

# ASPECTES JURÍDICS I TÈCNICS DE LA CERTIFICACIÓ DIGITAL EN RELACIÓ AMB LA SEU ELECTRÒNICA

Carles Alonso Espinosa<sup>1</sup>

## 1. Introducció

La seu electrònica és una de les novetats més importants de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (en endavant, LAECSP). En aquest document analitzem les condicions jurídiques i tecnològiques relatives al certificat digital de seu electrònica, amb l'objecte d'esclarir el seu ús en relació a les seus electròniques i d'altres instruments de difusió d'informació administrativa.

Intentarem delimitar el concepte jurídic de seu electrònica i les condicions necessàries per assegurar l'efectivitat de la funció de la certificació digital, que no és altra que la d'assegurar les condicions de confiança per als receptors de la informació allotjada i el compliment legal de les condicions jurídiques que les normes imposen a les seus electròniques.

Com a punt de partida, analitzarem breument el concepte de seu electrònica per distingir-lo d'altres instruments d'informació al públic. A continuació farem un petit recorregut per les normes tècniques aplicables, així com les dimensions organitzatives i de validesa jurídica d'aquestes normes, provinquin d'organitzacions de normalització tècnica o d'altres organitzacions. Tanmateix veurem el context en què sorgeixen les normes tècniques i en quina mesura condicionen les característiques dels certificats digitals, tot analitzant les possibilitats d'actuació de l'Administració en aquest àmbit.

Finalment, mirarem d'analitzar el marc jurídic que condiciona l'ús dels certificats de seu electrònica, conformat per normes aprovades recentment i les activitats administratives de supervisió dels prestadors de serveis de certificació. Un cop reunides totes aquestes dades analitzarem qüestions de present i futur que poden sorgir en l'ús de certificats digitals en les seus electròniques i les implicacions de totes aquestes qüestions en el disseny dels serveis de certificació digital.

## 2. La seu electrònica com a instrument legal per a l'exercici de potestats administratives

### 2.1. El caràcter limitat del concepte de la seu electrònica en virtut de la distribució competencial

El concepte de seu electrònica apareix arrel del debat previ a l'aprovació de la LAECSP, quan es discutia sobre una futura "Llei d'Administració Electrònica". Els primers debats al respecte tenen lloc no en seu parlamentària sinó en una discussió prèvia. En efecte, el concepte és fruit de la taula rodona sobre "Aspectos legales en la construcción de la Administración Electrónica: el camino hacia una Ley de Administración electrónica", celebrada en las IX Jornadas sobre Tecnologías de la Información para la Modernización de las

---

<sup>1</sup> Carles Alonso Espinosa. Tècnic de Regulació i Procediments. CATCert, Agència Catalana de Certificació.

Administraciones Públicas Tecnimap 2006 (Tecnimap és un fòrum de debat i trobada de responsables i alts funcionaris en matèria tecnològica i administrativa).<sup>2</sup>

El primer esborrany de l'avantprojecte de la Llei (anomenat 'esborrany d'avant-projecte de Llei d'Administració electrònica') ja esmentava el concepte de seu electrònica, de forma quasi idèntica al que fou recollit finalment a la llei. Aquest és el contingut final de la LAECSP (les diferències del text final amb l'esborrany són de matís):

“Article 10. La seu electrònica.

1. La seu electrònica és aquella adreça electrònica disponible per als ciutadans a través de xarxes de telecomunicacions la titularitat, gestió i administració de la qual correspon a una administració pública, òrgan o entitat administrativa en l'exercici de les seves competències.
2. L'establiment d'una seu electrònica comporta la responsabilitat del titular respecte de la integritat, veracitat i actualització de la informació i els serveis a què es pugui accedir a través d'aquesta.
3. Cada administració pública ha de determinar les condicions i instruments de creació de les seues electròniques, amb subjecció als principis de publicitat oficial, responsabilitat, qualitat, seguretat, disponibilitat, accessibilitat, neutralitat i interoperabilitat. En tot cas s'ha de garantir la identificació del titular de la seu, així com els mitjans disponibles per a la formulació de suggeriments i queixes.
4. Les seues electròniques han de disposar de sistemes que permetin l'establiment de comunicacions segures sempre que siguin necessàries
5. La publicació en les seues electròniques d'informacions, serveis i transaccions respectarà els principis d'accessibilitat i usabilitat d'acord amb les normes establertes al respecte, estàndards oberts i, en el seu cas, aquells altres que siguin d'ús generalitzat pels ciutadans”.

Per entendre bé aquest text hem de tenir en compte el context normatiu en què es situa. En primer lloc, cal tenir en compte que es tracta d'una norma de caràcter estatal i que, per tant, es troba limitada per la distribució competencial establerta a la constitució i al bloc de constitucionalitat. Doncs bé, d'acord amb l'article 148.1.18, l'Estat té competència per dictar les bases del règim d'actuació administrativa. Correspon, per tant, a les Comunitats Autònomes desenvolupar la normativa bàsica de l'Estat, completant les particularitats de règim jurídic i de procediment, si escau, ja sigui en la normativa sectorial o en una norma administrativa de caràcter general com és el cas de la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.

Cal entendre que el títol competencial de l'Estat està limitat a determinar els efectes de les actuacions administratives en relació al seu règim jurídic, és a dir, la facultat de determinar, per llei o per norma reglamentària, segons el cas, les conseqüències jurídiques d'una determinada actuació, el règim de procediment (recursos, efectes dels diferents tràmits, ...), i el règim bàsic de la responsabilitat administrativa. Pel que a nosaltres ens afecta, la LAECSP estableix el règim de publicitat oficial de la seu electrònica i en delimita els principis generals així com les mesures de protecció mitjançant 'certificats de dispositiu segur' (article 17) que poden ser de nivell mig o nivell alt, depenent del tipus de danys que podria causar una

---

<sup>2</sup> LINARES GIL, Maximino. “Identificación y autenticación de las administraciones públicas”, en GAMERO CASADO, Eduardo; VALERO TORRIJOS, Julián (Coords.) *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Cizur Menor: Thomson Aranzadi. 2008, p. 296.

disfunció, d'acord amb les categories establertes a l'Esquema Nacional de Seguretat (Reial Decret 4/2010, de 8 de gener), que desenvolupa la llei.

Un cop que la normativa estatal ha determinat el valor legal de l'acte de publicar un determinat contingut a la seu electrònica, d'altres normes (autonòmiques, d'àmbit local o sectorials) poden establir els supòsits en què s'ha de realitzar l'esmentada publicació (vegeu apartat 2.4) o bé, adaptar les característiques de la seu electrònica a la pròpia organització o a les seves pròpies polítiques de comunicació. Una de les possibilitats a l'hora de desenvolupar les normes sobre seu electrònica seria, per exemple, determinar el tractament de la seu electrònica en relació als instruments d'informació administrativa.<sup>3</sup>

Un altre dels àmbits en què es pot dur a terme el desenvolupament de la LAECSP és en la determinació del contingut de la seu electrònica. En el cas de Catalunya, per exemple, el Decret d'Impuls, en l'àmbit de la generalitat de Catalunya, estableix l'obligació de publicar determinats actes a la seu electrònica de l'Administració de la Generalitat i així mateix en delimita les característiques i les qüestions organitzatives;<sup>4</sup> i aquestes possibilitat també és oberta a les ordenances locals en l'àmbit de l'administració electrònica.

Aquest és un exemple prou clar de com funciona, en relació amb la seu electrònica, la distribució de competències, però cal tenir present que l'evolució previsible és que incrementin les crides de la normativa sectorial a la publicació d'actes a la seu electrònica. En aquest punt entren en joc les competències autorganitzatives i de desenvolupament de la legislació bàsica estatal de les CCAA i els poders locals per tal de determinar els continguts de la seu electrònica.

## 2.2. El funció de la seu electrònica com a mecanisme auxiliar a la tramitació administrativa

Al llarg de la història, l'Administració s'ha assegurat mitjans complementaris per divulgar les normes i els actes administratius, a través d'anuncis en diaris de major difusió o mitjançant l'edició de documents divulgatius o inclòs mitjançant tècniques legislatives (el codi napoleònic per exemple, compleix aquesta funció). Aquest és l'origen, de fet, dels butlletins provincials que, en un primer moment tenien per objectiu informar els funcionaris destacats a les províncies sobre les normes aprovades a la capital i després es van anar incorporant com a mecanisme per dotar d'eficàcia a les normes i actuacions produïdes per les institucions d'àmbit municipal.<sup>5</sup> Les webs administratives també han evolucionat d'aquesta forma, fins l'aprovació de la LAECSP constituïen un mitjà complementari de difusió d'informació administrativa general o particular que, tot i no tenir caràcter oficial, tenia per objectiu donar més accessibilitat i més

<sup>3</sup> Així doncs, es pot segregar la seu del portal com en el cas de l'Ajuntament de Barcelona (la seu [bcn.cat/tramits](http://bcn.cat/tramits) s'integra en el portal general, que seria [bcn.cat](http://bcn.cat)) o bé pot deixar-se aquesta decisió en mans dels gestors com en el cas de la generalitat de Catalunya que simplement ordena que la seu electrònica estigui 'ubicada' al portal institucional [www.gencat.cat](http://www.gencat.cat). Cfr. Ordenança de l'Ajuntament de Barcelona, de 30 de gener de 2009, Reguladora de l'Administració Electrònica (en endavant ORAE) i *Decret 56/2009*, de 7 d'abril, per a l'impuls i el desenvolupament dels mitjans electrònics a l'Administració de la *Generalitat (en endavant Decret d'Impuls)*.

<sup>4</sup> D'acord amb l'art. 23, la Direcció General d'Atenció Ciutadana en determina els estàndards, normes, especificacions, i guies d'estils i posa a disposició la infraestructura tècnica necessària a través del Centre de Telecomunicacions i Tecnologies de la Informació.

<sup>5</sup> LORENTE SARIÑENA, Marta. *La voz del Estado. La publicación de las normas (1810-1889)*. Madrid: Boletín Oficial del Estado, Centro de Estudios Políticos y Constitucionales. 2001.

*legibilitat* a la informació relativa a les activitats administratives,<sup>6</sup> tal i com es desprèn del ja derogat Decret d'Impuls dels mitjans electrònics a l'administració de la Generalitat de Catalunya.<sup>7</sup>

Amb la consolidació de les noves tecnologies, calia esclarir el règim jurídic de determinades actuacions com la difusió d'informació a través de les noves tecnologies. Així doncs, l'operació de la LAECSP consistia en equiparar la informació difosa per Internet amb la informació dels diaris oficials en format paper, per dotar de les màximes garanties al ciutadà en les seves relacions amb l'Administració (i la publicació és la principal d'aquestes garanties).

L'eficàcia d'una norma o acte administratiu i la seva capacitat de produir efectes en l'esfera dels drets dels ciutadans ve determinada per la seva notificació o la seva publicació i aquesta eficàcia és el que permet l'executivitat de l'acte administratiu perquè es presumeix el coneixement de l'acte per part del destinatari.<sup>8</sup> D'aquesta manera, mitjançant la publicació, l'acte pot produir uns efectes en l'esfera d'interessos dels ciutadans. La publicació, per posar un exemple, pot donar lloc a diferents conseqüències per al ciutadà i que poden implicar l'execució unilateral dels actes administratius, com ara l'inici de les actuacions d'execució, el còmput del temps per a la meritació d'interessos, o, fins i tot, la destrucció de béns que són l'objecte d'una infracció administrativa.

L'Administració actua de forma unilateral i té privilegis extraordinaris com l'autotutela, i per aquest motiu ha d'assegurar-se que els afectats tenen l'ocasió de conèixer l'acte, perquè així s'afavoreix el seu compliment i es permet l'exercici del dret a controvertir les decisions de l'Administració en via administrativa o judicial. Per aquest motiu, la publicitat de les normes i els actes administratius és tan important, perquè la decisió de l'Administració es pot imposar, i l'Estat té el privilegi de l'ús de la força en monopoli, però el ciutadà ha de poder exercir la seva defensa. Per tant, el coneixement de les decisions per la persona afectada, o la presumpció del seu coneixement a través de la seva publicació, és un aspecte formal important per a l'eficàcia de l'Administració.

El corol·lari jurídic de considerar un determinat instrument com a mitjà de publicació oficial no és altre que donar-li un determinat valor. En aquest cas, la publicació a la seu electrònica permetrà a un determinat acte desplegar els seus efectes (permetre'n l'executivitat, meritació d'interessos, còmput de terminis, ...). D'altra

<sup>6</sup> Entenem en aquest punt l'accessibilitat i la *legibilitat* com a aspectes diferenciats, el primer més tècnic relatiu a la igualtat en l'accés independentment dels mitjans tècnics usats i el segon referit a la capacitat de la informació de ser materialment compresa pel destinatari.

<sup>7</sup> Els articles 4 i 9 del Decret 324/2001, de 4 de desembre, s'expressaven així:

“Article 4. Principis de la informació

La informació administrativa de la Generalitat a través d'Internet ha de ser, com a mínim, la mateixa que es doni presencialment o per altres mitjans i s'haurà de subjectar als mateixos principis i garanties. En tota informació administrativa que es doni a través d'Internet s'haurà de fer constar la data d'actualització. Els ciutadans hauran de poder rebre la informació a través d'Internet de la manera més accessible possible, especialment els que pateixin algun tipus de discapacitat.

[...]

Article 9. Publicació oficial

La informació administrativa facilitada a través d'Internet no substitueix la publicitat legal de les lleis, de les disposicions generals i dels actes que hagin de ser publicats formalment al DOGC i a altres diaris oficials, l'edició impresa dels quals és l'únic instrument que dona fe de la seva autenticitat i contingut”.

<sup>8</sup> Cfr. els articles 56 a 60 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú.

banda, la seu electrònica també es projecta com a complement de la tramitació de procediments. Recordem que una de les utilitats de la seu electrònica, en aquest sentit, és la de permetre l'acarament de còpies autèntiques en suport paper, consultant el document original que es troba a la seu electrònica i que se'ns mostrarà introduint el Codi Segur de Verificació que apareix en les còpies autèntiques (article 30.5 LAECSP). Recentment, la Llei 26/2010, de 3 d'agost de règim jurídic i de procediment de les administracions públiques catalanes permet al seu article 58 la notificació a través de la seu electrònica.

Per tant, i sense deixar de banda el caràcter complementari de la seu electrònica per donar una difusió ampliada a determinats continguts de caire jurídic,<sup>9</sup> sembla prou clar que la projecció de la seu electrònica com a element instrumental en la tramitació administrativa (inclosa la notificació) és indiscutible, tot formalitzant un canal de comunicació informal que tenia per objectiu apropar la informació als ciutadans.

Aquesta caracterització de la seu electrònica suposa una visió limitada de l'abast de l'ús de les noves tecnologies per a la difusió d'informació administrativa, per diversos motius. En primer lloc, aquesta reducció de la norma administrativa a la reglamentació de l'ús de la tecnologia com a instrument de la tramitació deixa de banda l'evolució de les tècniques administratives.<sup>10</sup> Es tractaria d'una visió orgànica i que deixa de banda gran part de l'activitat administrativa.<sup>11</sup> Pel que fa a l'objecte del nostre treball, hem de tenir en compte la pluralitat de continguts que conviuen als portals institucionals i el canvi de paradigma que suposa l'activitat de difusió d'informació enfront de l'accés tradicional. El marc legal, doncs, hauria d'abastar a la convivència de diferents tipus de continguts (audiovisuals, estadístics, cartogràfics, meteorològics, etcètera), la difusió dels quals té una lògica i, per tant, un règim jurídic diferenciat.

D'altra banda, les tasques d'editorialització suposen la creació de contingut *ex novo* necessari per a la contextualització de la informació i la realització efectiva de funció social de la difusió d'informació administrativa. En efecte, la informació administrativa no es pot reduir al contingut dels documents, també s'ha de contextualitzar i oferir els elements necessaris per a la seva comprensió.<sup>12</sup> Aquesta activitat d'editorialització s'hauria de subjectar a determinades garanties d'objectivitat per al públic, adaptades a les concretes característiques del mitjà de difusió. Aquestes qüestions bé mereixen una reflexió més pausada sobre la posició de l'Administració en la comunicació social que ara no podem encetar. En qualsevol cas, la seu electrònica constitueix un bon exemple d'adaptació de les noves tecnologies a les característiques de l'activitat administrativa.

### 2.3. Quines administracions han de disposar d'una seu electrònica?

<sup>9</sup> Cfr. art. 6 LAECSP, que introdueix obligacions de difusió d'informació respecte de la tramitació de procediments d'accés a activitats de serveis.

<sup>10</sup> BARNÉS, Javier. "El procedimiento administrativo y el gobierno electrónico", en DE LA HERA PASCUAL, Cristina (Coord.) *Administración electrónica: Estudios, buenas prácticas y experiencias en el ámbito local*. Barcelona: Fundación Democracia y Gobierno Local. 2010, pp. 82 y ss.

<sup>11</sup> MALARET, Elisenda; ALONSO, Carles. "Els serveis públics informacionals: l'emergència de nous serveis públics en la societat de la informació i el coneixement". *Revista Catalana de Dret Públic*, nº 35/2007, pp. 170-173.

<sup>12</sup> Efectivament, seguint en BRUGIÈRE, la informació administrativa no és reduïble al contingut d'un document administratiu, sinó que s'hauria d'estendre a tota dada o informació susceptible de situar el document en el seu context. BRUGIÈRE, J.M. *Les données publiques et le droit*. Paris: Litec. 2002.

D'acord amb el caràcter de publicació oficial de la seu electrònica, com acabem de veure, només podran gaudir d'una seu electrònica les administracions públiques que actuen sotmeses al Dret Administratiu. L'article 2 (àmbit d'aplicació) LAECSP enumera l'Administració General de l'Estat, l'Administració de les comunitats autònomes i de nivell local, així com les "entitats de dret públic vinculades o dependents de les mateixes". L'article 2.2 exclou explícitament "les Administracions públiques en les activitats que desenvolupen en règim de dret privat". Aquest extrem ens confirma que la seu electrònica és un instrument per assegurar l'eficàcia en l'exercici de potestats típicament administratives, és a dir, les activitats en les que es fan servir prerrogatives o privilegis (de caràcter declaratiu o executiu), i que les actuacions sotmeses a dret privat estan fora de l'àmbit d'aplicació de la llei i, per tant, de l'obligació de disposar d'una seu electrònica.

La LAECSP s'aplica a les administracions en sentit estricte i exclou, per tant, totes les organitzacions públiques *quan* no exerceixen potestats. Per entendre amb precisió quines són les organitzacions destinatàries de l'obligació de disposar de seu electrònica, el criteri subjectiu o formal, doncs, s'ha de completar amb el criteri objectiu o material. Qualsevol actuació administrativa quedarà sotmesa a la LAECSP depenent de si es despleguen potestats administratives, és a dir, en funció de l'activitat objectivament considerada. Això vol dir que la seu electrònica és un instrument per a l'exercici de les competències atribuïdes per les lleis i quan aquest exercici de competències implica la funció d'*administrar*.<sup>13</sup>

En efecte, algunes organitzacions públiques que realitzen activitats típicament comercials o associatives, és a dir, en règim de dret privat, poden exercir, amb la deguda autorització per norma amb rang de llei, algunes funcions de caràcter administratiu. És a dir, es poden servir de privilegis que poden afectar els drets i interessos dels ciutadans en ocasions puntuals o per determinades actuacions, i aquestes actuacions restaran sotmeses al Dret Administratiu. En aquests casos, aquestes organitzacions podrien disposar de seu electrònica per publicar, exclusivament, la informació relacionada amb actes de caràcter administratiu que siguin conseqüència d'aquella concreta potestat administrativa. L'exemple més clar és el de les societats de gestió urbanística, que realitzen activitats en règim privat però eventualment són investides de la potestat expropiatòria.

#### 2.4. El contingut de la seu electrònica

La LAECSP no es preocupa gaire del contingut que hagi de tenir la seu electrònica. Si bé la norma determina alguns continguts bàsics, entenem que tant la norma sectorial com l'autonòmica poden incidir en els continguts i les característiques de les seus electròniques, complementant la normativa estatal. Aquesta reglamentació mínima de la seu l'hem d'entendre com a una conseqüència de la distribució competencial i també com a fruit de la vocació limitada de la LAECSP a tractar l'ús de les noves tecnologies com a eina per a la tramitació procediment administratiu electrònic. Per aquests dos motius, i més enllà de l'obligació de publicar informació sobre l'organigrama de l'Administració i els tràmits relatius a la prestació de serveis

---

<sup>13</sup> MARTÍN, Isaac. "Concepto y régimen jurídico de la sede (administrativa) electrónica", a COTINO, Lorenzo; VALERO, Julián. *Administración Electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant lo Blanch. 2010, pp. 506-509.

establerta a l'article 6.3, la LAECSP no ens dóna un llistat exhaustiu i tancat de la informació que ha de contenir la seu electrònica ni del règim de difusió de la informació general o específica sectorial que, per les seves característiques, no podria formar part d'una publicació oficial.

Els continguts a difondre establerts a l'article 10 LAECSP s'han d'entendre com a continguts mínims lligats al seu caràcter de publicació oficial i d'altres obligacions de publicació d'informació relacionada amb el caràcter instrumental que la normativa atribueix a la seu electrònica com a eina de tramitació procedimental.<sup>14</sup> Així, la tasca de definir els continguts de la seu electrònica recau en els legisladors autonòmics i locals.<sup>15</sup>

Un primer complement del contingut de les seus electròniques el podem situar en la normativa general, ja sigui normativa de desenvolupament de les bases de la LAECSP com la normativa de desenvolupament d'aquestes. Així, en el cas de Catalunya existeixen tres escenaris per a la delimitació de continguts per norma general. El primer és la Llei d'ús dels mitjans electrònics, que és d'aplicació general i conté mandats per a totes les administracions, amb caràcter general, així com obligacions concretes per a les administracions municipals (article 10.2, sobre la publicació a les seues electròniques de les actes de sessions del ple). La Llei catalana de règim jurídic també hi intervé, tot donant utilitat a la seu electrònica per a la publicació d'actes administratius, com és el cas de les delegacions de competències, revocacions o extincions (art. 8.6), els avisos sobre disfuncions del registre (art. 49.1), o la publicació d'anuncis de tràmits d'informació pública (art. 52.2). Veiem, doncs, que la LAECSP ha creat un instrument que després serà utilitzat per d'altres normes generals per donar suport a l'actuació administrativa.

Aquestes normes de caràcter general es complementen sovint amb les normes reglamentàries que les desenvolupen. La primera norma d'aquest tipus que es va aprovar a Catalunya després de la LAECSP, específicament per al seu desenvolupament, fou el Decret d'Impuls, que fixa els continguts mínims de la seu electrònica de la generalitat (inventari de serveis i tràmits electrònics, formularis per iniciar procediments, accés al DOGC, accés al Registre electrònic, sistema d'accés a les comunicacions i notificacions amb l'Administració i al tauler d'anuncis) i estableix l'obligació de publicar determinats actes a la seu electrònica;<sup>16</sup> i aquesta operació també la realitzen les ordenances locals en l'àmbit de l'administració electrònica.<sup>17</sup>

Un altre àmbit de definició dels continguts de la seu electrònica es situa en la normativa sectorial. De fet, la mateixa Llei catalana de règim jurídic ja adverteix que els continguts de les seues electròniques es poden nodrir tant de decisions administratives com de les exigències de 'disposicions específiques' (cfr. art. 7.2). El

<sup>14</sup> A tall d'exemple, vegeu l'article 25 LAECSP (publicació de la disposició de creació i accés als registres electrònics), article 27 (publicació dels mitjans per a comunicar-se amb l'Administració a disponibilitat del públic); cal destacar que la relació de sistemes de signatura i segells electrònics s'ha de publicar 'per mitjans electrònics', sense que es faci referència explícita a la seu electrònica.

<sup>15</sup> Vid. CERRILLO, Agustí. "La difusió de informació de la Administració local a través de mitjans electrònics", en CERRILLO, Agustí; GALÁN, Alfredo. *Informe sobre la administració electrònica local*. Fundació Pi i Sunyer. 2009, p. 158.

<sup>16</sup> Art. 7.3 Acte d'aprovació del Protocol de tràmits i serveis; art. 10.4 Aprovació de programes i aplicacions; Art. 17 Catàleg de dades i documents, etcètera.

<sup>17</sup> L'article 17 de l'ORAE, per exemple, incorpora el tauler d'edictes a la seu electrònica; a l'art. 37 es disposa l'obligació de publicar-hi el Catàleg de tràmits i procediments accessibles per via electrònica.

comportament previsible de la norma sectorial és que vagin adequant la seu electrònica com a instrument de publicació d'informació d'utilitat per al ciutadà o per assegurar l'efectivitat de la seva actuació.

Aquestes crides a la incorporació d'informació a la seu electrònica poden provenir, doncs, de qualsevol tipus de norma que disciplini l'activitat administrativa, com en el cas de les obligacions introduïdes a la Llei Reguladora de les Bases del Règim Local (per la Llei 56/2007, d'Impuls de la Societat de la Informació), sobre la publicació d'informació relativa al planejament urbanístic per mitjans electrònics, en el seu article 70 ter.2. En conseqüència, és possible que el contingut de les seus electròniques es vagi configurant no només amb les aportacions de les normes generals relatives a l'actuació administrativa electrònica, autonòmiques o locals, sinó també amb la reforma o aprovació de normes sectorial o d'altres normes especials.

### 3. Condicions tècniques de la certificació digital en matèria de seu electrònica

#### 3.1. L'adopció de tecnologia per l'Administració en condicions de neutralitat

Quan l'Administració crea la seu electrònica ha de fer-ho en condicions de neutralitat tecnològica. La neutralitat tecnològica és un dels principis d'actuació enunciats a l'article 4.i) LAECSP.<sup>18</sup> L'ús d'estàndards oberts és, segurament, un dels elements més importants de la neutralitat, i això es veu reforçat per la seva inclusió, pel que fa al nostre estudi, en la descripció de les condicions de creació i característiques de la seu electrònica de l'article 10.5 LAECSP.<sup>19</sup> La garantia d'aquestes condicions de neutralitat es troba també recollida a l'article 42.4, que realitza la remissió per a l'elaboració de les normes de desenvolupament de la llei, a través de l'Esquema Nacional d'Interoperabilitat (en endavant ENI) i l'Esquema Nacional de Seguretat (en endavant, ENS).<sup>20</sup>

La visió del principi de neutralitat tecnològica dels preceptes a què ens referíem parteix d'una definició de mínims de la neutralitat tecnològica que pregona la *independència en l'ús de la tecnologia*. Aquesta definició mínima s'ha relacionat sovint amb qüestions de caràcter econòmic i, de fet, existeix en gran part de les administracions i juristes espanyols una visió de la neutralitat vinculada exclusivament a aquesta vessant del principi de neutralitat, que ens és útil per evitar la captivitat de l'Administració respecte d'uns productes sobre d'altres, i evitar la discriminació. Aquesta visió de la neutralitat tecnològica es traduiria, doncs, en

---

<sup>18</sup> “i) Principi de neutralitat tecnològica i d'adaptabilitat al progrés de les tècniques i sistemes de comunicacions electròniques garantint la independència en l'elecció de les alternatives tecnològiques pels ciutadans i per les Administracions Públiques, així com la llibertat de desenvolupar i implantar els avenços tecnològics en un àmbit de lliure mercat. A aquests efectes, les Administracions Públiques utilitzaran estàndards oberts, així com, en el seu cas y de forma complementària, estàndards que siguin d'ús generalitzat pels ciutadans”.

<sup>19</sup> “5. La publicació a les seus electròniques d'informacions, serveis i transaccions respectarà els principis d'accessibilitat i usabilitat d'acord amb les normes establertes al respecte, estàndards oberts i, en el seu cas, aquells altres que siguin d'ús generalitzat pels ciutadans”.

<sup>20</sup> “4. En l'elaboració dels dos esquemes s'han de tenir en compte les recomanacions de la Unió Europea, la situació tecnològica de les diferents administracions públiques, així com els serveis electrònics ja existents. A aquests efectes han de considerar la utilització d'estàndards oberts així com, si s'escau i de forma complementària, estàndards que siguin d'ús generalitzat pels ciutadans”.



l'obligació que l'Administració difongui informació i presti serveis en formats que no requereixin el pagament d'una llicència per tal de llegir els arxius.<sup>21</sup>

Aquesta és una visió força limitada, sobretot si tenim en consideració l'enunciació del principi de neutralitat tecnològica en d'altres legislacions com l'audiovisual o la de telecomunicacions.<sup>22</sup> Caldria, doncs, fer un exercici d'aprofundiment en la definició de la neutralitat tecnològica i, més enllà, pensar en la seva utilitat per al Dret Administratiu, una concepció que ens ajudi, més tard, a avaluar les normes i les tecnologies que intervenen en la posada en marxa de la seu electrònica i els sistemes de protecció, entre els quals els basats en la certificació digital. BOIX PALOP ja adverteix que, tot i que la definició de la LAECSP sembla limitada, en l'esperit i en l'articulat del text és suficientment clar que la neutralitat va més enllà, que també està present en el disseny de les aplicacions i en les qüestions relatives a l'acreditació de la identitat.<sup>23</sup>

La primera conseqüència del principi de neutralitat tecnològica és que permet l'aplicació analògica del dret, quan un supòsit de fet és indiferent a l'ús d'una tecnologia. Una signatura electrònica, per exemple, constituirà un acte d'expressió de la voluntat, independentment dels mitjans utilitzats o la tecnologia emprada per dur-la a terme, per exemple, i que la seva eficàcia no es pot posar en dubte només per aquest fet, com reconeixia la Sentència del Tribunal Suprem de 3 de novembre de 1997. És en aquest sentit també que s'ha de llegir l'article 3.9 de la Llei 59/2003, de 19 de desembre, de Signatura electrònica. El problema el trobem quan la tecnologia permet activitats qualitativament diferents, que abans no eren possibles o bé quan la tecnologia permet una transformació radical en les condicions d'aplicació de les normes. En aquests casos, l'aplicació analògica del dret esdevé impossible o problemàtica, i la norma ha de respondre a aquesta situació de forma adient, sense trencar amb les garanties constitucionals i tenint en compte les característiques de la tecnologia.

En definitiva, l'element de novetat de les noves tecnologies obliga a l'Administració a realitzar una reflexió abans d'adoptar les diferents tecnologies i normes tècniques, amb la finalitat de detectar aquestes incompatibilitats i adaptar les decisions al marc normatiu d'aplicació, per tal d'evitar les disfuncions (normalment en forma de pèrdua de garanties per als ciutadans) que provocaria una importació descontextualitzada d'institucions.<sup>24</sup> Una reflexió que estarà destinada a analitzar el canvi que introdueixen les noves tecnologies en les activitats de l'Administració. En definitiva, estem parlant d'un canvi en el model d'Administració que requereix d'una visió científica, tal i com exposa el professor BARNÉS.<sup>25</sup> Una visió

<sup>21</sup> En aquest sentit s'expressa VALERO TORRIJOS, Julián. "Acceso a los servicios y difusión de la información por medios electrónicos", a Gamero, Juan; VALERO, Julián (Coords.) *La Ley de Administración electrónica. Comentario sistemático a Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Cizur Menor: Aranzadi, 2007.

<sup>22</sup> Cfr. Article 3.f) Llei 32/3002, de 3 de novembre, General de Telecomunicacions; article 16 Llei 22/2005, de 29 de desembre, de Comunicació Audiovisual de Catalunya.

<sup>23</sup> BOIX PALOP, Andrés. "Previsiones en materia de neutralidad tecnológica y acceso a los servicios de la administración", a COTINO, Lorenzo; VALERO, Julián. *Administración Electrónica. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y los retos jurídicos del e-gobierno en España*. Valencia: Tirant lo Blanch. 2010, pp. 318-322.

<sup>24</sup> NIETO, Alejandro. "Globalización y Administración pública", a AAVV *La globalización más allá de la empresa*. Valencia: Universitat Jaime I. 2003.

<sup>25</sup> BARNÉS, Javier. "La Internet y el derecho: una nota acerca de la libertad de expresión e información en el espacio cibernético". *Cuadernos de derecho judicial*, nº6/1997.

que ha de tenir ben present els principis de proporcionalitat i que, com afegiria més tard, tingui en compte l'impacte de la interdisciplinarietat, especialment respecte de les noves tecnologies de la informació i la comunicació, en el Dret Administratiu.<sup>26</sup>

En definitiva, la norma pot intervenir, fins a cert punt, en l'ordenació de l'ús de la tecnologia, però tenint en compte els condicionants jurídics que conformen el context normatiu en què es defineixen aquestes normes. Aquestes normes s'expressaran d'acord amb el seu espai; així, en el cas de l'ús per part dels particulars, l'ús de la tecnologia estarà menys limitat i en el cas de l'Administració és necessària una habilitació legal i una definició del règim jurídic que cobreix les diferents actuacions encarregades a l'Administració.

Per facilitar un ús correcte de les noves tecnologies per part de l'Administració, cal que s'avalui constantment la capacitat de les tecnologies de complir amb les especificitats de l'activitat administrativa i la seva adequació a l'ordenament jurídic. Veiem l'exemple de l'adopció de normes tècniques. L'Administració, quan adopta les noves tecnologies per prestar serveis, treballa en un entorn que li és estrany i en moltes ocasions no participa en l'elaboració de les normes tècniques que condicionen l'ús de la tecnologia. D'aquesta manera, l'Administració es situa en la reraguarda de l'evolució tecnològica. En conseqüència, perd agilitat a l'hora de planificar i prestar serveis i en molts casos l'adopció de la norma tècnica és irreflexiva. Per evitar això, es poden dur a terme accions dirigides a avaluar l'ús d'una norma tècnica. Haurem d'examinar: 1) la norma sorgida de l'autoregulació haurà d'aportar quelcom més que la norma sorgida d'organitzacions de normalització, 2) aquesta funcionalitat haurà de ser vàlida per complir amb les obligacions de l'Administració que la fa servir, i 3) la norma no pot vulnerar drets fonamentals ni pot ser contrària a les lleis vigents. Si més no, també es poden dur a terme accions que vagin més enllà i que situïn a l'Administració en el marc de creació de les normes tècniques. En aquest sentit, algunes organitzacions públiques s'integren en les tasques de regulació tècnica, integrant les necessitats de l'Administració en la creació de les normes tècniques i, alhora, absorbint coneixement que més tard permetrà la prestació de serveis d'alt valor afegit.<sup>27</sup>

En el cas de la seu electrònica, la normativa ha actuat imposant a les administracions la necessitat de mesures que garanteixin la confiança dels ciutadans respecte de la informació que publica l'Administració. La seu electrònica ha d'estar protegida amb un certificat 'de dispositiu segur o mitjà equivalent'. Aquest ús de la tecnologia de la certificació digital és una mesura que permet als ciutadans accedir a uns edificis electrònics de l'Administració minorant el risc de suplantació i permetent en tot moment al ciutadà conèixer l'administració responsable de la gestió d'aquell dispositiu d'informació que és la seu electrònica. Així es garanteix l'accés a la informació sense en condicions de seguretat, gràcies a l'ús de protocols segurs (el certificat de seu electrònica també actua com a agent de negociació de claus de sessió).

<sup>26</sup> BARNÉS, Javier. "Sobre el derecho administrativo de la información", *Revista Catalana de Derecho Público*, nº 35, pp. 125 y ss.

<sup>27</sup> Exemples d'aquesta estratègia ho serien la participació de l'Agència Catalana de Certificació a OASIS i ETSI, participant en la gestió de protocols i normes tècniques per a certificats digitals, o la participació de l'Ajuntament de Gijón a les activitats del World Wide Web, gràcies a la qual, es situa al capdavant del ranking d'administracions accessibles. Aquesta tècnica suposa la integració de l'administració en les tasques de regulació tècnica i és una de les opcions existents per assegurar-ne un bon compliment de la norma tècnica i de la seva avaluació, vegeu ALONSO, Carles. "La accesibilidad de los portales institucionales; especial consideración de las administraciones locales", a CERRILLO, Agustí (coord.). Informe sobre la Administración Electrónica Local. Barcelona: Fundació Carles Pi i Sunyer d'estudis autonòmics i locals. 2009.

Aquesta solució està basada en l'existència de tecnologies de certificació digital i, més concretament, els mecanismes de seguretat i certificació que ja s'havien consolidat en la indústria informàtica. Es tractaria d'una solució tecnològicament neutra, que respecta el dret dels ciutadans d'accedir a la informació general sense haver d'identificar-se i que, alhora, dota al dispositiu d'informació de mesures per donar confiança i seguretat a l'Administració i els ciutadans. Ens trobem davant d'una matèria complexa, que implica la participació d'una diversitat gens menyspreable de normes tècniques i requereix la presa de decisions amb un contingut tècnic important. Aquestes normes tècniques han de ser analitzades des del punt de vista del seu impacte en l'activitat administrativa. En el cas que ens ocupa, s'ha de tenir en compte les capacitats i/o les limitacions de les normes tècniques relacionades amb el certificat de seu electrònica per permetre a l'Administració complir amb les seves obligacions d'identificació i autenticació de l'activitat administrativa.

### 3.2. Les organitzacions d'autoregulació i de normalització en relació a les tecnologies de certificació digital

El funcionament de les tecnologies no es regeix primigèniament per normes jurídiques, sinó per normes tècniques, que sorgeixen de fonts diverses. De fet, les normes jurídiques sovint estan molt influenciades per les normes tècniques. Aquestes normes tècniques elaboren conceptes que després passen a la norma jurídica (aquest és el cas del concepte “dispositiu segur de creació de signatura” o les “declaracions de pràctiques de certificació”, per exemple), cosa que cal tenir molt en compte, doncs les normes tècniques poden néixer en àmbits de diferent tradició jurídica i poden portar a disfuncions en detriment de les garanties jurídiques, com dèiem. En aquest apartat intentarem donar una visió de les normes tècniques que intervindran en relació amb la seu electrònica i els certificats destinats a publicar-hi informació.

En primer lloc, les normes que regulen el funcionament de les xarxes de telecomunicacions són elaborades per l'Internet Engineering Task Force que ha elaborat les normes relatives a la infraestructura de clau pública (PKI, el seu acrònim en llengua anglesa).<sup>28</sup> L'estructura inicial dels certificats digitals va ser definida per l'ITU,<sup>29</sup> que és una organització de dret internacional públic i que elabora estàndards per al funcionament de les xarxes de telecomunicacions.

En l'àmbit europeu les normes tècniques són elaborades per dues instàncies. En primer lloc trobem el Comitè Europeu de Normalització (CEN), que és l'organització de normalització tècnica en l'àmbit de les normes tècniques i estableix els estàndards a la Unió Europea.<sup>30</sup> Pel que ara ens interessa, el principal fruit dels

<sup>28</sup> La principal norma tècnica en aquesta matèria és la Request for Comments n° 2527 (substituída per la RFC 3647), que estableix els principals ítems relatius a la infraestructura PKI i la gestió dels llistats per la comprovació de la vigència dels certificats (Llistes de Revocació de Certificats, LRC). Aquesta normativa tècnica defineix tots els elements que una autoritat de certificació ha de tenir en compte a l'hora de gestionar una infraestructura PKI i que, finalment, hauran de formar part de la Declaracions de Pràctiques de Certificació dels prestadors de serveis de certificació. Respecte d'aquesta i d'altres organitzacions de regulació tècnica d'Internet vegeu ALONSO, Carles. “La governança d'Internet, cap a una regulació compartida”. *Quaderns del CAC*, n° 37 vol. XIV (2). 2011.

<sup>29</sup> Els certificats digitals per a infraestructures de clau pública respon a la norma tècnica X.509, que és una evolució de l'estàndard X.500, que inicialment va ser definit per a l'intercanvi d'informació relativa a l'aplicació de tractats internacionals.

<sup>30</sup> Cal recordar que d'acord amb les directives de contractació pública, les normes sortides d'aquestes organitzacions són les normes aplicables preferents, i que només es pot contractar productes elaborats d'acord amb una norma tècnica diferent en cas d'aportar igual o major seguretat que la norma tècnica ‘normalitzada’. Vegeu l'article 23 de la **Directiva 2004/18/CE del Parlament Europeu i del**

treballs del CEN en matèria de signatura electrònica són les normes CEN CWA 14169 i CWA 14170, relatives als dispositius segurs de creació de signatura (hardware criptogràfic i targetes intel·ligents) i les aplicacions de signatura, respectivament, que, com veurem més endavant, són fruit de la successiva emissió de normes tècniques ISO i IETF en la matèria. D'altra banda, també s'han de tenir presents les normes de l'Institut Europeu d'Estàndards de Telecomunicacions (ETSI), que formalment és una organització sense afany de lucre i informalment està impulsada per la Unió Europea com a organització de normalització d'estàndards.<sup>31</sup> L'ETSI actua en molts àmbits, des dels estàndards per a la radiocomunicació i l'aeronàutica fins a la telefonia i la televisió. Són diverses les especificacions ETSI aplicables a les tecnologies de signatura electrònica, tot completant, en l'àmbit europeu alguns dels elements que la normativa RFC.

En matèria de certificació digital és important destacar l'existència de l'organització privada d'autoregulació OASIS, que elabora estàndards per a la societat de la informació.<sup>32</sup> En l'actualitat, aquesta organització està definint el protocol DSS (Digital Signature Services), mitjançant el qual es realitzaran les operacions de validació dels certificats.

Finalment, existeixen unes normes relatives a la validació de certificats de forma directa pel navegador, que són elaborades per un fòrum de trobada entre prestadors de serveis de certificació i fabricants de navegadors anomenada CA/Browser Forum.<sup>33</sup> Aquesta organització aprova els estàndards i les condicions de gestió dels certificats per tal que els navegadors reconeixin directament els certificats dels prestadors de serveis de certificació i aquests mostrin la seva validesa automàticament, mitjançant la coloració (en verd, si és vàlid, en vermell si el certificat no és vàlid) de la barra de navegació.

### 3.3. Certificats de dispositiu segur per a la seu electrònica

La transmissió de dades en les xarxes de comunicació fa servir protocols que xifren la comunicació de forma simètrica, és a dir, emissor i receptor fan servir la mateixa clau. El canvi que introdueix el certificat de seu electrònica al respecte és que negocia una clau asimètrica per al xifrat de les comunicacions, dotant la comunicació amb la seu electrònica d'un major grau de seguretat. El certificat de seu electrònica dificulta que la pàgina sigui eliminada o falsejada, però el més important és que ofereix informació per generar confiança respecte de l'origen i la seva autoria.

Els certificats de seu electrònica de nivell alt de seguretat utilitzen maquinari criptogràfic HSM (Hardware Security Module). Aquesta és una tecnologia que assegura l'aïllament físic de les claus del certificat. Aquests dispositius poden ser maquinari o productes d'un altre tipus com les targetes intel·ligents (amb circuit integrat), i el seu ús és un requisit de la Llei de Signatura Electrònica per a l'emissió de la signatura reconeguda, que gaudeix de l'equivalència funcional amb la signatura manuscrita. Amb aquests dispositius, a

---

Consell, de 31 de març de 2004, sobre coordinació dels procediments d'adjudicació dels contractes públics d'obres, de subministrament i serveis. La norma que reconeix les organitzacions de normalització és la Directiva 98/34/CE del Parlament Europeu i del Consell, de 22 de juny de 1998, per la que s'estableix un procediment d'informació en matèria de les normes i reglamentacions tècniques, que reconeix les organitzacions al seu Annex.

<sup>31</sup> <http://www.etsi.org/>

<sup>32</sup> <http://www.oasis-open.org/>

<sup>33</sup> <http://www.cabforum.org/>

més de les claus (*something you know*), hi ha un factor físic de seguretat (*something you have*). En el cas de les targetes, la clau privada no surt del xip de la targeta i, per tant, el perill d'intrusió és menor; respecte del hardware criptogràfic, parlem d'un maquinari que està protegit i que pot generar claus per sí mateix.

Donada la importància de les seus electròniques com a fonts d'eficàcia de l'activitat administrativa, la LAECSP vol assegurar-se que estan protegides amb la tecnologia més solvent. Així quan designa el mecanisme de protecció es refereix a sistemes de signatura basats en 'certificats de dispositiu segur'. El concepte de 'dispositiu segur' és un concepte tècnic que està basat en la necessitat de normes tècniques que defineixin les seves característiques i el disseny de les garanties que han de donar (normalment, mitjançant l'elaboració de nivells de protecció). Aquest concepte tècnic fou adoptat per primer cop per la Directiva de Signatura Electrònica,<sup>34</sup> per vincular la validesa jurídica directa dels actes signats a l'ús d'aquest tipus de dispositius.<sup>35</sup> La Directiva inclourà una definició de mínims dels DSCS que es completarà amb les normes aprovades pel CEN.

Posteriorment, la LAECSP imposarà l'ús de certificats basats en tecnologies de dispositiu segur per a les seus electròniques. D'acord amb l'art. 17 LAECSP: "Les seus electròniques utilitzaran, per identificar-se i garantir una comunicació segura amb les mateixes, sistemes de signatura electrònica basats en certificats de dispositiu segur o mitjà equivalent". Aquest aspecte és reiterat a l'article 13.3.a): "Sistemes de signatura electrònica basats en l'ús de certificats de dispositiu segur o mitjà equivalent que permeti identificar la seu electrònica i l'establiment amb ella de comunicacions segures". Aquest matís "o mitjà equivalent" està dirigit a permetre l'ús de tecnologies superiors que encara no hagin estat adoptades per les organitzacions de normalització, una possibilitat que normalment es reserva per no aturar l'adopció de normes tècniques en un context d'innovació constant.

Tot i que l'eficàcia d'aquest dispositius està provada i és generalment acceptada, existeix un problema principal al respecte: la manca de normes tècniques europees que estableixin les condicions que han de complir els dispositius segurs *hardware* per a ser considerats com a tal. Anteriorment, les normes tècniques del Departament de Comerç dels Estats Units (més concretament del National Information of Standards and Technology) ja havien establert els criteris de seguretat (normes FIPS) per al maquinari criptogràfic que després s'adoptaran per la ISO Common Criteria (ISO/IEC 15408).

El problema avui dia és que les normes existents, d'origen americà (normes FIPS), no tenen perquè ser totalment adients en el context europeu. Aquesta és una circumstància que dificulta el correcte desenvolupament de la LAECSP i l'ENS, ja que la inexistència d'una norma tècnica genera dubtes sobre quins requisits de seguretat han de complir els dispositius de custòdia de la clau privada d'un certificat de seu

<sup>34</sup> Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la que s'estableix un marc comunitari per a la signatura electrònica.

<sup>35</sup> D'acord amb l'exposició de motius de la directiva: "Uns criteris harmonitzats en relació amb l'eficàcia jurídica de la firma electrònica mantindran un marc jurídic coherent en tota la Comunitat. Les legislacions nacionals estableixen requisits divergents en relació a la validesa jurídica de les signatures manuscrites; es poden utilitzar certificats per a confirmar la identitat de la persona que signa electrònicament; les signatures electròniques avançades basades en un certificat reconegut permeten aconseguir un major nivell de seguretat. Les signatures electròniques avançades relacionades amb un certificat reconegut i creades mitjançant un dispositiu segur de creació de signatura únicament es poden considerar jurídicament equivalents a les signatures manuscrites si es compleixen els requisits aplicables a les signatures manuscrites".

electrònica. Ara per ara, el Centre Criptològic Nacional té la competència d'avaluar i, en el seu cas, homologar aquests dispositius,<sup>36</sup> però sense la norma tècnica específica, aquest tràmit no garanteix la total adequació del dispositiu a uns criteris de seguretat precisos. De fet, el CCN realitza aquestes avaluacions fent servir els Common Criteria (normes elaborades per ISO) que, tot i ésser estàndards vàlids i tècnicament solvents, haurien de ser analitzats i adaptats al context europeu.

### 3.4. El certificat de seu electrònica en detall

#### 3.4.1. Descripció breu del certificat de seu electrònica

Els sistemes de certificació digital asseguren un mínim d'informació que s'ha establert en successives normes tècniques (de l'ISO i l'IETF).<sup>37</sup> La norma estàndard és la X.509, actualment en la seva versió 3, definida per ITU, i que estructura la informació a través d'extensions. Les extensions existents poden ser obligatòries i opcionals.<sup>38</sup> Gràcies a aquestes extensions, s'estructura la informació existent al certificat, que pot ser llegida per les plataformes de validació i per diferents aplicacions; cada extensió té diferents camps que poden allotjar la informació i que veurem seguidament. La informació pot ser extreta dels camps per complet o només parcialment. Gràcies a aquesta estructuració, les diferents aplicacions i sistemes poden operar de diferents formes, fins al punt que determinats serveis poden operar com a proveïdors d'atributs d'identitat, i es pot extreure informació dels certificats per combinar-les amb altra informació allotjada en un altre sistema.<sup>39</sup>

El certificat de seu electrònica conté, com la resta dels certificats, els camps estàndard del X.509, que li serviran per identificar el prestador de serveis de certificació emissor del certificat, les dades de vigència, els algorismes que fa servir i les dades del subscriptor que, lògicament, serà l'administració responsable de la seu electrònica. L'extensió "subject" (l'assumpte) donarà les dades de l'administració responsable, com diem, i la identificació numèrica i textual del sistema d'informació que és la seu electrònica.<sup>40</sup> Aquesta mateixa extensió recollirà els identificadors específics de la seu electrònica als que més endavant farem referència.

<sup>36</sup> Cfr. art. 2 Real Decreto 421/2004, de 12 de març, pel que es regula el Centre Criptològic Nacional.

<sup>37</sup> ISO 10181-1 i RFC 2459 i 3280. Per veure'n l'evolució i la relació existent entre elles, Ignacio. *ABC de la signatura electrònica*. Barcelona: Generalitat de Catalunya – Agència Catalana de Certificació. 2005, p. 53.

<sup>38</sup> Algunes d'aquestes extensions són la versió (version, actualment, v3), el número de sèrie del certificat (serial number), l'algoritme usat (Algorithm ID, els més usats actualment són SHA-1 i SHA-2), l'extensió que identifica les dades de l'emissor (Issuer, aquesta extensió inclou identificació, adreça postal i NIF, entre d'altres), les dades de validesa (amb una dada d'inici –not before- i una data de finalització de la vigència –not after-, en dates numèriques DD/MM/AAAA), el nom del subjecte (que dona les dades del subscriptor, amb identificació, adreça postal i NIF, entre d'altres) i la informació sobre la clau pública.

<sup>39</sup> D'aquesta forma es pot fer servir la informació dels certificats sense posar en perill la privacitat de la persona a l'hora d'al·legar un atribut d'identitat, HERRANZ, J.; ÍÑIGO, J.; PUJOL, H. "Privacy features of authentication systems", a ROIG, Antoni (Ed.) *Law and web 2.0*. Barcelona: Huygens. 2009.

<sup>40</sup> Aquesta informació seria numèrica i estaria allotjada en el camp "Common Name" on s'hi consignarien els quatre blocs de xifres separats per punts que componen la IP del servidor. El certificat de seu electrònica de CATCert disposa d'un camp addicional al subject (un "organisation Unit Name") que identifica textualment la seu electrònica (per exemple, s'hi consignaria "Seu electrònica de l'Ajuntament de XXXXXX").

Les altres extensions del certificat acostumen a tenir les dades típiques d'un certificat com ara la identificació de les dades de consulta d'estat del certificat on-line mitjançant protocol OCSP o bé mitjançant CRL (Certificate Revocation List, un arxiu que conté una llista dels certificats revocats i que es pot descarregar lliurement –depenent del model de negoci del prestador, ja que alguns prestadors cobren per consultar llistats). Una altra novetat que aporta el certificat de seu electrònica és el fet que dins dels camps obligatoris es pot fer servir el camp “subject alternate names” per fer-hi constar l'adreça de correu habilitada per la formulació de suggeriments i queixes. La disposició d'aquesta bústia es deriva de l'obligació establerta a l'article 10.3 LAECSP i que es podria consignar a la seu electrònica, però la inclusió de l'adreça de correu al mateix certificat constitueix una garantia complementària.

A més, aquest certificat, té activat el Qc Statement (Declaració sobre l'ús de certificat qualificat), on s'hi consigna el fet que el certificat està emès en un dispositiu segur de creació de signatura, tal i com ordena la LAECSP, i que s'acredita amb la referència d'un OID de la jerarquia de ITU que fa referència a un estàndard de l'ETSI que, tècnicament penja de l'arrel de ITU (0.4.0.1862.1.3; el primer zero identificaria l'arrel d'OID de l'ITU, el quatre identificaria que estem dins del camp dels estàndards definits per ETSI, el 1862 identificaria al prestador –en aquest cas, CATCert- i 1.3 identificaria la qualitat del DSCS).

### 3.4.2. Els camps específics del certificat de seu electrònica

La diferència més notable del certificat de seu electrònica és el fet que permet la identificació –territorial- de l'exercici de la competència, que s'opera mitjançant la inclusió de camps definits prèviament al “subject” que, com dèiem, recull les dades relatives al subscriptor. En concret, parlem dels atributs definits conjuntament per ISO i ITU, que defineixen tipus d'organització, número de sèrie, adreça, localitat, província, país i codi postal, i es deriven d'una norma ISO.<sup>41</sup>

Respecte d'aquests camps, sorgeixen alguns dubtes. Per exemple, el *Province Or State Name* fa referència a una delimitació territorial infraestatal. La nostra traducció literal de “province”, evidentment, és la província, però caldria afinar i saber a què ens estem referint, doncs en d'altres estats la província és l'equivalent a les nostres comunitats autònomes (com a Canadà), i quan es parla d'estats, en realitat s'està parlant dels estats federats en el marc d'una federació (en el cas dels Estats Units d'Amèrica). Així doncs, potser hauríem de replantejar-nos la forma com omplim aquest camp, ja que si només consignem aquest camp com el nivell territorial provincial, aquesta delimitació serà estèril quan a autenticació de la competència. En efecte, la denominació de la província no ens permet saber si l'Administració responsable de la seu electrònica exerceix les seves competències en l'àmbit estatal, autonòmica o local.

D'altra banda, els certificats haurien de poder donar alguna informació o alguna pista sobre la identificació material de la competència, és a dir, que haurien d'ajudar a trobar els títols competencials que ostenten els diferents subscriptors de certificats de seu electrònica. És evident que hauria de ser la seu electrònica o el portal web de la institució el que aportés aquesta informació, més encara si tenim en compte que la

<sup>41</sup> ISO/IEC 9834-3:1990, Procedures for the operation of OSI Registration Authorities -- Part 3: Registration of object identifier component values for joint ISO-CCITT use.

distribució competencial és una matèria força complexa i que no només relaciona normes de dret positiu, sinó també jurisprudència (del tribunal constitucional).

Una possibilitat seria la de disposar, en l'extensió "subject" d'un camp addicional que contingues un enllaç a la seu electrònica o qualsevol altra pàgina relacionada amb la seu electrònica on trobar aquesta informació; també es podria disposar informació sobre el tipus de potestats que s'exerceixen, si són declaratives o executives i en quines actuacions s'expressen. Segurament existeixen més opcions a desenvolupar, però també cal tenir en compte que la implementació d'aquestes opcions dependrà també, en gran mesura, del que disposin les diferents administracions a l'hora de construir les seves seus electròniques.

### 3.4.3. Els certificats de seu electrònica de validació estesa

El certificat de validació estesa és un certificat digital que dona una confiança afegida als dispositius – normalment servidors- gràcies a la indicació de la validesa del certificat en la barra d'adreces del navegador; si és vàlid, es mostra la barra de color verd i si no és vàlid, la barra serà de color vermell. Tecnològicament, el certificat de validació estesa és igual que la resta de certificats i té la mateixa base tecnològica tot i que incorpora algunes novetats per permetre la validació automàtica del certificat. Aquest resultat s'aconsegueix perquè els navegadors tenen carregats els certificats arrel dels prestadors de serveis de certificació que compleixen les normes de CA/B Forum i els navegadors poden validar el certificat emès pel prestador en l'instant de demanar accés a una adreça electrònica.<sup>42</sup> És a dir, existeix un procediment previ en què s'auditen els prestadors i es comprova que els seus productes i serveis són de confiança.

Normalment, aquest tipus de certificats es fan servir en el comerç electrònic, per incrementar la confiança dels compradors, ja que sovint s'intercanvien dades bancàries. En definitiva, aquest certificat reforça la confiança de l'usuari en el contingut i dificulta encara més el *phishing*, ja que si bé es pot falsejar un certificat, s'afegeix un altre punt de confiança que són els navegadors. Cal tenir en compte, en tot moment, que els certificats de validació estesa no poden evitar totalment el *phishing*, i que existeixen tècniques per induir a error el visitant com la "*picture-in-picture*", que imita el procés que duu a terme un certificat de validació estesa amb imatges que emulen la validació mitjançant imatges, o la interposició en la comunicació per simular la petició de validesa (una tècnica denominada "*man-in-the-middle*").<sup>43</sup> Val a dir que aquestes tècniques són efectives si l'usuari no és un usuari experimentat, ja que es poden detectar amb alguns coneixements bàsics.

El certificat de validació estesa té un avantatge principal i és el fet que l'usuari no haurà de carregar les claus públiques dels prestadors de serveis de certificació perquè els navegadors coneguin la font del certificat de seu. Així s'evita l'aparició d'un missatge en el navegador que alerta del desconeixement del prestador de

<sup>42</sup> Aquest certificat va ser proposat el 2005 per Melih Abdulhayoglu al CA/Browser Forum (<http://www.cabforum.org/>), un fòrum de debat voluntari entre fabricants de navegadors i prestadors de serveis de certificació i va ser aprovat el 12 de juny 2008. Els aspectes tècnics de funcionament el podeu trobar al document *Guidelines for Extended Validation Certificates* [http://www.cabforum.org/Guidelines\\_v1\\_2.pdf](http://www.cabforum.org/Guidelines_v1_2.pdf)

<sup>43</sup> Vegeu l'estudi de JACKSON, Collin; SIMON, Daniel R.; TAN, Desney S.; BARTH, Adam. *An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks*. [www.adambarth.com/papers/2007/jackson-simon-tan-barth.pdf](http://www.adambarth.com/papers/2007/jackson-simon-tan-barth.pdf).



serveis de certificació (per part del navegador), doncs aquest avís surt amb independència que el certificat hagi estat vàlidament emès per un prestador legalment establert i que el certificat estigui vigent. Aquest és, si tenim en compte que els certificats digitals estan destinats a millorar la confiança dels ciutadans en el tràfic jurídic, un element distorsionador de la confiança entre ciutadà i Administració que cal evitar, ja que la simple aparició d'aquest missatge –originat per la inexistència de les claus públiques en el navegador– produirà, en un usuari mitjà, la lògica desconfiança en la seu electrònica.

Evidentment, la càrrega de les claus públiques dels prestadors de serveis de certificació en els navegadors per part dels ciutadans evitaria problemes d'aquest tipus, i unes bones pràctiques en matèria de divulgació podrien facilitar aquesta feina, ja que el problema es concentra en el fet que els ciutadans no tenen carregades les claus públiques dels certificats arrels dels prestadors en els seus navegadors. En conseqüència, els prestadors públics de certificació hauran de procedir, per evitar la confusió del públic i millorar les condicions d'identificació, adaptar-se a l'ús de certificats de validació estesa.

Aquesta adaptació passa per l'assumpció de les normes del CA/Browser Forum, sempre que siguin assumibles dins del marc normatiu de referència. Aquestes normes inclouen especificacions sobre la gestió dels certificats i, molt especialment, de la necessitat de procurar la revocació de certificats o la negativa d'emetre'ls a subscriptors que estiguin inclosos en llistes negres confeccionades per a víctimes de *phishing*.

#### **4. La definició i la classificació dels certificats digitals en la norma jurídica i la pràctica administrativa**

##### **4.1. La definició de les normes tècniques d'interoperabilitat per als certificats digitals**

La LAECSP no es pronuncia sobre quines hagin de ser les característiques dels certificats digitals, és a dir, sobre la seva estructura interna, a la que ens referim generalment com a perfil del certificat, així com tampoc estableix un procediment per a l'admissió dels certificats per part de les administracions públiques. La definició dels perfils és, *a priori*, una tasca dels prestadors de serveis de certificació i, en principi, els poden definir lliurement sempre que es respectin les prescripcions de la LAECSP, és a dir, sempre que acreditin l'exercici de la competència. L'admissió de certificats està contemplada a l'article 21 LAECSP, que estableix les condicions d'interoperabilitat dels certificats digitals, les condicions en què les administracions han d'admetre el seu ús. Aquest precepte té un contingut material però cap exigència formal o de procediment a l'hora de decidir l'admissió dels certificats en els procediments administratius o els documents electrònics.

La definició dels perfils de certificats ha estat un dels punts de debat constant durant l'elaboració de l'Esquema Nacional d'Interoperabilitat que, en les seves versions de treball, atorgava la competència sobre aquesta matèria al govern estatal. És, si més no, bastant dubtós que aquesta possibilitat de definir perfils comuns pugui emparar-se en la distribució competencial vigent. En efecte, la imposició de perfils comuns, com la resta dels extrems relacionats amb la interoperabilitat no es pot emparar en l'article 4 LSE, que

permet imposar condicions addicionals a les administracions en l'ús de la signatura electrònica.<sup>44</sup> Tampoc no és clar que l'ENI pugui entrar a definir perfils comuns, d'acord amb el tenor literal de l'article 42 LAECSP, ja que es refereix a l'ENI com a una norma dirigida a definir (el subratllat és nostre) “el conjunt de criteris i recomanacions en matèria de seguretat, conservació i normalització de la informació, dels formats i de les aplicacions que hauran de ser tingudes en compte per les Administracions Públiques per a la presa de decisions tecnològiques que garanteixin la interoperabilitat”.

Doncs bé, l'habilitació al reglament que disposa l'article 42 LAECSP era bastant limitada, però el contingut de la DDAA 1<sup>a</sup> de l'ENI defineix aquesta tasca permetent al Ministeri de la presidència (a proposta del Comitè Sectorial d'Administració Electrònica) l'aprovació de les “normes tècniques” que conformaran els requisits de signatura, entre las quals es poden definir els perfils de certificat, tot fent una interpretació extensiva de l'àmbit de la remissió reglamentària que donava lloc a l'ENI.

Durant els anys 2008 i 2009 els prestadors públics de serveis de certificació i el Ministeri de Presidència van negociar uns perfils comuns de certificats (segell electrònic, treballador públic i seu electrònica) per millorar la interoperabilitat entre aplicacions i certificats de l'Administració i donar així compliment a la LAECSP. Aquests acords s'acabarien plasmant en un document administratiu aprovat en el context de les normes tècniques d'interoperabilitat esmentades per l'ENI, anomenat ‘Perfils de certificats electrònics’, aprovat formalment pel Consejo Superior de Administración Electrónica.<sup>45</sup>

D'aquesta manera, una norma que semblava establir una limitació complementària a la limitació de la distribució competencial, ha acabat per emparar, en una doble remissió reglamentària, aspectes tècnics de detall per als prestadors de serveis de certificació, retenint un ampli control sobre els productes de certificació digital. I tot i que inicialment aquesta documentació es produeix de forma negociada, la decisió final acaba per recaure en l'AGE.

#### 4.2. L'admissió de certificats com a potestat administrativa: la classificació

La pràctica desenvolupada en relació a l'admissibilitat dels certificats digitals augmenta la complexitat de la matèria. Els certificats digitals funcionen gràcies a l'existència d'una infraestructura tècnica que permet validar els certificats, és a dir, tornant una resposta als sol·licitants sobre l'estat de validesa, caducitat o revocació del certificat. En el cas de les administracions públiques, s'han creat, a més dels prestadors públics de serveis de certificació, plataformes de validació que constitueixen un intermediari entre les administracions i els prestadors privats de serveis de certificació tot realitzant aquesta tasca de comprovar l'estat d'un certificat.

---

<sup>44</sup> Vegeu els comentaris d'ALAMILLO a l'avant-projecte de l'ENI. ALAMILLO, Ignacio. “Reflexions competencials sobre l'esborrany d'Esquema Nacional d'Interoperabilitat”. *Revista Catalana de Dret Públic*, nº 40/2010.

<sup>45</sup> La versió consultada és la 1.7.6, de 21 de juliol de 2010.

En l'àmbit estatal, l'accés a la validació dels certificats en la plataforma interadministrativa denominada @firma es produeix d'acord amb una documentació que estableix les condicions del servei.<sup>46</sup> Aquesta documentació, però, no abasta tots els extrems relacionats amb la càrrega dels perfils al validador ni l'estructura dels perfils ni els requeriments als prestadors; tampoc no s'estableixen límits quantitius a l'entrada dels certificats en la plataforma ni especificitats de procediment. Existeix una condició formal prèvia a la càrrega de certificats en la plataforma, que és el 'reconeixement' per part del Ministeri d'Indústria, que registra els certificats reconeguts que emeten els prestadors de serveis de certificació. En realitat, només hauria de ser això, un registre que determinés el compliment dels articles 11 i següents LSE. Ara bé, aquest registre acaba sent un element predeterminant per a la càrrega dels certificats al validador de l'AGE. D'aquesta manera, les exigències del Ministeri d'Indústria acaben per determinar la possibilitat d'usar els certificats en l'àmbit de l'AGE, constituint, *de facto*, una exigència afegida als requisits d'interoperabilitat *ex art. 21 LAECSP*, ja que la documentació de servei d'@firma no en fa cap referència.

En el cas català, el Decret d'Impuls, en el seu article 32 condiona l'admissió de certificats a la 'classificació' dels sistemes de signatura, tot dibuixant els contorns d'una potestat administrativa que s'haurà de realitzar de conformitat amb el que estableixi un Protocol d'Identificació i Signatura.<sup>47</sup> És a dir, supedita l'ús dels certificats dels prestadors privats en l'àmbit de la Generalitat a la seva classificació, que és una activitat de supervisió dels prestadors privats de serveis de certificació. Aquesta funció és l'expressió d'una potestat administrativa de comprovació del compliment de la Llei de Signatura Electrònica i permet a l'Administració una supervisió de l'activitat del prestador que realitza la sol·licitud inicial de la classificació o la seva renovació.

La classificació funciona com a un servei lligat a la prestació dels serveis de validació dels certificats. Els serveis de l'Administració catalana consumeixen recursos de validació prestats per CATCert i el Consorci d'Administració Oberta de Catalunya. Per tal d'agilitzar l'admissió dels certificats dels prestadors de serveis de certificació, es classifica els certificats assignant un nivell de classificació que facilitarà les decisions de l'administració a l'hora d'implementar els serveis i ordenar els tràmits que requereixen l'ús dels certificats digitals.<sup>48</sup> Un cop realitzada la classificació, s'han de carregar els perfils dels certificats dels prestadors en la plataforma de validació, per tal que hi pugui treballar; si el validador coneix l'estructura dels certificats permetrà a l'aplicació consumidora accedir efectivament a la informació. Aquesta activitat és necessària perquè els prestadors de serveis de certificació estructurin la informació dels certificats de forma diferent; aquesta diversitat d'estructures i formes d'emetre els certificats s'ha de respectar i aquest fet implica la tasca d'adequar el validador a les diferents formes d'estructurar la informació dels prestadors per tal que siguin

---

<sup>46</sup> Les condicions del servei s'estableixen a l'Acord de Nivell de Servei i la Declaració de Pràctiques de Validació, que podeu trobar a <https://administracionelectronica.gob.es/>.

<sup>47</sup> Article 32. *Els sistemes de signatura electrònica de persona jurídica*

Les persones jurídiques poden fer servir, en les seves relacions electròniques amb l'Administració, els sistemes d'identificació i signatura electrònica que hagin estat classificats d'acord amb el protocol d'identificació i signatura electrònica. Això també és aplicable a les entitats sense personalitat jurídica, sense perjudici de les especificitats derivades de la seva naturalesa.

<sup>48</sup> Mitjançant aquesta classificació, l'Administració només ha de consignar el nivell de seguretat requerit, confiant que en el tràmit de classificació s'han comprovat les mesures de seguretat per part dels prestadors que emeten certificats d'aquell nivell.

intel·ligibles per l'aplicació consumidora. D'una altra forma, l'Administració estaria imposant als prestadors una forma d'emetre els certificats, de forma contrària a la LAECSP i la LSE.<sup>49</sup>

Aquesta forma de treballar respon a la necessitat que les administracions comprovin que els prestadors de serveis de certificació compleixen amb la legalitat i, en conseqüència, s'accepten els certificats dels prestadors privats tal i com s'emeten, sempre que compleixin, també, les condicions establertes a les normes tècniques pel que fa la gestió de la infraestructura de clau pública. En interposar-se com a intermediari, el classificador evita que cada administració hagi de comprovar per si mateixa les condicions de gestió dels certificats i prepara les condicions de validació d'un certificat. Es tracta, doncs, d'una feina de valor afegit que supera el compliment de la legalitat i que té sentit per millorar el funcionament dels serveis de l'Administració, descarregant-les de funcions pesades en la interpretació dels certificats.

Aquesta activitat, si més no, no està completament reglamentada pel que fa al tractament de les sol·licituds, a la supervisió dels prestadors de serveis de certificació i al procediment per a la classificació o la revocació de la classificació de certificats. En una obra anterior, ja advertíem que en moltes ocasions, es tracten funcions d'autoritat com a activitats mercantils i a l'inrevés, com en el cas de tractar l'assignació de dominis com a activitat mercantil i al contrari considerar la difusió d'informació com a serveis de la societat de la informació.<sup>50</sup> En aquest cas, l'enunciació d'una activitat que és pròpiament administrativa es realitza d'una forma indefinida i mitjançant tècniques que no responen a les necessitats i obligacions que cobreixen les potestats administratives –com el cas del registre per un ministeri com a requisit per a validar certificats pel servei prestat per un altre ministeri- o bé queda ocult darrera de la seva caracterització de serveis, com si es tractés de conceptes contraposats.

El resultat d'aquesta confusió és, en definitiva, que aquests serveis no tenen una reglamentació administrativa acurada que estableixi les condicions i el procediment mitjançant el qual es classifiquen els certificats i, en definitiva, poden donar lloc a una manca de transparència respecte dels pressupòsits de l'actuació administrativa i, en darrer terme, a l'arbitrarietat. La definició del procediment de classificació hauria de vetllar per l'establiment de les condicions en què es poden excloure els certificats o com es duu a terme la supervisió dels prestadors, i com els criteris a aplicar com per exemple en quina mesura es considera que una determinada tecnologia és obsoleta i/o insegura i com es determinen les normes tècniques a aplicar.

## 5. A mode de conclusió: qüestions tecnològiques i jurídiques de futur entorn de la certificació digital de les seues electròniques

Gràcies a la flexibilitat i la constant evolució de les noves tecnologies, la capacitat de la tecnologia de certificació digital per donar més transparència i fiabilitat a l'actuació administrativa pot augmentar considerablement. Segons hem tingut oportunitat de veure, la seua electrònica constitueix una evolució de la difusió d'informació administrativa adaptada a la singularitat i l'especificitat de l'activitat administrativa.

<sup>49</sup> ALAMILLO, Ignacio. "Reflexions competencials...", op.cit., apartat 2.7.

<sup>50</sup> MALARET, Elisenda; ALONSO, Carles. "Els serveis públics...", op.cit.

Hem pogut examinar la forma en què es garanteix la identificació de la seu electrònica i l'autenticació l'exercici de la competència gràcies a la certificació digital. Si bé hem comprovat la capacitat d'aquests mecanismes per donar satisfacció a la necessitat de garantir l'exercici de la competència, també hem constatat que es poden incrementar els esforços per millorar la informació del públic respecte de les potestats administratives.

Un segon factor que permet adaptar la tecnologia a les necessitats de l'Administració és la incorporació del coneixement tècnic a través dels prestadors de serveis públics informacionals. En el cas de la certificació digital, l'existència dels prestadors públics de serveis de certificació permet la constant avaluació de la tecnologia en termes d'interès general com, igualment, la participació en la creació de les normes tècniques, directament a les organitzacions d'autoregulació o, de forma indirecta, reglamentant els aspectes tècnics dels certificats digitals i duent a terme la classificació dels certificats digitals, a mode d'activitat de supervisió de compliment dels requisits legals i reglamentaris establerts.

L'evolució de les noves tecnologies és una matèria que no queda, doncs, fora de l'abast de les potestats administratives. El coneixement de la tecnologia resulta indispensable, primer per adaptar i avaluar les capacitats de la tecnologia sota el prisma de les necessitats de l'Administració i també per adaptar d'una forma efectiva les peculiaritats de l'actuació administrativa a l'ús de les noves tecnologies. D'aquesta forma, el coneixement flueix en totes dues direccions i l'Administració guanya efectivitat en l'acompliment de les tasques que té assignades.

Finalment, hem vist que les administracions prenen decisions en l'àmbit tecnològic però aquestes decisions no han d'estar destinades a uniformar l'ús de la tecnologia, sinó més aviat el contrari, a fomentar un ús avançat de les tecnologies, i en definitiva un impuls del canvi de la cultura administrativa. L'acompliment d'aquests objectius requereix d'una reflexió profunda i un edifici jurídic i administratiu objectiu, neutral i, sobretot, transparent.