cada moment tingui encomanades l'organisme. Per això, les consideracions jurídiques que es faran en aquest informe s'han d'entendre fetes també en termes generals i sens perjudici que, a la vista de la concreta informació que es reculli o de les finalitats amb que es faci, s'hagi de matisar o corregir algunes de les consideracions que s'hi contenen.

### III

Abans d'entrar però a donar resposta a aquesta pregunta formulada per l'organisme, cal fer un breu esment a la possibilitat de dur a terme el tractament consistent en Declaracions de l'IRPF destinades als Departaments de la Generalitat per a ser utilitzades en la tramitació d'un determinat procediment de contractació administrativa o de concessió d'ajuts o subvencions. En aquest cas, es manifesta que l'organisme es limitarà a trametre les declaracions al departament al qual van adreçades, sense que es faci cap incorporació immediata de dades als sistemes d'informació de l'organisme, i sense perjudici que aquest organisme, posteriorment, en demani la cessió, a l'empara de l'article 94 de la Llei general tributària.

Aquesta previsió, cal posar-la en relació amb el que estableix l'article 133 de la Llei 2/2014, del 27 de gener, de mesures fiscals, administratives, financeres i del sector públic.

*“Article 133. Aportació o lliurament de declaracions tributàries als òrgans de l’Administració de la Generalitat per al compliment de llurs funcions*

*1. Els òrgans de l’Administració de la Generalitat poden sol·licitar el lliurament o exigir l’aportació de declaracions tributàries si el coneixement de les dades declarades és necessari per al desenvolupament de les funcions que tenen atribuïdes. El lliurament o l’aportació de les declaracions tributàries es pot efectuar pels mitjans electrònics posats a disposició dels contribuents per l’Agència Tributària de Catalunya.*

*2. La informació amb transcendència tributària continguda en les declaracions aportades o lliurades en virtut del que estableix l’apartat 1 i en les certificacions emeses amb els mateixos efectes per l’Administració tributària estatal pot ésser utilitzada per l’òrgan peticionari amb la finalitat per a la qual ha estat sol·licitada i s’ha d’incorporar a l’expedient administratiu corresponent. Així mateix, la informació tributària obtinguda pot ésser cedida a l’Agència Tributària de Catalunya, d’acord amb el que determina l’article 94 de la de la Llei general tributària, a l’efecte de la comprovació del compliment d’obligacions fiscals en l’àmbit de les seves competències.*

*3. El control i la seguretat de la informació continguda en les declaracions tributàries lliurades o aportades als òrgans de l’Administració de la Generalitat en virtut del que estableix l’apartat 1 es regeix pel que disposen la Llei general tributària i la normativa de protecció de dades de caràcter personal i de seguretat dels fitxers automatitzats que continguin dades de caràcter personal.”*

Des del punt de vista de la normativa de protecció de dades, cal apuntar que la funció esmentada, de possibilitar la presentació d’aquestes declaracions tributàries a través d’una aplicació facilitada per l’organisme, a la qual es refereix també l’apartat 1 de l’article 133, per la informació de què es disposa sobre l’abast del projecte, es podria dur a terme sense necessitat que l’organisme accedeixi ni tracti les dades personals que s’hi continguin. En aquest esquema l’organisme facilitaria l’aplicació informàtica, que seria emprada per cadascun dels organismes receptors d’aquesta documentació, sense intervenció de l’organisme.

Pel que es descriu a la consulta no sembla que sigui aquesta però, l’opció escollida, atès que sembla que l’organisme intervindrà en el procés de tramesa de les declaracions a l’organisme al qual van dirigides.

Per altra banda, en la consulta no s’especifica si aquestes declaracions les aportaran les persones interessades o si es tracta de declaracions de les quals ja disposa l’organisme. En aquest segon cas, la tramesa d’informació a l’organisme de que es tracti hauria de comptar amb el consentiment de la persona afectada –llevat que una llei n’habiliti la cessió directament-. Però no sembla que sigui aquest el supòsit contemplat a la consulta, atès que després s’indica que l’organisme després en podria demanar la cessió a l’organisme al qual anava dirigida.

Per tant, sembla que ens trobaríem davant del primer cas. Això és, ens trobaríem davant d’un supòsit en què l’organisme intervindria en el tractament de dades per compte d’un tercer (l’organisme al qual van dirigides). Es tractaria per tant d’un supòsit en què l’organisme actuaria

com a encarregat del tractament (arts. 3.g) i 12 del la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD)).

En aquest cas, caldria tenir en compte que, d'acord amb l'article 12 de la LOPD, s'hauria d'establir el corresponent acord d'encàrrec del tractament (ens remetem sobre això a la Recomanació 1/2010 sobre l'encarregat del tractament en la prestació de serveis per compte d'entitats del sector públic de Catalunya, disponible a <http://www.apd.cat> ) i que, entre d'altres mesures, l'encarregat del tractament –en aquest cas l'organisme- no pot utilitzar les dades per a una finalitat diferent a la que figuri en l'encàrrec (en principi, la tramesa de les declaracions a l'organisme destinatari). En el cas que ens ocupa, aquest encàrrec podria fer-se, per exemple, mitjançant un acord.

D'acord amb això, i tal com recull la conclusió segona de l'informe de l'Assessoria Jurídica que s'adjunta a la consulta, no seria procedent la incorporació en els fitxers propis de l'organisme de la informació recollida per aquesta via per a ser tramesa a l'òrgan davant el qual s'hagin d'aportat en procediments de contractació o d'atorgament de subvencions i ajuts.

L'apartat 2 de l'article 133 apunta en aquesta direcció quan indica que la informació s'ha d'incorporar a l'expedient administratiu corresponent, i això implica que l'organisme s'haurà d'abstenir de fer qualsevol altre tractament d'aquesta informació que no estigui adreçat a assolir aquesta finalitat.

Òbviament, l'organisme pot requerir per la via de l'article 94 de la LGT, i sense el consentiment de les persones afectades, ja sigui mitjançant disposicions de caràcter general o a través de requeriments concrets, les dades, informes i antecedents amb transcendència tributària en poder de les administracions públiques. De fet pot fer-ho no només respecte les informacions a que es refereix l'article 133 esmentat sinó també respecte qualsevol altra informació en poder de les administracions públiques que tingui rellevança tributària. Però per a prendre la decisió de requerir-la no pot basar-se en la informació de la qual hagi tingut coneixement com a encarregat del tractament en un tractament amb una finalitat diferent (art. 12.2 LOPD).

#### IV

Pel que fa a la primera pregunta plantejada, això és, si les dades fiscals lliurades es poden escindir en dos fitxers diferents -l en el cas que això sigui possible, quin és el tractament que cal donar a les dades que no es puguin incorporar als fitxers existents fins que no se'n creï un de nou- cal partir de la base que la informació a la qual ens referirem és només aquella que principi sigui susceptible d'incorporar-se als fitxers de l'organisme. Per tant en quedaria exclosa aquella informació, a la qual ens acabem de referir, de la qual l'organisme n'hagi tingut coneixement com a encarregat del tractament.

Respecte aquesta informació, que segons la consulta es tractaria de dades fiscals vinculades a l'IRPF lliurades voluntàriament pels contribuents, la consulta diferencia entre aquella informació que pugui ser d'utilitat per a la gestió tributària que sigui competència de l'organisme (és a dir, la referida als anomenats tributs propis i totalment cedits) i aquella altra informació que no pugui ser d'utilitat per a la finalitat de gestió tributària.

Així, mentre la primera seria incorporada al seu sistema d'informació a través dels fitxers que actualment té aprovats l'organisme -o si escau els que pugui aprovar per a l'exercici de les seves funcions- el segon tipus d'informació, és a dir les dades que segons la consulta es considerarien “no útils” s'inclouria en un altre fitxer –fins ara inexistent-.

D'acord amb la normativa de protecció de dades, les administracions públiques estan habilitades per a recollir i tractar la informació necessària per a l'exercici de les seves funcions (art. 6.2). Ara bé, només poden tractar les dades que siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'hagin obtingut (art. 4.1 LOPD).

Això, que forma part del que s'anomena el principi de qualitat de les dades en la seva vessant de proporcionalitat, comporta que no es pot recollir informació que no sigui necessària per a les funcions que té atribuïdes l'administració, en aquest cas l'organisme. I en el cas que es reculli, tan aviat com es constati que la informació no és necessària o pertinent per a la finalitat per la qual ha estat recollida, ha de ser cancel·lada (art. 4.5 LOPD).

En el cas que ens ocupa, si la informació recollida no resulta necessària per a l'exercici de les funcions de l'organisme caldria procedir a la seva cancel·lació.

D'acord amb l'article 5.1.b) del Reglament de desplegament de la LOPD (RLOPD), aprovat pel R. Decret 1720/2007, de 21 de desembre, la cancel·lació es defineix com:

*“Procediment en virtut del qual el responsable cessa en l'ús de les dades. La cancel·lació implica el bloqueig de les dades, consistent en la identificació i reserva d'aquestes dades amb la finalitat d'impedir-ne el tractament excepte per posar-les a disposició de les administracions públiques, jutges i tribunals, per a l'atenció de les possibles responsabilitats nascudes del tractament i només durant el termini de prescripció de les responsabilitats esmentades. Transcorregut aquest termini s'ha de procedir a la supressió de les dades.”*

El que no procediria en cap cas és incorporar aquesta informació en un fitxer per a informació “no útil”, atès que no queda clara quina seria la finalitat d'aquest fitxer. Si es tracta d'informació que no pot ser útil als efectes de la gestió tributària o de les altres funcions que tingui encomanades l'organisme no sembla que es pugui justificar la legitimitat de la conservació d'aquesta informació.

En la consulta s'apunta a que no és factible demanar al contribuent que separi la informació útil d'aquella que no ho sigui. Si bé és cert que pot resultar difícil que el ciutadà faci amb absoluta precisió aquesta separació de la informació, sí que es pot facilitar aquesta tasca a través de diferents mesures com ara si el mateix organisme identifica prèviament el tipus d'informació que vol recollir o facilita formularis per a trametre-la. Si, fins i tot així, es segueix recollint informació que no resulta necessària per a la gestió tributària, caldrà procedir a un cribatge i a la cancel·lació d'aquella que no ho sigui.

## V

Pel que fa a la segona qüestió, això és, l'adequació de la normativa sobre protecció de dades del sistema d'identificació i autenticació per relacionar-se electrònicament amb l'organisme basat en el NIF i el codi d'identificació personal de la targeta d'identificació sanitària (CIP-TIS) expedida per Cat Salut, cal tenir en compte el següent.

D'entrada, i tal com s'apunta en la conclusió núm. 6 de l'informe de l'Assessoria Jurídica que s'acompanya a la consulta, atès que no sembla que per les competències que té atribuïdes, l'organisme disposi del número de la Targeta d'Identificació Sanitària, caldria comptar amb el consentiment de la persona afectada per a que l'organisme pugui tenir accés a aquesta identificació establerta en principi només per a l'accés als serveis de salut. A manca d'aquest consentiment, com s'apunta a la consulta, caldria que el ciutadà pogués optar per un altre sistema d'identificació.

Ara bé, més enllà d'això, i més enllà també de la problemàtica que es podria derivar del fet que no tots els ciutadans disposen de la targeta d'identificació sanitària, la utilització d'un sistema d'identificació i autenticació basat en el NIF més el número de la TIS planteja seriosos problemes des del punt de vista de la seguretat de la informació.

La consulta es refereix a què aquest sistema s'emprarà per tal que els ciutadans puguin relacionar-se amb l'organisme. Tot i que no s'aclareixi a la consulta, s'entén que es refereix tant a la possibilitat de presentar documents com a la possibilitat d'accedir a informació personal en poder de l'organisme a la qual, d'acord amb la legislació vigent, cada ciutadà pugui tenir accés.

S'ha de garantir, des de la vessant del dret a la protecció de dades personals, que terceres persones alienes a aquest entorn no puguin accedir fàcilment a aquesta informació. En aquest sentit, la normativa de protecció de dades personals imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

Aquestes mesures de seguretat venen regulades en el Títol VIII del RLOPD, que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar. Cal tenir en compte, que aquestes mesures tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

En el cas examinat, i d'acord amb la tipologia de dades personals que sembla ser que serien tractades (dades identificatives, de característiques personals i altres dades de l'administració tributària relacionades amb l'exercici de les seves potestats), les mesures de seguretat a implementar corresponen a les de nivell mitjà (article 81.2.c) RLOPD) i, en concret, tenint en compte que el seu tractament s'efectuarà de manera automatitzada, correspondrà aplicar les mesures descrites en els articles 89 a 100 del RLOPD i, especialment, pel que ara ens interessa, les relatives a l'establiment d'un control d'accés (article 91) i a l'adopció de mecanismes que permetin la correcta identificació i autenticació dels usuaris (article 93 RLOPD) (entenen com a "autenticació" el procediment de comprovació de la identitat de l'usuari (art.

5.2.b) i com a “usuaris” els subjectes i processos autoritzats per accedir a dades o recursos (art. 5.2.p)), complementat amb l'article 98 per a les mesures de nivell mitjà:

**Article 89. Funcions i obligacions del personal**

*1. Les funcions i obligacions de cadascun dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació han d'estar clarament definides i documentades en el document de seguretat.*

*També s'han de definir les funcions de control o autoritzacions delegades pel responsable del fitxer o tractament.*

**Article 91. Control d'accés**

*1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.*

*2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.*

*3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.*

*4. Exclusivament el personal autoritzat per fer-ho en el document de seguretat pot concedir, alterar o anul·lar l'accés autoritzat sobre els recursos, de conformitat amb els criteris que estableix el responsable del fitxer.*

*5. En cas que existeixi personal aliè al responsable del fitxer que tingui accés als recursos, ha d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.*

**Article 93. Identificació i autenticació**

*1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.*

*2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.*

*3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.*

*4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma intel·ligible.*

**Secció segona. Mesures de seguretat de nivell mitjà**

**Article 98. Identificació i autenticació**

*El responsable del fitxer o tractament ha d'establir un mecanisme que limiti la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.*

La normativa de protecció de dades però, no estableix un sistema concret d'identificació i autenticació, sinó que poden ser admissibles diferents sistemes, sempre que es compleixin determinats requisits.

Per altra banda, s'ha de fer referència a la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP), que reconeix el dret dels ciutadans a relacionar-se amb les administracions públiques per mitjans electrònics (art. 1) i que té com una de les seves finalitats facilitar l'accés per mitjans electrònics dels ciutadans a la informació i al procediment administratiu (art. 3.2).

En concret, l'article 13 de la LAECSP que regula els requisits d'identificació i d'autenticació dels ciutadans en les seves relacions amb l'administració pública per mitjans electrònics que després es desenvolupen als articles 14 a 16, permet la utilització (apartat 2):

- “a) En tot cas, dels sistemes de signatura electrònica incorporats al document nacional d'identitat, per a persones físiques.*
- b) De sistemes de signatura electrònica avançada, inclosos els basats en un certificat electrònic reconegut, admesos per les administracions públiques.*
- c) D'altres sistemes de signatura electrònica, com la utilització de claus concertades en un registre previ com a usuari, l'aportació d'informació coneguda per les dues parts o altres sistemes no criptogràfics, en els termes i les condicions que es determinin en cada cas.”*

Així doncs la mateixa LAECSP (art. 13.2.c) i art. 16) permet, quan es justifiqui tenint en compte les dades i els interessos afectats, la utilització d'altres sistemes de signatura electrònica diferents al DNI electrònic o la signatura electrònica avançada, com ara els basats en claus d'accés o alguna informació coneguda per ambdues parts i que ofereixi suficients garanties de confidencialitat.

En aquest punt, convé assenyalar que tot i que la consulta es refereix a l'article 15 del Decret 324/2001, de 4 de desembre, relatiu a les relacions entre els ciutadans i l'Administració de la Generalitat de Catalunya a través d'internet, aquesta disposició va ser derogada per la Disposició Derogatòria del Decret 56/2009, de 7 d'abril, per a l'impuls i el desenvolupament dels mitjans electrònics a l'Administració de la Generalitat.

D'acord amb el que s'ha exposat, el mecanisme d'identificació i autenticació haurà de garantir:

- a) La correcta identificació i autenticació dels usuaris que accedeixen a les dades de caràcter personal. És a dir, que en l'accés no es produeixin suplantacions, ja siguin intencionades o accidentals.
- b) La confidencialitat de la contrasenya (en aquest cas el CIP-TIS). El procediment d'assignació i emmagatzematge de les contrasenyes ha de garantir la seva confidencialitat, és a dir, que en qualsevol circumstància la contrasenya només pot ser coneguda per l'usuari.
- c) El canvi periòdic de la contrasenya.
- d) La utilització de mecanismes que evitin intents reiterats d'accessos no autoritzats.

Pel que fa a la utilització del NIF com a usuari, la Disposició adicional sisena de la Llei 58/2003, de 17 de desembre, General Tributària (Llei 58/2003) estableix que els obligats tributaris han d'incloure el seu NIF en totes les autoliquidacions, declaracions, comunicacions o escrits que presentin davant l'Administració Tributària.



Segons l'article 18.1 del Reial decret 1065/2007, de 27 de juliol, que aprova el Reglament general de les actuacions i dels procediments de gestió i inspecció tributària i de desenvolupament de les normes comunes dels procediments d'aplicació dels tributs (RD 1065/2007), les persones físiques i jurídiques, així com els obligats tributaris a què es refereix l'article 35.4 de la Llei 58/2003, tindran un NIF per a les seves relacions de naturalesa o amb transcendència tributària.

L'apartat 2 d'aquest mateix precepte disposa que el NIF podrà acreditar-se pel seu titular mitjançant l'exhibició del document expedit per a la seva constància per l'Administració Tributària, del document nacional d'identitat (DNI) o del document oficial en què s'assigni el número personal d'identificació d'estranger (NIE).

D'acord amb aquests preceptes, en la mesura que el NIF permet acreditar la identitat inequívoca del ciutadà davant l'administració pública tributària, es considera que tot i que cal tenir en compte que és una dada que pot ser coneguda per tercers –i per tant oferiria majors garanties de seguretat u usuari que no pogués ser conegut per tercers-, la seva utilització com a usuari no es pot descartar, sempre que a l'hora d'establir i gestionar la contrasenya s'estableixin les garanties adequades, atès que és la contrasenya la que, en major mesura, permetrà garantir la confidencialitat. Això és, que sigui coneguda exclusivament per la persona a la qual li ha estat assignada.

En el supòsit plantejat, en que el CIP-TIS fa les funcions de contrasenya, ja que és el que permet, en combinació amb el NIF, establir la relació electrònica entre ciutadà i l'organisme, aquest requisit de confidencialitat no es compleix.

L'estructura del CIP-TIS permet conèixer amb esforços gens desproporcionats quin codi li correspon a una persona concreta, ja que aquest codi es forma en base a certes dades de caràcter personal que poden ser fàcilment conegudes per terceres persones, de manera que podrien arribar a construir-lo i utilitzar-lo, en combinació amb el NIF, per suplantar algú o per accedir a la informació.

Concretament el CIP de la TIS està compostat per 14 posicions, que poden ser lletres (en majúscules) o números, i es genera de la següent manera (d'esquerra a dreta):

- a) Les primeres 4 posicions corresponen a les 2 primeres lletres de cada cognom. En el cas de "MORENO GARCIA " seria «MOGA».
- b) La posició 5 indica el sexe: «0» home i «1» dona. Per tant, seguint l'exemple, si es tractés d'un home seria «MOGA 0»
- c) Les posicions 6 a 11 (és a dir 6 caràcters) són la data de naixement en format any, mes, dia, utilitzant 2 posicions per a cada part de la data. Per exemple la data de 6 d'abril de 1958 seria «580406», per tant «MOGA 0 580406».
- d) Les 2 següents posicions (12 i 13) s'utilitzen pel cas de que es donin coincidències de codi (el mateix codi) per a diferents persones en la primera part del CIP, començant per «00» per a la primera persona que se li assigna, «01» a la segona i així successivament.

e) L'últim caràcter (14), és un codi de control, calculat a partir de les 13 primeres posicions, a fi d'evitar possibles errades de transcripció.

A la vista d'això, només el 3 darrers codis tenen un cert element "d'aleatorietat", mínima per al 12 i 13, i entre el 0 i el 9 per a la posició 14. Per tant, d'una manera molt simple, es podria conèixer el CIP d'una persona, i per tant utilitzar-lo en combinació amb el seu NIF.

D'altra banda, en un supòsit com el plantejat, tot i que les contrasenyes es guardessin de forma segura, cal tenir en compte que hi hauria diverses entitats (per exemple el Departament de Salut i altres entitats que intervinguin en la prestació de serveis sanitaris), que disposarien dels usuaris i les contrasenyes de tots els ciutadans de Catalunya que els permetrien accedir al sistema d'informació de l'organisme.

Per això, un sistema d'identificació i autenticació basat en la combinació del NIF amb el CIP-TIS no sembla que ofereixi suficients garanties per a la seguretat de la informació.

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada en relació amb diverses qüestions relacionades amb una aplicació informàtica d'entrada massiva de documents a un organisme tributari, es fan les següents,

## **Conclusions**

Pel que fa a la primera qüestió plantejada, això és, el tractament de la informació que rebí l'organisme i que no sigui necessària per a l'exercici de les seves funcions, cal concloure que procedeix la seva cancel·lació d'acord amb el que estableix l'article 4.5 de la LOPD.

Pel que fa a l'adequació a la normativa sobre protecció de dades del sistema d'identificació i autenticació per relacionar-se electrònicament amb un organisme tributari basat en el NIF i el codi d'identificació personal de la targeta d'identificació sanitària (CIP-TIS) expedida per CatSalut, no ofereix garanties suficients per a la seguretat de la informació.

Barcelona, 11 de abril de 2014