ESTUDIS DE RECERCA DIGITALS 3

Ignacio Alamillo Domingo
F. Xavier Urios Aparisi

L'actuació administrativa automatitzada en l'àmbit de les administracions públiques

Anàlisi jurídica i metodològica per a la construcció i l'explotació de tràmits automàtics

Generalitat de Catalunya
Escola d'Administració Pública de Catalunya

L'ACTUACIÓ ADMINISTRATIVA AUTOMATITZADA EN L'ÀMBIT DE LES ADMINISTRACIONS PÚBLIQUES

Anàlisi jurídica i metodològica per a la construcció i l'explotació de tràmits automàtics

---

Ignacio Alamillo Domingo
F. Xavier Urios Aparisi

Barcelona, 2011

Generalitat de Catalunya
Escola d'Administració Pública de Catalunya

Aquest estudi és fruit d'una subvenció de l'Escola d'Administració Pública de Catalunya destinada a elaborar treballs de recerca per a la millora de les administracions públiques (Resolució GAP/2965/2008, de 17 de setembre), i ha estat sotmès a una avaluació externa que n'ha validat el contingut i n'ha recomanat la publicació.

Primera edició: gener de 2011
ISBN: 978-84-393-8702-2
Dipòsit legal: B.7247-2011

SUMARI

PRESENTACIÓ

La regulació legal de les tecnologies de la informació i les comunicacions en l'àmbit de les administracions públiques no és, ni de bon tros, un fenomen nou a Espanya, que, en la seva primera regulació amb una vocació general i sistemàtica, troba el punt de partida en la ja llunyana Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú i, en concret, a l'article 45, avui en gran part derogat. No obstant això, cal reconèixer que només ha estat en els últims anys que el seu ús ha experimentat un nivell considerable i, en conseqüència, s'han evidenciat els inconvenients i els desajustos provocats per un marc normatiu que, des d'una visió prospectiva i, per tant, gaudint d'un cert avantatge, no s'adequava ja a les necessitats de modernització tecnològica que plantejava l'exigència d'una Administració pública moderna i preparada per assumir els desafiaments de la societat de la informació.

Fa poc més de tres anys, la Llei 11/2007, de 22 d'abril, d'accés electrònic dels ciutadans als serveis públics (LAE) ha intentat oferir un marc normatiu adequat al context referit en el qual, com la seva exposició de motius afirma, «les administracions s'han de comprometre amb la seva època i oferir als seus ciutadans els avantatges i les possibilitats que la societat de la informació té, assumint la seva responsabilitat de contribuir a fer-la realitat». Tanmateix, com ja ho he mantingut en un altre lloc,[1] encara que cal reconèixer que s'han produït avenços significatius amb la Llei esmentada, el cert és que es podia haver anat més enllà, sobretot tenint en compte que es tractava d'una oportunitat històrica per avançar en la consolidació i l'enfortiment de molts principis de l'Estat democràtic i arribar a un nou model d'Administració pública bolcada efectivament a resoldre els problemes de la societat i dels ciutadans, amb una participació i un control efectius, més enllà de les limitacions pròpies dels processos electorals de cada quatre anys. I, per això, concloïa amb un desig que «la nova regulació no es converteixi en una excusa per a un mer canvi de suport que acabi per justificar la versió actualitzada d'una indesitjable *burocràcia electrònica*».

La posterior consolidació a Espanya d'un corrent d'opinió, no tant doctrinal com sobretot des de la valoració pràctica, sobre la necessitat d'un nou model de govern i Administració pública basat en l'ús de les tecnologies de la informació i la comunicació —del qual el denominat *Open Government* és un dels millors exponents—[2] sembla donar suport a aquesta tesi, de manera que es reclama l'aprofitament de les possibilitats que ofereix la

[1] «La nova regulació legal de l'ús de les tecnologies de la informació i les comunicacions en l'àmbit administratiu: el viatge cap a un nou model d'Administració, *electrònica*?». *Revista Catalana de Dret Públic*, núm. 35, pàg. 242.

[2] http://eadminblog.net/post/2007/05/27/administracion-abierta-open-government-un-modelo-a-partir-del-open-business

tecnologia per reformular tant l'activitat de les administracions públiques com, des d'una dimensió externa, les relacions amb els ciutadans. En aquest sentit, la utilització de la tecnologia en l'àmbit esmentat s'està començant a concebre no ja com una simple oportunitat per a la modernització de les estructures i els procediments sinó, fins i tot i sobretot, per a la innovació, és a dir, per il·luminar una nova concepció de l'Administració pública que, a través de la tecnologia, permeti donar verdadera satisfacció a la seva raó de ser: el servei als interessos generals, això és, a la societat i els ciutadans, amb eficàcia i eficiència, de manera que s'eradiqui, una vegada per sempre, la percepció tan freqüent en molts àmbits que l'Administració és un autèntic llast social.

Precisament, el recent Pla d'acció europeu sobre e-Government 2011-2015[3] estableix entre els seus eixos prioritaris l'increment d'eficiència i una efectiva atenció a les prioritats dels usuaris, la millora dels processos organitzatius i la reducció de les càrregues administratives, així com, en última instància, la necessitat de plantejar els serveis electrònics des de la perspectiva de la innovació. Es tracta, en definitiva, de reptes i desafiaments a què només es pot aspirar a partir de l'actuació administrativa automatitzada: resulta clarament ineficient que, malgrat els avenços tecnològics i, sobretot, les abundants inversions realitzades, les decisions de les administracions públiques continuïn basant-se en la intervenció directa de persones físiques quan aquesta no és necessària o oportuna. Ara bé, les enormes possibilitats que ofereix la tecnologia pel que fa a això s'han de plantejar des de la necessària primacia del dret i, en particular, de les normes juridicoadministratives que assegurin que les decisions administratives s'adopten amb les màximes garanties.

Per això, i per les raons que més endavant s'exposaran, el llibre que el lector té a les mans (o a la seva pantalla) era certament necessari, ja que es tracta de la primera monografia que aborda amb caràcter exclusiu aquesta transcendent problemàtica, de manera que es converteix en una referència inexcusable a l'hora d'abordar qualsevol iniciativa mínimament ambiciosa de modernització administrativa. Més encara, la indiscutible qualificació dels autors constitueix una garantia que el tractament dels problemes que s'aborden i les solucions que es proposen no solament s'han plantejat des del coneixement teòric sinó, a més i sobretot, en vista de la seva efectiva implicació en la realitat en què han d'aplicar-se les mesures proposades.

Encara recordo quan vaig tenir la sort de conèixer Ignacio Alamillo Domingo, a Múrcia, cap a l'any 2000, acabat d'aprovar el Decret llei 14/1999, en ocasió de la impartició d'una conferència sobre la signatura electrònica en un moment en què aquesta eina estava tenyida d'unes connotacions futuristes que pràcticament la situaven al marge dels cercles en què habitualment ens movíem els juristes: avui dia, sense cap dubte és un dels màxims experts europeus en relació amb la gestió de les identitats electròniques, en

[3] http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/index_en.htm

particular pel que fa a la seva projecció en la prestació de serveis administratius. Al seu costat, F. Xavier Urios Aparisi aporta, des de la seva condició de cap de l'Assessoria Jurídica del Departament de Governació i Relacions Institucionals de la Generalitat de Catalunya, una sòlida formació juridicoadministrativa que, més enllà de la perspectiva teòrica, es fonamenta en el coneixement directe dels problemes que, en aquest procés, ha d'abordar el dret, perquè s'hi ha hagut d'enfrontar —i, sobretot, solucionar-los, de vegades de manera imaginativa—, en prestar els seus serveis en una organització que, sens dubte, ha liderat la modernització tecnològica de l'Administració pública a Espanya durant molts anys.

Així doncs, des de la perspectiva que aporta el coneixement efectiu de la matèria, els autors han fet una aportació de gran vàlua amb aquesta obra ja que, en definitiva, s'han vist obligats a enfrontar-se *cara a cara* amb un dels principals encotillaments que pateixen les administracions públiques espanyoles: la percepció del dret i, en concret, del dret administratiu com un inconvenient per a la modernització tecnològica de l'Administració pública, que, com una de les seves principals manifestacions, determina l'existència d'una cultura administrativa que, més enllà de les estrictes exigències del principi de legalitat pròpies d'un Estat de dret, reclama una regulació exhaustiva extrema; *reglamentista* en l'accepció més pejorativa del terme, en la qual absolutament tots els detalls han d'estar regulats en la norma escrita, encara que aquesta solució dificulti i, fins i tot, impedeixi qualsevol intent de modernització en benefici d'una pretesa seguretat jurídica que, en definitiva, a mitjà termini pot arribar a produir un efecte contrari al volgut. Precisament, aquest llibre suposa un avenç decidit en aquesta ingent tasca, sobretot tenint en compte les deficiències de la regulació que, en relació amb l'automatització de l'activitat administrativa, conté la LAE i que els autors lúcidament aborden per oferir solucions efectives, ajustades a les exigències que planteja la realitat administrativa, tan necessitada d'una autèntica renovació per fer front, a través de la tecnologia, a alguns dels desafiaments més rellevants que la societat exigeix amb vehemència a les nostres administracions públiques.

En aquest sentit, des d'una perspectiva tecnològica s'enfronten a conceptes nuclears del dret administratiu com ara el principi de la competència, l'exercici de les potestats o, sobretot, la teoria de l'òrgan i, en concret, l'exigència que les decisions administratives siguin adoptades directament per la persona física a la qual en correspongui la titularitat; entroncant d'aquesta manera amb el que, fins ara, havia estat considerat l'element subjectiu de l'acte administratiu. O, pel que fa a l'eventual invalidesa de l'actuació administrativa, la incidència que pugui tenir sobre aquesta la deficient programació de l'aplicació informàtica utilitzada és analitzada amb encert pels autors malgrat la seva dificultat, actualitzant conceptes tradicionals de gran arrelament com és la desviació de poder, que, en aquest context, es projectaria en la informàtica decisional aplicada a les administracions públiques. Tanmateix, lluny d'un exercici d'erudició allunyat de la realitat

pràctica a la qual es refereix, el treball que ara presento se centra en la realització d'una anàlisi rigorosa però, alhora, basada en el coneixement directe de la matèria i, per tant, no ha de sorprendre que es plantegin propostes concretes en forma de recomanacions concretes i l'anàlisi d'exemples concrets d'actuacions administratives l'automatització de les quals es proposa en forma de taules. Tot això, a partir d'una anàlisi que té en compte tant la perspectiva jurídica com l'organitzativa, la tecnològica i, fins i tot, la filosòfica a través de la denominada *lògica deòntica*.

Certament, es podrien haver abordat altres problemes i aspectes encara latents en relació amb les actuacions administratives automatitzades o, fins i tot, haver-ho fet des d'altres perspectives, però aquest pròleg no és el lloc més adequat per iniciar un debat doctrinal sobre el tema. Simplement m'agradaria explicitar la idea que he tractat de transmetre en els paràgrafs anteriors: la meva recomanació que llegeixin amb gran interès aquest llibre suggeridor, ja que sens dubte val la pena.

Julián Valero Torrijos
Professor titular de Dret Administratiu
Universitat de Múrcia

1. INTRODUCCIÓ GENERAL

L'objecte d'aquest treball consisteix en l'anàlisi de la viabilitat jurídica i tècnica de l'automatització dels actes administratius a partir de les reflexions i els resultats principals d'un treball de recerca patrocinat per l'Escola d'Administració Pública de Catalunya realitzat durant els anys 2008 i 2009.

Durant aquesta recerca, s'han pres en consideració uns supòsits d'actes administratius que, en una primera aproximació, eren susceptibles d'automatització. Un cop analitzats, s'han intentat extrapolar les condicions jurídiques i tècniques que s'haurien de dur a terme per tal de garantir que l'actuació administrativa automatitzada s'adeqüi al marc normatiu de referència i a les condicions tècniques que facin viable aquesta automatització.

En aquest sentit, durant la recerca s'ha analitzat cadascun dels elements que han de ser considerats i en relació amb els quals l'òrgan responsable de l'automatització ha de prendre decisions concretes a fi de garantir que l'automatització de l'acte administratiu no tan sols s'ajusta a la norma, sinó també que no produeix perjudicis o reducció de garanties als administrats.

Es pot avançar que l'anàlisi s'ha dut a terme des de la prudència, per tal com la cautela és un principi o criteri bàsic a l'hora d'implementar l'administració electrònica i, especialment, més encara quan parlem de la reducció de la capacitat de decisió de la voluntat humana, en la mesura que és la màquina la que pren decisions. Tanmateix, el treball s'ha conformat sobre la base d'una programació prèvia que, lògicament, parteix de la factura humana, raó per la qual l'anàlisi i les conclusions es poden considerar conservadores.

1.1. Sobre la viabilitat de l'automatització de processos

No obstant això, la primera conclusió a extreure és la viabilitat de l'automatització de processos, per les raons que posteriorment es presentaran i que es poden concretar en una premissa: hi ha actuacions administratives que es poden automatitzar, i fins i tot raons d'eficiència en recomanen l'automatització.

Les raons d'aquesta conclusió són evidents: es tracta de situacions en què l'acte administratiu com a expressió d'una voluntat humana és reduït, perquè aquest element volitiu es limita sovint a la comprovació d'uns elements reglats, cosa que, en la pràctica, s'arriba a convertir en un automatisme. En aquests casos, no s'aprecien problemes

rellevants per a l'automatització. De tota manera, això no significa una llibertat absoluta per integrar una resposta automàtica a determinades actuacions, sinó que caldrà instrumentar un protocol que asseguri que la implementació de l'automatisme es duu a terme adequadament i, en la mesura que ens trobem davant actes administratius, permetre el control de la legalitat de l'actuació administrativa.

Aquesta adequació, necessària tant en l'àmbit normatiu com en l'àmbit tècnic, és objecte de tractament als capítols 2 i 3 d'aquest treball. En aquests apartats s'analitzen els requeriments jurídics i tècnics que cal tenir en compte en l'automatització i s'intenta donar respostes concretes a cadascuna de les qüestions plantejades.

Finalment, s'ha generat una guia de recomanacions que es presenta en aquest mateix capítol. Aquesta guia intenta resumir les recomanacions de caràcter jurídic, d'anàlisi i de disseny, com també sobre tècniques de sistema, de signatura electrònica, de certificats de segell automàtic i de seguretat i auditoria, les quals garantirien, des del nostre punt de vista, que l'actuació administrativa automatitzada s'adeqüés a la norma.

Parlem necessàriament d'adequació a la norma, ja que és evident que, en l'àmbit del dret administratiu, la submissió a la norma és essencial, sense que altres fonts del dret —com el costum— resultin rellevants.

En aquest sentit, la recerca ha analitzat, des de la teoria de les potestats administratives, les actuacions que les diferents administracions públiques han de dur a terme en l'àmbit normatiu a l'hora de donar cobertura a aquesta automatització. Naturalment, s'ha partit de la base del marc jurídic vigent —essencialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics— i s'ha fet esment sobretot de la normativa catalana aprovada recentment en l'àmbit de l'Administració de la Generalitat de Catalunya, en què hi ha previsions normatives específiques relatives a aquesta automatització.

De l'anàlisi d'aquesta normativa s'han extret conclusions que, en principi, es poden traslladar a altres administracions públiques de caràcter territorial —les administracions locals—, amb el límit evident que suposa el respecte al principi d'autonomia local en aquest àmbit.

En la mateixa línia, en la mesura que les matèries relatives a impuls, ordenació i desenvolupament dels serveis electrònics tenen un caràcter organitzatiu, i que de l'article 103.1 i 2 de la Constitució deriva la indicació que les decisions organitzatives s'han d'adoptar d'acord amb una llei, és essencial que els aspectes bàsics de l'automatització estiguin recollits en una norma amb rang de llei.

Aquesta habilitació es troba a l'article 39 de la Llei 11/2007:

«En cas d'actuació automatitzada s'ha d'establir prèviament l'òrgan o òrgans competents, segons els casos, per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema d'informació i del seu codi font. Així mateix, s'ha d'indicar l'òrgan que ha de ser considerat responsable als efectes d'impugnació.»

Aquest article té una naturalesa doble: es tracta d'un article principal, en la mesura que preveu els trets bàsics de l'automatització d'una manera molt somera, però, a més, no té caràcter bàsic, cosa que significa que, en principi, altres titulars de la potestat legislativa podrien establir requeriments diferents.

No obstant aquesta previsió, ja hem avançat que l'automatització de processos haurà de respectar aquests mínims, atès que eliminar-los podria comportar una reducció de les garanties de la ciutadania i de la transparència de l'actuació administrativa automatitzada.

Aquesta habilitació legal de caràcter estatal permet que les comunitats autònomes estableixin altres condicionants de l'actuació administrativa automatitzada amb normes amb rang de llei, si bé en tot cas caldrà un desplegament reglamentari que complementi els criteris legals establerts, que manquen d'un nivell de concreció reservat al reglament.

En aquest sentit, la recentment aprovada Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, al seu article 44, tal com veurem, regula l'actuació administrativa automatitzada, sense que es contradigui amb el que es preveu a la normativa estatal.

A més, existeix igualment la possibilitat que, al marge de la regulació legal dels aspectes bàsics i el desplegament reglamentari corresponent, es produeixi una descàrrega dels aspectes més tècnics i canviants, que es poden concretar amb normes de rang inferior, en què aquests es concretin i se sotmetin a un règim de publicitat inferior (es tractaria sobretot dels aspectes més tècnics i d'alguns d'organitzatius).

En resum, a l'empara d'una previsió legal habilitadora de caràcter estatal i d'una habilitació reglamentària, es pot dur a terme l'automatització de processos en el marc legal establert sense que sigui necessari que tots els elements tècnics es trobin recollits a les normes esmentades anteriorment. No obstant això, sí que cal que un instrument normatiu de nivell inferior reculli o reguli aquests aspectes tècnics o de detall que, per la seva naturalesa, no és recomanable que s'incloguin en una norma legal o reglamentària,

la qual, atesa la seva naturalesa, és molt més difícil d'adaptar o d'adequar a les circumstàncies tècniques que vagin variant.

En qualsevol cas, l'article 39 de la Llei 11/2007 enumera els elements que han estat objecte d'anàlisi: l'òrgan administratiu, la competència, la definició de les especificacions o els programes, l'auditoria i el control de qualitat, i la impugnació de l'actuació administrativa automatitzada.

1.2. Elements a considerar a l'hora d'automatitzar els actes administratius

Els elements següents han estat analitzats al llarg de la recerca. Tots ells es presenten detalladament al capítol 2 d'aquest treball.

1.2.1. *L'òrgan administratiu*

Tot i que l'automatització suposa la desaparició de la voluntat humana *stricto sensu*, no planteja problemes per una raó doble: en primer lloc, per l'habilitació legal existent per a aquesta substitució, i, en segon lloc, pel fet que la desaparició de la voluntat humana és merament aparent, ja que aquesta es manifesta mitjançant la programació que s'ha de confeccionar i aprovar amb caràcter previ a l'automatització de l'acte de què es tracti.

Aquesta programació parteix de la realització d'una metodologia d'anàlisi i disseny que parteix de l'acte administratiu a automatitzar —la seva naturalesa i particularitats— i que es trasllada al que ha de ser una informatització correcta, és a dir, aconseguir que la resposta de la màquina derivi d'una programació que respon als criteris tècnics establerts sobre la base de criteris jurídics (la resposta o la decisió de la màquina és, evidentment i en última instància, una actuació jurídica de la qual deriven efectes jurídics).

En aquest sentit, les recomanacions sobre anàlisi i disseny que s'exposen als capítols 3 i 5 són enormement rellevants, atès que la connexió o l'entesa entre el jurista i el tècnic, sempre important quan parlem d'administració electrònica, és especialment significativa en l'àmbit de l'automatització.

Per aquesta raó, la desaparició de la voluntat humana és merament aparent, ja que la conjunció de l'anàlisi, evidentment humana, dels aspectes jurídics i tècnics per part de persones habilitades o capacitades legalment a aquest efecte —és a dir, competents— fan que, en última instància, l'actuació administrativa automatitzada es pugui considerar

l'exteriorització d'una voluntat humana, d'un òrgan administratiu competent a aquests efecte.

1.2.2. *La competència*

La competència de l'òrgan parteix de la base que, en l'àmbit del dret administratiu, la competència és irrenunciable i l'exerceix l'òrgan que la té atribuïda legalment.

En aquest cas, quan parlem de competència, ho hem de fer en un nivell doble: competència per automatitzar i competència per determinar com automatitzar.

1.2.2.1. Competència per automatitzar

La competència per automatitzar suposa una decisió discrecional del poder públic, que decideix que determinats actes administratius són susceptibles d'automatització. Tal com hem indicat, aquesta decisió és clarament discrecional i prèvia a l'automatització pròpiament dita, i fins i tot pot obeir a criteris de valoració de riscos a l'hora de concretar els actes que es podrien automatitzar.

Ja hem advertit que, en principi, aquesta decisió s'hauria de prendre d'acord amb criteris de prudència, i que l'automatització s'hauria de traslladar inicialment a les actuacions que, per la seva naturalesa, han de plantejar menys riscos.

La recerca s'ha centrat en diferents supòsits classificats en tres grups:

1) Els actes que es podrien anomenar *d'entrada*, en la mesura que tenen lloc en el moment inicial del procediment. Es tracta dels rebuts de registre electrònic, les comprovacions automàtiques de sol·licituds i la digitalització automàtica de documents.

2) Els actes *interns del procediment*, que es produeixen en l'àmbit de la tramitació administrativa des de la vessant interna. Són els actes d'impuls automàtic del procediment, actes automàtics de constància, les còpies autèntiques automàtiques, l'obertura i el tancament de llibres, la foliació automàtica de documents i les migracions automàtiques.

3) Els *actes de sortida*, ja siguin fruit d'actes de comunicació amb altres administracions públiques o bé amb la ciutadania (les notificacions pròpiament dites).

De l'anàlisi d'aquests supòsits s'han extret les conclusions que l'automatització no plantejaria problemes des de la vessant jurídica ni des de la vessant tècnica, sens perjudici que s'han de prendre decisions concretes basades en la plasmació documental de l'acte, el tipus de signatura electrònica a emprar i altres elements que s'han de singularitzar en funció de cada acte.

Al mateix temps, la decisió sobre l'automatització ha d'implicar una millora de l'eficiència administrativa, tant des de la vessant de funcionament com des de la vessant econòmica. Des de la vessant de funcionament, l'automatització ha de comportar una reducció de terminis, conseqüència lligada a l'administració electrònica configurada globalment però que en l'automatització de processos ha de ser encara més evident. Des de la vessant econòmica, tot i que és una obvietat, l'automatització ha de permetre alliberar o destinar a altres activitats d'interès general recursos humans destinats tradicionalment a feines que, encara que sigui parcialment, es poden considerar mecàniques i que una màquina programada degudament pot dur a terme.

En particular, cal destacar que supòsits com la digitalització de documents, els rebuts de registre, la comunicació de dades entre administracions públiques o les notificacions administratives són paradigmàtics en relació amb els avantatges comentats. No obstant això, la resta d'actuacions analitzades, tot i que potser són menys visibles, tampoc no deixen de tenir rellevància en el funcionament ordinari dels òrgans administratius.

Les decisions relacionades amb els actes administratius susceptibles de ser automatitzats es poden prendre aïlladament, cas per cas, o bé en el marc d'una política de planificació en què, encara que sigui parcialment, els criteris discrecionals es condicionen al marc de planificació que hagi estat determinat o aprovat.

En un segon nivell, fins i tot es podria plantejar l'automatització de decisions administratives en què, malgrat que es basen aparentment en l'exercici de potestats discrecionals, hi ha elements reglats que condicionen el contingut de la resolució a dictar. Aquest seria el cas, per exemple, de l'atorgament de subvencions —amb la comprovació prèvia del compliment de les condicions d'atorgament— o la denegació de subvencions per manca de compliment dels requisits establerts a la convocatòria —que es podria comprovar de manera automàtica mitjançant el control de la sol·licitud presentada, integrada, si s'escau, a una notificació automàtica prèvia per esmenar la sol·licitud corresponent.

D'acord amb el que hem exposat, les possibilitats de l'automatització de l'actuació administrativa són evidents i clarament avantatjoses per al funcionament de l'Administració.

1.2.2.2. Competència per determinar com automatitzar

Quan l'òrgan administratiu competent hagi determinat quins actes són susceptibles d'automatització, cal instrumentalitzar aquesta automatització. Es tracta d'una competència dels òrgans administratius que tinguin atribuïdes aquestes funcions de caràcter tècnic des de la doble vessant, jurídica i estrictament tècnica, en relació amb les actuacions que s'han de practicar.

En aquest segon nivell, el marge d'actuació és menys ampli, perquè el marc normatiu que cal aplicar a l'automatització considerada formalment l'integra el conjunt d'aspectes jurídics i tècnics que han de ser avaluats i als quals es tracta de donar resposta mitjançant una programació adequada.

En aquesta fase, caldrà concretar les condicions jurídiques i tècniques d'automatització amb una programació lògica i de codificació que garanteixi que l'acte administratiu emès és correcte, complet, suficient i no discriminatori.

A l'hora de determinar com s'ha d'automatitzar, cal resoldre igualment aspectes concrets de l'actuació administrativa en funció de l'acte o el tràmit de què es tracti, com ara la signatura electrònica a emprar i els certificats de segell automàtic.

Com s'ha indicat a l'anàlisi, tota actuació administrativa automatitzada és, en definitiva, una manifestació més de la manera d'actuar de l'Administració, en la mesura que implica, en darrera instància, l'emissió o la producció d'actes administratius. Aquest fet porta aparellada la identificació i l'autenticació necessàries de qui produeix l'acte, la qual cosa està lligada clarament a la competència de l'òrgan per dur a terme l'actuació concreta.

Per aquesta raó, la utilització o la regulació del segell d'òrgan ens farà plantejar la teoria general de l'acte administratiu i de la competència de l'òrgan administratiu, els supòsits en què aquesta figura es podria admetre, així com els límits a la informàtica decisional que s'hauran d'establir en la construcció i l'aprovació de programes i aplicacions.

1.2.2.3. Un tercer nivell de competència

Al marge dels dos nivells de competència exposats, existiria un tercer nivell: el de la competència que percep directament la ciutadania, és a dir, l'actuació administrativa concreta que deriva de l'automatització del procediment i, en definitiva, d'un maquinari programat degudament per produir actes amb un contingut determinat en funció dels pressupostos que concorrin.

Aquest darrer concepte de competència, des de la vessant ciutadana, ha de ser en principi irrellevant, ja que l'actuació administrativa s'ha de configurar de manera indiferenciada tant si es duu a terme presencialment com si es fa per mitjans electrònics i, en aquest darrer cas, fins i tot si és conseqüència de l'automatització.

La capacitat de reaccionar que té l'administrat o l'administrada davant l'actuació que l'afecta serà, tanmateix, una qüestió diferent. En aquest supòsit, de la mateixa manera que es pot instar la revisió de l'acte des del punt de vista substantiu —és a dir, pel que fa al seu contingut material—, l'acte també pot ser revisat des de la vessant formal, configurada al voltant de la regularitat formal de la seva producció (competència de l'òrgan, aptitud del titular, etc.).

1.2.2.4. La definició de les especificacions i els programes

Ja hem incidit anteriorment en el concepte de definició de les especificacions i els programes, que gira al voltant del compliment dels requeriments jurídics i tècnics que són aplicables.

A més, cal tenir present que, en l'àmbit del dret administratiu, un element essencial de l'actuació administrativa és la motivació de l'acte, fonamental per controlar-ne la regularitat. En el cas de l'actuació administrativa automatitzada, no hi ha una motivació aparent, per tal com les màquines no poden emetre declaracions de voluntat pròpiament dites ni formular declaracions de voluntat, de judici, de coneixement o de desig, si recordem la definició clàssica d'acte administratiu que va fer Zanobini.

És per això que la motivació de l'acte automatitzat es relaciona de manera directa amb la programació adequada de l'actuació, ja que en aquesta es plasmen els criteris tècnics i jurídics que, davant determinats supòsits, comporten determinades conseqüències observades en actes administratius concrets.

Aquesta definició de les especificacions i els programes ens ha portat a avaluar si continua sent necessari aprovar els programes i les aplicacions i difondre'n públicament les característiques, com preveia l'article 45.4 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, tenint present que la Llei 11/2007 ha implicat justament el contrari: la desaparició de les obligacions esmentades (no regulant la qüestió i derogant l'article 45.4).

Des del nostre punt de vista, aquesta aprovació —lligada directament a la doctrina de la vinculació positiva i les potestats administratives— continua resultant necessària. Tanmateix, pel que fa a la difusió pública, es poden establir sistemes de publicitat de les característiques de les aplicacions que no impliquin necessàriament publicacions en diaris oficials, sinó que es poden substituir per altres mitjans de difusió, com ara la incorporació d'aquestes característiques a la seu electrònica corporativa.

Sigui com sigui, en l'àmbit de l'actuació administrativa automatitzada es parla específicament de la definició de les especificacions i els programes, la qual cosa s'ha d'entendre equiparable a l'aprovació.

Com a regla general, aquesta aprovació es preveu ja en àmbits com el dret tributari, en què la duria a terme l'òrgan competent a efectes d'impugnació. Això garantiria que el control de l'acte el mantingués qui, en darrera instància, verificaria la regularitat de l'actuació administrativa.

1.2.2.5. L'auditoria i el control de qualitat

Un altre element a avaluar en l'àmbit de l'actuació administrativa automatitzada és l'establiment de sistemes d'auditoria i control de qualitat.

És evident que l'actuació administrativa automatitzada s'ha de fer de forma segura. S'ha d'articular, per tant, al voltant de la seguretat dels sistemes i les aplicacions emprats, cosa que es pot acreditar mitjançant l'auditoria d'aquests sistemes i d'aquestes aplicacions.

Aquest àmbit inclou dues fases clarament diferenciades: l'establiment i la implementació de sistemes de seguretat, d'una banda, i la realització d'auditories que acreditin que la primera fase compleix els paràmetres legals i tècnics exigibles, de l'altra.

Quant a la primera fase, i partint igualment dels casos d'ús d'autenticació dels subjectes que intervenen en el procediment i de la documentació gestionada, s'han d'establir

normatives de seguretat, bàsicament criptogràfica, que garanteixin la seguretat en les actuacions administratives mitjançant la definició d'estàndards, claus a emprar, i d'aplicació de les signatures electròniques adequades.

Pel que fa a la segona fase, l'auditoria de tercers de confiança, qualificats degudament, és la que garanteix de forma més adequada que la implementació de l'automatització, des de la vessant de la seguretat, resulta correcta.

1.2.2.6. Impugnació de l'actuació administrativa automatitzada

La capacitat de reaccionar de l'administrat o l'administrada davant els actes administratius que l'afecten és un dret bàsic que, en l'àmbit de l'actuació administrativa automatitzada, s'ha d'enfocar des d'una perspectiva doble:

- el control de l'acte administratiu produït, i
- el control de la regularitat o la correcció de la programació realitzada.

Aquesta capacitat de reaccionar ens ha conduït igualment a avaluar les conseqüències de la manca de compliment dels requeriments que resultin aplicables a l'automatització.

Aplicant la teoria general de la invalidesa dels actes jurídics, si l'actuació administrativa automatitzada no es troba emparada en una habilitació suficient, la regularitat del mecanisme de producció d'actes administratius es trenca.

Aquest vici entraria en la consideració d'invalidesa absoluta, que, traslladada a l'àmbit del dret administratiu, determinaria un supòsit de nul·litat absoluta, ja sigui per considerar que es tracta d'un acte dictat per un òrgan manifestament incompetent (lletra b de l'article 62.1 de la Llei 30/1992), ja sigui per un supòsit de prescindir totalment del procediment (lletra e del mateix article).

En aquest sentit, la regla general seria la nul·litat de ple dret, vici determinant de l'actuació administrativa que, en l'àmbit de la utilització dels mitjans electrònics, és especialment significatiu atesa la manca de confiança que la utilització d'aquests mitjans genera encara actualment als administrats.

Això ens ha de portar a ser prudents a l'hora d'implementar l'automatització de processos. No podem caure en una automatització irracional i arbitrària, sinó que el que és recomanable és automatitzar els processos que ho permeten clarament i, a la vista dels resultats assolits, plantejar l'automatització de processos de decisió més complexos.

D'altra banda, seria igualment possible que el vici que es produís no fos la nul·litat de ple dret, sinó l'anul·labilitat de les actuacions administratives realitzades, la qual podria tenir lloc en els supòsits d'una programació inadequada. Això deriva del caràcter restrictiu que es predica de la nul·litat de ple dret, aplicable tan sols als supòsits establerts taxativament i legalment com aquells que porten aparellada la nul·litat de ple dret (que són els esmentats a l'article 62.1 de la Llei 30/1992). En aquest sentit, en la mesura que una programació inadequada no s'encabiria en cap dels supòsits taxatius de nul·litat de ple dret, s'hauria de considerar una causa d'anul·labilitat, recollida a l'article 63 de la Llei 30/1992.

Per contra, una programació indeguda o qualsevol altre defecte de caràcter semblant no es podria considerar una actuació administrativa irregular, ja que difícilment es produirien els supòsits previstos legalment. En qualsevol cas, caldria remetre's a les circumstàncies del cas concret a l'efecte d'avaluar aquest punt (per exemple, una notificació més enllà del termini establert legalment per raó de la caiguda del servidor es podria considerar un acte de notificació irregular, sempre que no s'hagués produït el silenci administratiu positiu i que la notificació fos d'un acte de contingut negatiu).

Finalment, es podria produir una desviació informàtica de poder, cosa que implicaria traslladar al camp de la informàtica decisional la doctrina de la desviació de poder. En aquest sentit, la desviació de poder, configurada com a supòsit d'anul·labilitat, tindria lloc quan la programació dels programes i les aplicacions que han de dur a terme l'actuació administrativa automatitzada corresponent, tot i que aparentment s'adequa a la legalitat aplicable, s'ha realitzat per a una finalitat o persegueix una finalitat diferent de la que preveu l'ordenament jurídic. En definitiva, lligaria amb la idea que la motivació de l'acte administratiu automatitzat deriva de la programació practicada i aprovada degudament.

1.3. Altres qüestions objecte d'anàlisi

La recerca ha incidit en altres aspectes de l'actuació administrativa automatitzada:

- Els drets dels ciutadans com a límit de l'automatització.
- Els límits de l'actuació administrativa automatitzada.

1.3.1. *Els drets dels ciutadans com a límit de l'automatització*

A la recomanació de prudència a l'hora d'automatitzar els actes administratius, s'hi ha d'afegir que, com a conseqüència de l'automatització, els drets dels ciutadans en les seves relacions amb les administracions públiques no es poden reduir.

Aquests drets han de ser els que reconeix la normativa específica, particularment la Llei 11/2007, però també caldrà respectar tots els drets que reconeix l'ordenament jurídic amb caràcter general.

Tan sols una norma amb rang de llei podria alterar aquest règim de drets, com a conseqüència del principi de legalitat i de la reserva de llei en la matèria.

1.3.2. *Els límits de l'actuació administrativa automatitzada*

L'automatització de processos no es pot traslladar a qualsevol actuació administrativa. En aquest sentit, l'automatització és més viable en l'àmbit de les potestats reglades que en l'àmbit de les potestats discrecionals.

El segell d'òrgan també obliga a revisar el règim de recursos administratius i els mitjans d'impugnació, perquè el recurs d'alçada o de reposició, admesos tradicionalment com a mitjans d'impugnació o recursos ordinaris en l'àmbit del dret administratiu, no poden ser traslladats a l'actuació administrativa automatitzada sense cap matisació. A títol d'exemple, en el cas del recurs de reposició, no ens trobaríem amb una reposició per part del mateix "òrgan" que va decidir l'acte impugnat; en el cas del recurs d'alçada, si l'òrgan competent és el que ha acordat l'automatització de l'acte i ha aprovat les condicions d'aquesta automatització, ens trobaríem *de facto* amb un recurs de reposició. Així, en la pràctica, significaria traslladar al mateix òrgan que ha pres la decisió d'automatitzar una actuació administrativa determinada la resolució dels recursos que es puguin interposar.

Paral·lelament, l'automatització ha de quedar exclosa de tots aquells supòsits en què hi hagi un element subjectiu o una valoració en l'actuació administrativa, així com una

motivació més enllà d'aquella que sigui viable predeterminar mitjançant una programació concreta. Altrament, s'estarien vulnerant els principis generals del procediment administratiu i, a més, es produiria una rebaixa dels drets dels ciutadans que no estaria emparada per la Llei 11/2007.

En resum, correspon a cada Administració determinar els supòsits i els tràmits en què es pot aplicar el segell d'òrgan, si bé aquesta determinació no es pot dur a terme indiscriminadament, sinó a partir d'una valoració adequada dels actes administratius que es poden fer de forma automatitzada, d'acord amb el principi de proporcionalitat, i sense que es produeixi una minva de garanties de l'administrat o l'administrada.

Per acabar, també cal tenir present el respecte a la normativa de protecció de dades. L'automatització no pot partir de la base del tractament indiscriminat de dades de caràcter personal de què disposi l'Administració per avaluar determinats aspectes, sinó que s'haurà de fer respectant plenament la normativa esmentada.

Així es preveu a l'article 13 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal. En qualsevol cas, aquesta previsió s'ha d'interpretar en termes molt estrictes, sense fer-ne una interpretació restrictiva ni tampoc extensiva, ja que això impediria la presa de decisions derivada de dades que posseeix l'Administració, la qual cosa no és la finalitat de la Llei orgànica de protecció de dades.

1.4. Recomanacions per a l'automatització de l'actuació administrativa

En resum, es pot concloure que l'actuació administrativa automatitzada és jurídicament viable i que el marc jurídic actual n'habilita la implementació. No obstant això, no n'hi ha prou amb una habilitació legal genèrica, sinó que cal un desplegament en un segon nivell, al marge de determinats aspectes tècnics que poden ser objecte de regulacions de rang inferior.

D'altra banda, l'automatització requereix una decisió prèvia de l'òrgan competent que, en funció de la naturalesa de l'acte, en determini, per raons d'interès general, l'automatització. Aquesta circumstància comportarà el desenvolupament d'unes tasques administratives, jurídiques i tècniques per fer efectiva l'automatització en el marc jurídic i tècnic aplicable. Així mateix, caldrà determinar les condicions de programació que garanteixin que el contingut de l'acte s'adequa a la finalitat prevista i establir, amb una concreció lògica i tècnica adequada, les condicions de producció de l'acte.

L'aprovació més o menys formal d'aquests programes i especificacions no exclou una supervisió de l'actuació administrativa produïda, tant des de la vessant interna com la

que derivi de la reacció del destinatari de l'acte, que, amb caràcter general, pot reaccionar davant una actuació administrativa que l'afecta. Concretament, si es tracta d'un acte administratiu automatitzat, podrà reaccionar tant respecte al contingut —com passa en qualsevol acte administratiu— com respecte a les condicions de l'automatització. Ja hem avançat que, segons els casos, es podria arribar a determinar la nul·litat de ple dret de l'actuació produïda.

1.4.1. *Recomanacions jurídiques*

Recomanació 1.1. L'automatització dels processos s'ha d'adequar al marc jurídic vigent, en particular, l'article 39 de la Llei 11/2007 i la normativa dictada en desplegament d'aquesta Llei.

Recomanació 1.2. L'automatització suposa una decisió prèvia discrecional de l'òrgan competent, que ha de determinar els actes administratius susceptibles d'automatització i controlar la programació de les aplicacions per tal de garantir que l'emissió dels actes administratius automatitzats s'adequa a les condicions d'aplicació.

Recomanació 1.3. Com a regla general, són susceptibles d'automatització els actes administratius reglats. L'automatització de l'actuació administrativa en l'exercici de potestats discrecionals és més complicada.

Recomanació 1.4. L'automatització de processos no ha de significar una reducció de les garanties dels administrats, que han de tenir la possibilitat de reaccionar davant l'actuació administrativa automatitzada per defensar els seus drets i els seus interessos legítims.

Recomanació 1.5. L'automatització requereix l'aprovació dels programes i les aplicacions per part de l'òrgan competent, que, a més, hauria de difondre'n públicament les característiques a l'efecte de garantir el dret de la ciutadania i la transparència en l'actuació administrativa.

Recomanació 1.6. L'actuació administrativa automatitzada s'ha de produir d'acord amb una atribució expressa de competències, que actuarà igualment com a límit del seu exercici.

Recomanació 1.7. La identificació i l'autenticació de l'actuació administrativa automatitzada es practicaran d'acord amb els criteris o les polítiques de signatura electrònica aplicables, en funció de l'acte, el tràmit o el servei de què es

tracti.

Recomanació 1.8. La motivació de l'acte administratiu automatitzat es fonamenta en l'adequada programació. Per aquesta raó, només es podrà reaccionar davant l'acte administratiu emès mitjançant la revisió d'aquesta programació (possibilitat de revisió o de reacció que s'ha de donar a l'administrat).

Recomanació 1.9. L'automatització de processos al marge de la normativa habilitadora configura un supòsit de nul·litat de ple dret, mentre que una programació indeguda es podria integrar en un supòsit d'anul·labilitat.

1.4.2. *Recomanacions sobre cicle de vida del programari*

Recomanació 2.1. Adoptar una metodologia de gestió del cicle de vida del programari per reduir els riscos d'errors en l'automatització. Resulta força evident, segons la nostra opinió, que no disposar d'una metodologia més o menys formalitzada i madura per desenvolupar el programari que suporta l'aplicació d'actuació administrativa automatitzada implica assumir una sèrie de riscos, especialment en relació amb possibles errors de programació, que es poden actualitzar en forma d'una programació inadequada del sistema i, per tant, en motiu d'impugnació de l'actuació per part de les parts afectades.

Recomanació 2.2. Avaluar formalment, en la fase d'anàlisi de viabilitat del sistema, la possibilitat d'automatitzar actes administratius de voluntat en consideració a dos factors principals: la configuració de l'acte administratiu com a potestat reglada o la predeterminació raonable dels casos en què actua la discrecionalitat administrativa, d'una banda, i de la informatització correcta de la norma aplicada, especialment en termes de la necessària motivació-justificació dels actes automàtics, que a parer nostre s'haurà d'incorporar al text de la resolució de forma particularment detallada, sobretot en els actes de voluntat i en els actes de judici.

Recomanació 2.3. Un cop decidit que fer l'actuació de forma automatitzada és viable, cal tractar específicament l'aspecte lògic i semàntic en relació amb els sistemes d'actuació administrativa automatitzada, tenint en compte les necessitats de satisfacció i completesa en la interpretació de la norma o conjunt de normes a aplicar de manera automàtica, per tal de complir el criteri de la programació adequada.

Recomanació 2.4. Durant les fases d'anàlisi i disseny, cal involucrar intensament personal expert en l'àmbit legal per tal de garantir una anàlisi adequada dels requisits funcionals a partir d'una interpretació jurídica apropiada de les normes en què es basaran els actes administratius i, molt especialment, els de naturalesa decisòria. Segons la nostra opinió, l'analista informàtic necessita suport específic per poder transformar la norma jurídica en un conjunt de regles programables.

Recomanació 2.5. En la fase de disseny, abans d'especificar els components, s'ha de dur a terme una verificació i una validació amb la finalitat d'analitzar la consistència entre els diferents models i formalitzar l'acceptació del disseny de l'arquitectura del sistema per part dels usuaris d'explotació i sistemes. Al nostre entendre, és necessari involucrar en aquesta verificació i en aquesta validació personal expert en qüestions legals que pugui garantir la consistència entre el disseny i la interpretació legal fixada en les etapes anteriors, a fi d'evitar possibles errors.

Recomanació 2.6. En la fase de construcció del programari, cal emprar metodologies de desenvolupament segur i tècniques de qualitat, ja que l'automatització de l'actuació exigeix una diligència particular en el procés de producció d'una decisió que ja no pren una persona, sinó un sistema programat adequadament. Si la qualitat i la seguretat del programari són importants en qualsevol aplicació, en el programari d'actuació automàtica són absolutament imprescindibles.

Recomanació 2.7. En la fase d'explotació, i en relació amb el manteniment del programari, cal implementar una funció de vigilància de les normes jurídiques que suporten actuacions automàtiques per detectar les derogacions amb temps suficient per actualitzar el sistema o, si s'escau, aturar-lo i evitar decisions automàtiques basades en normes derogades.

1.4.3. *Recomanacions especials sobre la viabilitat del sistema*

Recomanació 3.1. Les eines lògiques jurídiques (deòntica, refutable i descriptiva) ens poden ajudar a adquirir i formalitzar els coneixements jurídics de la norma a automatitzar, així com a establir mecanismes de validació, amb la finalitat de reduir els riscos inherents a l'actuació administrativa automatitzada.

En particular, l'ús d'una lògica modal híbrida, amb elements de lògica deòntica i refutable, molt especialment en el context de la lògica de l'acció, constitueix un element molt potent per obtenir una interpretació

objectiva i acurada dels aspectes estructurals de la norma i del seu comportament argumentador (la qual cosa permet una certa previsibilitat de les possibles aplicacions de la norma en cas de conflicte, sigui judicial o administratiu, en termes de procés).

D'altra banda, l'ús de la lògica descriptiva i de les ontologies ens permet un formalisme de representació del coneixement jurídic que actua com a base per al disseny d'aplicacions jurídiques avançades.

Recomanació 3.2. L'aplicació que permet l'actuació administrativa automatitzada és una aplicació d'informàtica jurídica de decisió. Aquesta aplicació s'ha de basar intensament en l'anàlisi lògica de les proposicions normatives, tot i que cada Administració pública tindrà la potestat de decidir el llenguatge que s'hi ha d'aplicar.

Mentre que en alguns casos s'optarà per una aproximació de sistema expert (basat en una representació plena del coneixement del domini jurídic involucrat) i l'ús de llenguatges de programació lògica capaços de decidir en temps d'execució, en la majoria de casos existirà una primera fase d'anàlisi i disseny de l'aplicació que hauria de considerar les eines de formalització i d'interpretació lògica indicades a la recomanació anterior. Posteriorment es codificarà un programa emprant llenguatges i mètodes de computació tradicionals, sovint obeint a criteris d'eficiència computacional i de cost.

Recomanació 3.3. La interpretació lògica pot quedar formalitzada en diversos moments al llarg del cicle de vida del programari que ofereix suport a l'actuació administrativa automatitzada:

- Una primera possibilitat és realitzar i formalitzar la interpretació lògica en la fase d'anàlisi funcional i disseny del programari. En aquest cas, la interpretació és un procés dut a terme per un intèrpret humà. El procés generarà un conjunt de casos que més tard han de servir per codificar informàticament el tractament d'aquests casos (la funcionalitat del programa que permet l'actuació administrativa automatitzada).

- Una segona possibilitat, complementària de l'anterior, consisteix a realitzar i formalitzar la interpretació lògica en el moment de construir el programari i, en concret, en el procés de codificació informàtica. Novament la interpretació es un procés dut a terme per un intèrpret humà, però en el mateix moment de produir el codi del programa.

- Una tercera possibilitat és realitzar i formalitzar la interpretació

lògica en forma de regles a aplicar en el moment d'execució del programa, sense que en el codi del programa es trobi cap lògica de funcionament de l'aplicació. Constitueix un exemple d'aquesta tercera possibilitat l'anomenada *programació lògica*, basada en l'ús de programes raonadors, com succeeix en els anomenats *sistemes experts* i, més recentment, en la Web semàntica. Caldrà avaluar amb molta cura aquesta possibilitat, ja que aquestes tècniques presenten problemes de rendiment.

- Una quarta possibilitat és dissenyar el sistema de tal manera que sigui ell mateix qui generi, a partir de la lectura i la comprensió de la norma jurídica, tant la representació del coneixement jurídic com les regles d'inferència lògica necessàries per aplicar les normes. Només en aquest cas podríem considerar que existeix una veritable interpretació per part de la màquina, que, malgrat el volum d'experiències realitzades, especialment en el domini de la recerca de textos jurídics, no considerem practicable en l'actualitat i per, tant, no recomanem.

- D'altra banda, s'ha de considerar la utilitat d'aquestes eines en els processos de verificació del programari produït. Efectivament, una de les possibilitats més interessants que ofereixen les eines lògiques que hem presentat és, precisament, la possibilitat d'avaluar formalment el programa que ofereix suport a l'actuació administrativa automatitzada, de forma integrada durant el procés de construcció o com a procediment d'avaluació de la idoneïtat del programa en moments posteriors, durant el procés natural de manteniment del programa, que en aquest cas esdevé particularment rellevant pel fet que el sistema experimentarà ordinàriament l'impacte dels canvis normatius.

1.4.4. *Recomanacions sobre signatura electrònica*

Recomanació 4.1. Analitzar detalladament els requisits de signatura de l'aplicació en termes d'autenticitat, integritat i confidencialitat. Per exemple, amb la metodologia PADS desenvolupada per l'Agència Catalana de Certificació, una eina dissenyada específicament per analitzar els requisits en relació amb els actes documentats que es produeixen dins els processos i els procediments de l'Administració i els seus organismes i entitats, públics o privats.

Recomanació 4.2. Definir una normativa de signatura electrònica que determini com s'ha de

generar la signatura dels actes automàtics, amb quins certificats, quins controls s'aplicaran per verificar els permisos i els privilegis, si la signatura se segellarà amb la data i l'hora, de quina manera es verificaran els certificats, quins algorismes es podran emprar per signar i, molt especialment, què vol dir legalment l'acte de signar i quins controls de programari s'aplicaran per garantir l'autenticitat de la voluntat del signatari.

Recomanació 4.3. Desplegar la normativa de signatura electrònica en forma d'estàndards tècnics de nivells de signatura (alt, mitjà i baix), estàndards de signatura per als diferents tipus d'actes (resoldre, expedir una còpia, certificar, notificar, etc.), en guies de signatura (PDF, ODF, Word, WS, S/MIME, etc.) i procediments de signatura.

1.4.5. *Recomanacions sobre certificats de segell automàtic*

Recomanació 5.1. Analitzar detalladament els requisits de certificació de l'aplicació en termes d'autenticitat, integritat i confidencialitat. Per exemple, amb la metodologia PADS desenvolupada per l'Agència Catalana de Certificació, una eina dissenyada específicament per analitzar els requisits en relació amb els actes documentats que es produeixen dins els processos i els procediments de l'Administració i els seus organismes i entitats, públics o privats.

Recomanació 5.2. Emprar certificats de segell d'Administració pública, òrgan o entitat públic d'elevada qualitat i seguretat, preferiblement en maquinari criptogràfic amb la seguretat certificada, d'acord amb les normes ISO Common Criteria EAL4+ (amb un perfil de protecció adequat, com ara CEN 14167) o FIPS 140-2 nivell 3.

Recomanació 5.3. Emprar certificats de segell d'Administració pública, òrgan o entitat públic sense dades personals del titular de l'òrgan o càrrec, ja que aleshores només es podran fer servir mentre aquesta persona en mantingui la titularitat. L'actuació administrativa automàtica permet que el funcionament de l'òrgan, com a unitat administrativa, es pugui mantenir malgrat l'absència del titular, cosa que a parer nostre és un avantatge important d'aquesta figura legal.

Recomanació 5.4. Emprar un sistema basat en doble certificat de segell, de manera que la possible pèrdua d'un certificat de segell no impliqui l'aturada de l'operació del sistema d'actuació administrativa automatitzada.

Recomanació 5.5. Definir una normativa de certificació de clau pública que reculli les recomanacions anteriors i altres que l'Administració pública consideri

necessàries per tal de regular adequadament el cicle de vida dels certificats de segell, ja que la possibilitat de dur a terme l'actuació administrativa automatitzada depèn de la disponibilitat i l'operativitat dels certificats.

Recomanació 5.6. Desplegar la normativa de certificació de clau pública mitjançant estàndards de certificació, tipus de certificats a adquirir o admetre, procediments d'admissió de certificats, procediments d'adquisició de certificats i d'una base dades de certificats vàlids.

1.4.6. *Recomanacions sobre seguretat i auditoria*

Recomanació 6.1. Analitzar detalladament els casos d'ús de seguretat del sistema, incloent-hi almenys els següents:

- Casos d'ús d'autenticació dels actors i de la documentació gestionada pels sistemes.
- Casos d'ús de signatura electrònica de documentació pels actors.
- Casos d'ús de signatura electrònica de transport segur de missatges entre actors i sistemes, com ara en el cas de la missatgeria de serveis web entre sistemes remots.
- Casos d'ús d'arxiu de signatura electrònica.
- Casos d'ús associats a les evidències electròniques, incloent-hi els procediments judicials i administratius en paper.

Recomanació 6.2. Definir una normativa de seguretat criptogràfica que especifiqui les normes d'ús en relació amb la criptografia, incloent-hi estàndards per implementar-los a l'organització, ja que l'actuació administrativa automatitzada es basa en l'ús de la criptografia i, per tant, cal regular-ne l'ús de manera apropiada amb la legislació i les necessitats de l'Administració pública o l'entitat de dret públic.

Recomanació 6.3. Desplegar la normativa de seguretat criptogràfica mitjançant estàndards d'implementació d'infraestructura criptogràfica, estàndards i procediments en relació amb els algorismes segurs i guies d'ús de la criptografia en les aplicacions, amb recomanacions conformes a la legislació aplicable.

Recomanació 6.4. Definir una normativa de gestió de claus que detalli les normes d'ús en relació amb les claus criptogràfiques d'acord amb la normativa de seguretat criptogràfica, ja que l'actuació administrativa automatitzada es basa en l'ús de les claus criptogràfiques corresponents als certificats i,

per tant, són actius de l'Administració pública o l'entitat de dret públic que cal protegir adequadament.

Recomanació 6.5. Desplegar la normativa de gestió de claus mitjançant estàndards d'infraestructura tècnica de gestió de claus, procediments previs a les operacions de gestió de claus, procediments operatius de gestió de claus i procediments posteriors de gestió de claus.

Recomanació 6.6. Definir una normativa de desenvolupament segur aplicable a l'aplicació d'actuació administrativa automatitzada i a l'aplicació de signatura electrònica que hi dóna suport.

Recomanació 6.7. Implantar o ampliar la funció d'auditoria de qualitat i de seguretat a fi de vetllar per l'aplicació de les normatives i el desplegament corresponent. En particular, considerem imprescindible auditar l'aplicació del cicle de vida del programari (quan l'aplicació sigui de decisió), auditar el codi i, en tot cas, auditar l'aplicació de les mesures de seguretat i signatura electrònica.

2. ANÀLISI JURÍDICA GENERAL DE L'AUTOMATITZACIÓ DELS ACTES ADMINISTRATIUS

Aquest capítol tracta d'establir els requisits legals i de control tècnic necessaris per fer efectiva l'automatització dels tràmits en el marc del respecte a la legalitat vigent.

L'objectiu d'aquesta anàlisi és oferir criteris i controls legals i tecnològics inicials en relació amb la possibilitat de realitzar tràmits de manera automàtica i crear un marc de referència que aporti la seguretat jurídica necessària a aquesta nova possibilitat legal.

Primer de tot cal, doncs, diferenciar clarament els requisits o requeriments jurídics i tècnics.

2.1. Els requisits jurídics de l'actuació administrativa automatitzada

Pel que fa als requeriments jurídics, cal destacar la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics. D'acord amb la disposició final primera, aquesta Llei atribueix caràcter bàsic a una part significativa dels seus preceptes, a l'empara de l'article 149.1.18.a de la Constitució, que atribueix a l'Estat la competència sobre les bases del règim jurídic de les administracions públiques i sobre el procediment administratiu comú.

Aquesta Llei ha representat un avenç important pel que fa a la regulació de l'administració electrònica a l'Estat espanyol. El tret principal és que reconeix el dret dels ciutadans a relacionar-se amb les administracions públiques a través de mitjans electrònics i, correlativament, l'obligació de les administracions públiques de dotar-se de mitjans i sistemes electrònics per tal que aquest dret es pugui exercir. Tal com es reconeix a l'exposició de motius, «aquesta Llei pretén fer el pas del 'podran' a l''hauran de'». A més, la Llei estableix els principis que informen l'administració electrònica, regula els drets dels ciutadans, així com l'ús dels mitjans electrònics en relació amb diferents fases del procediment administratiu, i preveu els mecanismes de cooperació i col·laboració interadministrativa per a l'impuls de l'administració electrònica.

No obstant això, tot i l'ampli contingut, la Llei no determina un model específic d'administració electrònica, sinó que configura o enumera els elements bàsics que informen el procediment administratiu i defineix els trets bàsics d'aquesta regulació des de la vessant de garanties del ciutadà, de tal manera que concedeix a cadascuna de les administracions públiques la llibertat d'escollir les opcions que consideri més idònies a

l'hora de configurar un procediment administratiu. Sigui com sigui, això no podia ser d'una altra manera si es té en compte el seu caràcter bàsic, que no pot esgotar la capacitat normativa de la comunitat autònoma, sens perjudici del fet que, quan parlem de l'ús dels mitjans electrònics, existeix una important vessant autoorganitzativa, concretada en les decisions que adopta o pot adoptar cada Administració i que, en qualsevol cas, hauran de garantir uns drets bàsics dels ciutadans i un tractament administratiu comú.

La disposició final 3a.3 de la Llei 11/2007 estableix que, en l'àmbit de les comunitats autònomes, els drets dels ciutadans recollits a la mateixa Llei podran ser exercits a partir del 31 de desembre de 2009, sempre que les disponibilitats pressupostàries ho permetin.

Tal com hem indicat, una part significativa de la Llei 11/2007 té caràcter bàsic, malgrat que justament la previsió de l'article 39 no en té, cosa que, en principi, permetria que les comunitats autònomes, en desenvolupament de polítiques pròpies, incorporessin requeriments diferents dels establerts legalment a la Llei 11/2007. Tanmateix, podem avançar que difícilment es podrà establir un nivell de garanties inferiors a les que preveu aquell article, perquè altrament la seguretat jurídica en podria sortir malparada.

En aquest sentit, cal recordar el tenor literal de l'article 39 de la Llei 11/2007: «En cas d'actuació automatitzada s'ha d'establir prèviament l'òrgan o òrgans competents, segons els casos, per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema d'informació i del seu codi font. Així mateix, s'ha d'indicar l'òrgan que ha de ser considerat responsable als efectes d'impugnació.»

Tot i mancar de caràcter bàsic, aquest article ja ens dóna els trets bàsics que cal considerar respecte a l'automatització de processos, els quals hauran de ser tractats tant des de la vessant normativa com des de la vessant tècnica.

Des de la vessant normativa, s'han d'analitzar diferents elements enumerats a la norma no com a mínim normatiu comú des del punt de vista bàsic, però sí des del punt de vista material o pràctic: la competència de l'òrgan, que estendrà la seva actuació en relació amb la definició de les especificacions tècniques o els programes que han de donar resposta a una actuació administrativa determinada.

Aquesta competència que es configura des del punt de vista inicial o primari també haurà de verificar o assegurar el manteniment o la supervisió d'aquests programes i aplicacions a l'efecte d'assegurar la qualitat o garantir que no es pugui produir un mal funcionament. Cal remarcar que, en definitiva, un mal funcionament derivaria en una actuació administrativa irregular susceptible de donar lloc a un supòsit de nul·litat de ple dret o

d'anul·labilitat (si bé també ens podríem trobar davant una mera irregularitat no invalidant, en funció dels casos).

Finalment, com a garantia essencial del procediment administratiu comú trobem el dret de revisió dels actes administratius, regulat als articles 102 i següents de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú.

Aquest dret de revisió implica la capacitat que té l'administrat o l'administrada de reaccionar davant qualsevol actuació administrativa que l'afecta amb la finalitat d'evitar situacions d'indefensió material que anirien en contra de la tutela judicial efectiva garantida per l'article 24 de la Constitució espanyola. Aquesta reacció es pot produir dins el procediment administratiu mateix, mitjançant els recursos establerts legalment (sens perjudici de la possibilitat de revisió d'ofici dels actes administratius que pot dur a terme l'Administració quan es donen els supòsits establerts legalment), o ja en la via judicial, mitjançant el control que duen a terme els tribunals de justícia de la legalitat de l'actuació administrativa (tal com regula l'article 106 de la Constitució).

Quan ens trobem davant l'actuació administrativa automatitzada, aquesta reacció del particular pot assolir dues vies d'impugnació: per raons formals o per raons materials o de fons.

La diferenciació quant a les vies d'impugnació es produeix també en l'àmbit del procediment administratiu considerat tradicionalment, tot i que quan parlem d'actuació administrativa automatitzada s'ha de tenir present que, si bé les raons d'impugnació per raons materials sempre seran les mateixes —tant si es tracta d'una actuació administrativa automatitzada com si no—,[4] en el cas de l'actuació administrativa automatitzada la impugnació per raons formals és substancialment diferent. El motiu és que en la mesura que aquesta impugnació se centra en l'adequació a l'ordenament jurídic o la regularitat formal de l'actuació administrativa, caldrà analitzar justament si l'automatització dels processos s'ha dut a terme de manera correcta, cosa que suposarà avaluar, en primer lloc, la possibilitat que aquesta automatització o eliminació de la voluntat humana sigui factible, i, en segon lloc, si les aplicacions o els programes han estat configurats adequadament.

[4] Cal tenir present que l'actuació administrativa automatitzada no produeix sinó un acte administratiu, configurat com a declaració de voluntat, de coneixement, de judici o de desig, que es troba sotmès a uns requisits de validesa material i d'eficàcia que són els mateixos tant si ens trobem davant actes administratius de naturalesa presencial com realitzats per mitjans electrònics, i, per aquest motiu, la seva impugnació en aquest àmbit ho seria sempre per les mateixes raons materials o de fons.

2.1.1. *L'actuació administrativa automatitzada i la programació d'aquesta actuació*

Pel que fa a la voluntat humana, o la declaració de voluntat, ja hem comentat que, en el cas de l'actuació administrativa automatitzada, la seva formulació es trasllada a l'aplicació corresponent. Tanmateix, això no significa que aquella desaparegui, perquè la declaració de voluntat emanada existeix igualment, si bé es trasllada a un moment temporal anterior, que és el de la programació d'acord amb criteris que es podrien anomenar *de lògica jurídica*. L'annex de la Llei 11/2007 ho reconeix d'aquesta manera quan defineix l'aplicació com el «programa o conjunt de programes l'objecte dels quals és la resolució d'un problema mitjançant l'ús d'informàtica».

Malgrat que s'ha de reconèixer que la utilització del terme *problema* no és gaire encertada, descriu clarament quina és la finalitat d'una aplicació: oferir una solució tècnica a un plantejament jurídic; és a dir, establir una programació determinada que garanteixi que l'emissió d'un acte administratiu concret compleix els requeriments materials de contingut que l'acte administratiu corresponent ha de garantir.

En definitiva, es tracta de traslladar al camp de la programació informàtica els elements subjectius, objectius i formals que integren l'acte administratiu corresponent i garantir que l'acte administratiu respon a la mateixa finalitat que la que correspondria al mateix acte administratiu provinent d'una voluntat humana.

Seguint García de Enterría, diferenciarem cadascun dels elements:

1) Element subjectiu. L'acte administratiu ha de procedir del titular apte de l'òrgan competent de l'Administració pública competent, per la qual cosa exigeix alhora tres requisits:

    a. Que procedeixi d'una entitat de dret públic amb capacitat i competència per dictar-lo.
    b. Que procedeixi d'un òrgan competent objectivament, funcionalment i territorialment per dictar-lo. Així, l'article 62.1 de la Llei 30/1992 disposa el següent: «Els actes de les administracions públiques són nuls de ple dret en els casos següents: [...] Els que dicti un òrgan manifestament incompetent per raó de la matèria o del territori.»
    c. Aptitud del titular de l'òrgan davant l'òrgan (quan el titular hi ha estat adscrit) i davant les parts interessades (sempre que no concorri cap motiu d'abstenció de l'article 28.2 de la Llei 30/1992).

2) Element objectiu. El contingut de l'acte administratiu ha de ser, com qualsevol acte jurídic:

a. Possible i lícit o ajustat a l'ordenament jurídic. Per això, segons l'article 62, són nuls: «*c*) Els que tinguin un contingut impossible. *d*) Els que siguin constitutius d'infracció penal o es dictin com a conseqüència d'aquesta.»
b. Determinat o determinable.
c. Adequat als fins que persegueix i ajustat a l'ordenament jurídic.

3) Element causal. L'integren dos elements:

   a. La constatació del pressupòsit de fet que justifica que l'acte es dicti.
   b. La causa en sentit estricte, que és l'adequació o la congruència de l'acte amb el fi que en ell es persegueix.

4) Element teleològic, de manera que si l'Administració exercita la potestat per a un fi diferent del predeterminat pel dret parlarem d'*arbitrarietat* o de *desviació de poder*.

Pràcticament tots aquests elements són traslladables a l'automatització de processos, si bé cadascun s'ha de diferenciar a l'hora de tractar l'automatització.

Pel que fa als elements subjectius, relacionats amb el concepte d'òrgan administratiu, hem d'enfocar la qüestió des de la vessant del principi de legalitat i la doctrina de les potestats administratives, tal com tractarem de forma separada.

Contràriament, els elements objectius són els que, en la mesura que es refereixen al contingut de l'acte administratiu, han de derivar del que hagi estat objecte de programació.

Certament, la programació o l'adequació d'un procediment administratiu determinat a l'actuació automatitzada haurà d'incloure tant l'element subjectiu com l'element objectiu. Malgrat això, mentre que l'element subjectiu és una qüestió prèvia que està predeterminada i que es podria considerar que no varia, l'element objectiu es produirà cada vegada que s'emeti l'acte administratiu, i el seu contingut no es pot trobar predeterminat, sinó que serà conseqüència dels paràmetres introduïts per a la seva producció.

Per la seva banda, els elements causal i teleològic concorren igualment en qualsevol acte administratiu. El seu reflex en l'actuació administrativa automatitzada es produeix també en l'àmbit de programació, en la mesura que aquesta ha de respondre a una finalitat pròpia i específica de l'acte administratiu concret. A més, l'element teleològic es configura pel principi segons el qual qualsevol actuació administrativa ha de respondre a raons

d'interès general. Per tant, qualsevol vulneració informàtica d'aquests dos elements podria suposar incórrer en una desviació de poder.

En aquest sentit, tan sols una programació adequada pot permetre que la producció de l'acte corresponent respecti les garanties formals i materials necessàries i sigui, consegüentment, vàlid.

L'article 44.2 de la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, indica que «Només són susceptibles d'actuació administrativa automatitzada els actes que es puguin adoptar amb una programació basada en criteris i paràmetres objectius». Amb aquesta previsió es pretén, d'una banda, delimitar l'àmbit de l'automatització a aquests supòsits en què es puguin predeterminar les condicions de realització de l'acte de manera objectiva i, de l'altra, configurar aquesta programació com el paràmetre de legalitat a controlar, el que és rellevant a l'hora de valorar i, si escau, revisar l'actuació administrativa feta a partir d'aquesta programació.

2.1.2. *El control de l'actuació administrativa automatitzada*

És evident que el principi de validesa dels actes administratius es pot traslladar a l'actuació administrativa automatitzada, i que el control d'aquesta actuació administrativa passarà pel control d'una programació adequada. Es tracta de discernir si la informàtica decisional que configura l'acte administratiu produeix un acte administratiu de manera apropiada.

Aquest seria el control que es podria anomenar *natural* de l'acte administratiu, si bé cal afegir-n'hi un altre que es podria denominar *control previ* i que es relaciona amb el principi de legalitat i la doctrina de les potestats administratives.

2.1.3. *La doctrina de les potestats administratives*

El concepte de *potestat* fou elaborat en contrast amb el concepte de *dret subjectiu* dins la categoria genèrica dels poders jurídics o facultats d'obrar atribuïts per l'ordenament jurídic als subjectes respecte a interessos o béns protegits per aquest ordenament.

Així, a diferència del dret subjectiu, la potestat:

1) No deriva d'una relació jurídica, sinó directament de l'ordenament jurídic.
2) No recau sobre cap objecte determinat, sinó que té un caràcter genèric.

3) No es tradueix en una pretensió concreta, sinó en una possibilitat abstracta de produir efectes jurídics.
4) Es correspon amb una situació de submissió d'altres subjectes als eventuals efectes jurídics derivats de l'exercici de la potestat.
5) No s'atribueix en benefici del seu titular, sinó de terceres persones, ja que l'Administració ha d'exercitar les seves potestats per perseguir l'interès públic. Per aquest motiu, les potestats administratives són potestats-funció, la qual cosa exclou poders absoluts.

Segons Garrido Falla, la potestat administrativa es pot definir com un poder d'actuació genèric que, exercit d'acord amb les normes jurídiques, produeix situacions jurídiques en què quedaran obligats subjectes que, amb anterioritat, estaven simplement en una situació abstracta de submissió.

En qualsevol cas, per tal que l'Administració pugui exercitar qualsevol potestat cal que prèviament li hagi estat atribuïda per llei amb caràcter exprés i específic.

No obstant això, l'exigència de caràcter exprés s'ha de matisar amb la doctrina dels poders implícits o inherents del dret anglosaxó, d'acord amb la qual encara que no s'atorguin expressament per la llei, s'han d'entendre atribuïts aquells poders que siguin implicació necessària dels que s'atorguin expressament.

Quant al principi de legalitat com a pilar fonamental de l'estat de dret, cal dir que es caracteritza no tan sols pel reconeixement i la tutela dels drets públics subjectius dels ciutadans, sinó també per la forma en què aquest objectiu s'assoleix: mitjançant el submissió de l'Administració a la llei, que constitueix el principi de legalitat i es formulà inicialment concebent la llei com a font i justificació de totes les actuacions dels poders executiu i judicial.

La formulació inicial del principi de legalitat construïda entorn de l'exigència de la llei prèvia partia de dues justificacions ben clares:

1) En primer lloc, una de general basada en la idea roussoniana que la legitimitat del poder procedeix de la voluntat comunitària l'expressió típica de la qual és la llei.

2) En segon lloc, el principi tècnic de la divisió de poders, pel qual l'executiu té com a missió executar la llei dictada pel legislatiu.

Com indica Muñoz Machado,[5] el legislador no és plenament lliure a l'hora de decidir el grau de predeterminació amb què ha d'utilitzar les potestats administratives pel fet que es requereix una densitat normativa mínima que, en determinades matèries, resta reservada a la llei. Això es produeix perquè el legislador no pot deixar totalment obertes les seves decisions a fi que l'Administració les completi o les concreti, atès que això significaria el trencament de la reserva de llei, que exigeix que la llei reguli amb densitat suficient les qüestions principals que suscita la matèria reservada.

Així doncs, una regulació insuficient trencaria el principi de seguretat jurídica, la certesa que tal principi imposa a les normes, la previsibilitat de les conseqüències de la regulació, la igualtat de tracte davant situacions reiterades que siguin susceptibles de tractament igual, i la confiança legítima.

A l'hora d'analitzar la doctrina de la potestat administrativa, a la fase 1 ja vam avançar que és essencial distingir les potestats reglades de les potestats discrecionals.

2.1.4. *Les potestats reglades i les potestats discrecionals*

La llei pot determinar totes i cadascuna de les condicions d'exercici de la potestat o bé pot definir alguna de les condicions d'exercici de la potestat i deixar a l'estimació subjectiva de l'Administració la resta de condicions (el com, el quan i el sentit).

Això ens porta a distingir les potestats reglades de les discrecionals.

En relació amb la discrecionalitat, s'han formulat dues teories:

1) Teoria de la vinculació negativa, segons la qual s'entén permès a l'Administració allò que la llei no li prohibeix. D'aquesta manera, hi ha un "espai lliure de llei" en el qual l'Administració opera discrecionalment; per això l'activitat administrativa discrecional es desenvoluparia sempre fora de la llei i seria, per tant, incontrolable pels tribunals.

2) Teoria de la vinculació positiva, d'acord amb la qual s'entén prohibit a l'Administració el que no està permès per la llei, de manera que tota l'activitat administrativa ha d'estar coberta pel dret. Així, l'activitat discrecional es desenvoluparà sempre dins de la llei. No hi ha, doncs, discrecionalitat al marge de la llei, sinó només en virtut de llei i en la mesura que la llei ho hagi disposat.

[5] Muñoz Machado, S. *Tratado de derecho administrativo y derecho público general I*. Madrid: Ed. Iustel, 2a edició, 2006, pàg.

Aquesta darrera és la teoria que ha estat reconeguda majoritàriament en l'àmbit doctrinal i que s'empararia en l'article 9 de la Constitució, que adverteix que aquesta garanteix el principi de legalitat i la interdicció de l'arbitrarietat dels poders públics.

L'exposició de motius de la Llei de la jurisdicció contenciosa administrativa de 1956 consignava el tret bàsic de la discrecionalitat: «la discrecionalitat sorgeix quan l'ordenament jurídic atribueix a algun òrgan la competència per apreciar en un supòsit donat allò que sigui d'interès general».

Per tant, la discrecionalitat apareix per autorització legal. Per aquest motiu, en qualsevol acte discrecional existeixen uns elements reglats que actuen com a límits, i que són els següents:

1) L'existència i l'extensió de la potestat.
2) La competència.
3) La forma.
4) El procediment.
5) La finalitat a perseguir en l'actuació administrativa.
6) Els supòsits fàctics o de fet.
7) Els principis generals del dret.

2.1.5. *L'automatització de processos*

D'acord amb el que hem exposat, i traslladant aquestes reflexions a l'actuació administrativa automatitzada, es pot parlar de discrecionalitat en un doble sentit: amb caràcter previ i en relació amb els actes administratius discrecionals que puguin ser automatitzats.

La discrecionalitat prèvia suposa que, de la mateixa manera que l'Administració pot determinar, en el marc de la llei, quins procediments es poden tramitar electrònicament i, fins i tot, a l'empara de la previsió de l'article 27.6 de la Llei 11/2007, es pot imposar obligatòriament la realització d'aquests procediments per mitjans electrònics,[6]

519.

[6] Cal recordar que l'apartat 4 de l'article 26 indica que «Per reglament, les administracions públiques poden establir l'obligatorietat de comunicar-se amb aquestes utilitzant només mitjans electrònics, quan els interessats es corresponguin amb persones jurídiques o col·lectius de persones físiques que amb motiu de la seva capacitat econòmica o tècnica, dedicació professional o altres motius acreditats tinguin garantit l'accés i la disponibilitat dels mitjans tecnològics necessaris», previsió que, en l'àmbit de l'Administració de la Generalitat, ha concretat l'article 13 del Decret 56/2009, que, sota la rúbrica «Obligatorietat en l'ús dels mitjans electrònics», indica el següent: «Mitjançant ordre del conseller o consellera competent en la matèria es pot imposar, per causes objectives justificades, a les persones jurídiques, públiques o privades o col·lectius de persones físiques, l'obligació d'utilitzar només mitjans electrònics per a la comunicació amb els ens previstos a la lletra a) de l'article 2.1, sempre que per raó de la seva capacitat econòmica o tècnica, dedicació professional o altres motius acreditats tinguin garantits l'accés i la disponibilitat dels mitjans electrònics necessaris.»

l'Administració corresponent pot determinar discrecionalment quins actes administratius són susceptibles d'automatització.

Si tornem a l'annex de la Llei 11/2007, observem que defineix l'actuació administrativa automatitzada com aquella «actuació administrativa produïda per un sistema d'informació adequadament programat sense necessitat d'intervenció d'una persona física en cada cas singular. Inclou la producció d'actes de tràmit o resolutoris de procediments, així com de mers actes de comunicació».

D'aquest concepte, en podem extreure dues conclusions: en primer lloc, la supressió de la intervenció de la persona física en l'actuació administrativa materialment considerada, i, en segon lloc, el concepte omnicomprensiu que es conté a la definició.

Això significa que l'Administració disposa de la potestat discrecional d'automatitzar els processos en el marc de la normativa vigent.

2.1.6. *El marc normatiu en relació amb l'automatització de processos*

La normativa vigent conté una norma habilitadora genèrica, configurada per l'article 39 de la Llei 11/2007, que, pel que fa a l'Administració de la Generalitat, ha estat desplegada per l'article 34 del Decret 56/2009.[7] És a l'empara d'aquesta habilitació legal que es pot procedir a l'automatització de processos.

Igualment, l'article 44.1 de la Llei 26/2010 indica que «Les administracions públiques catalanes poden fer actuacions automatitzades per a constatar la concurrència dels requisits que estableix l'ordenament jurídic, declarar les conseqüències previstes, adoptar les resolucions i comunicar o certificar les dades, els actes, les resolucions o els acords que constin en llurs sistemes d'informació, mitjançant la utilització del sistema de signatura electrònica que determinin».

De conformitat amb aquest marc normatiu, estatal i autonòmic, ens trobem amb un nivell de regulació doble: la normativa estatal, que es pot considerar merament possibilitadora d'aquesta automatització, i la normativa autonòmica. Per aquesta raó és necessari un desplegament efectiu en què es concretin les condicions d'exercici, ja sigui

[7] Aquest article 34 indica: «L'exercici de la competència mitjançant l'actuació administrativa automatitzada.
1. Els ens previstos a la lletra a) de l'article 2.1 han d'impulsar l'automatització dels processos que per les seves característiques i per raons d'eficiència ho justifiquin, sense que es produeixi cap reducció de garanties de l'administrat o l'administrada i, si escau, determinant l'òrgan responsable a l'efecte d'impugnació.
2. El departament competent en matèria d'administració electrònica, amb la col·laboració del Centre de Telecomunicacions i Tecnologies de la Informació, estableix els requeriments tècnics i formals dels sistemes que automatitzin l'actuació administrativa. Així mateix, determina els criteris de programació, manteniment, supervisió i control de qualitat d'aquests sistemes.»

amb normes de caràcter reglamentari, ja sigui amb normes que, amb rang de llei, desenvolupin polítiques pròpies.

Això és el que ha fet l'Administració de la Generalitat de Catalunya, amb l'article 44 de la Llei 26/2010 i la previsió reglamentària esmentada abans, sens perjudici del fet que, tal com es desprèn de l'anàlisi del mateix Decret, aquest hagi adoptat una fórmula que es pot considerar nova a l'hora d'enfocar les solucions tècniques, la qual passa per la desreglamentació formal dels aspectes tècnics.

La regulació que es fa al Decret 56/2009 recolza en una concepció innovadora en la mesura que es despleguen, amb rang reglamentari, els aspectes bàsics que cal considerar a l'hora d'implementar o incorporar la tramitació electrònica al procediment administratiu.

No obstant això, es produeix una descàrrega dels aspectes més tècnics i canviants. Aquests es remeten a uns protocols que, en cadascun dels seus àmbits, són aprovats pels titulars dels departaments corresponents i objecte de publicació a la seu corporativa.[8]

La voluntat de la regulació és evitar una reglamentació excessiva sense que es produeixin problemes de seguretat jurídica. Aquest objectiu es vol assolir no tan sols amb la transparència derivada de la publicitat a la seu corporativa dels protocols corresponents, sinó també mitjançant un procediment d'elaboració en què es garanteix la intervenció d'un òrgan corporatiu competent en matèria de recursos comuns dels departaments, la Comissió de Coordinació Corporativa, regulada pel Decret 146/2007. La finalitat és que, en àmbits com els que són objecte de regulació en el Projecte de decret objecte d'informe, les solucions adoptades es puguin aplicar o traslladar al conjunt dels organismes de l'Administració de la Generalitat.

Com hem indicat, l'aprovació d'aquests protocols la duu a terme cadascun dels departaments competents per raó de la matèria: atenció ciutadana, administració electrònica, arxius. Pel que fa a l'actuació administrativa automatitzada, es preveu igualment que el Departament competent en matèria d'administració electrònica estableixi els requeriments tècnics i formals dels sistemes que automatitzin l'actuació administrativa, així com els criteris de programació, manteniment, supervisió i control de qualitat dels sistemes.

Respecte a aquesta desreglamentació, la Comissió Jurídica Assessora, en el Dictamen 22/2009, emès en relació amb el Projecte de decret, va matisar aquests protocols indicant el següent: «Apareix així un tercer nivell normatiu que, atesa la complexitat tecnològica de la matèria, hauria de complir la funció d'establir les normes i els

[8] Es tracta dels protocols de tràmits i serveis, el protocol d'interoperabilitat, el protocol de signatura i el protocol d'arxius.

procediments més tècnics que possibilitessin l'ús dels mitjans electrònics en el sector públic. Tanmateix, no és aquesta l'única comesa dels protocols, o, almenys, no es dedueix clarament de les diferents remissions del Projecte; i, en ocasions, aquests protocols semblen, més aviat, estar cridats a regular fins i tot àmbits reservats a la llei [...] En conseqüència, aquesta Comissió ha de concloure, formulant l'observació amb caràcter essencial, que hi ha la necessitat que, en el Projecte, d'una banda, es clarifiqui la naturalesa normativa d'aquests protocols i s'assenyali si són aprovats o no mitjançant un reglament en els termes previstos en l'article 40.1 de la Llei 13/2008, de 5 de novembre, de la Presidència de la Generalitat i del Govem. («Les disposicions reglamentàries dictades pel Govem o pel president o presidenta de la Generalitat adopten forma de decret. Les disposicions reglamentàries dictades pels consellers adopten forma d'ordre.») En aquest sentit, una acurada definició clara i segura del concepte, naturalesa, procediment i abast del protocol com a instrument d'intervenció, ja sigui en el cos del text o en el glossari a què s'al·ludeix al final del fonament jurídic següent, pot contribuir a aclarir els dubtes que la seva previsió suscita.

D'altra banda, i en la mesura que no existeix una llei prèvia, cal delimitar més acuradament el contingut de cadascun d'aquests protocols per tal que aquest se cenyeixi a regular els aspectes més tècnics de l'ús dels mitjans electrònics en cadascun dels àmbits sobre els quals es projecten, això és, els criteris operatius d'actuació (art. 6.3), i que se'ls impossibiliti, amb això, a suplir funcionament i materialment els àmbits propis de la llei.»

Segons això, la Comissió Jurídica Assessora admet la viabilitat jurídica dels protocols esmentats, si bé sotmet aquesta possibilitat a un condicionant doble:

- D'una banda, els protocols s'han de cenyir, en el seu contingut, a la regulació d'aspectes tècnics i organitzatius.
- D'altra banda, caldria delimitar-ne la naturalesa jurídica i admetre la consideració d'aquests protocols com a disposicions de caràcter general.

En aquest sentit, incorporant les previsions de la Comissió Jurídica Assessora, es van introduir unes modificacions en el text del Projecte que delimitaven el concepte i el contingut d'aquests protocols i en determinaven la naturalesa jurídica.

Aquest marc es pot traslladar igualment a l'automatització de processos en la mesura que, a l'empara d'una previsió legal habilitadora, de caràcter estatal o autonòmic, i una habilitació reglamentària, es pot dur a terme l'automatització de processos en el marc legal establert, sense que sigui necessari que tots els elements tècnics estiguin recollits a les normes esmentades anteriorment. Tanmateix, sí que caldrà que un instrument normatiu de nivell inferior reculli o reguli aquests aspectes tècnics o de detall que, per la

seva naturalesa, no és recomanable que s'incloguin en una norma legal o reglamentària —la qual, per la seva naturalesa, és molt més difícil d'adaptar o adequar a les circumstàncies tècniques que vagin variant.

Aquestes mateixes reflexions es podrien traslladar a l'àmbit local, en què la potestat reglamentària manifestada mitjançant l'aprovació de les ordenances locals és expressió de la potestat normativa que caracteritza igualment aquests ens locals territorials. D'acord amb això, serien les ordenances corresponents les que podrien concretar, en un primer nivell, les condicions en què l'automatització de processos seria viable des del punt de vista jurídic, sempre a l'empara de la previsió legal corresponent, ja sigui la de l'article 39 de la Llei 11/2007, ja sigui la de la norma legal autonòmica corresponent. En un segon nivell hi hauria instruments normatius de rang inferior (com podria ser un decret d'alcaldia) que podrien contenir els elements tècnics i organitzatius mutables.

Aquesta possibilitat que sigui una norma autonòmica la que concreti amb rang legal les condicions d'automatització deriva del caràcter no bàsic de l'article 39 de la Llei 11/2007, sens perjudici de la necessària reserva de llei que existeix en la matèria, ja que, segons els articles 103.1 i 2 de la Constitució, les decisions organitzatives s'han d'adoptar d'acord amb una llei. D'altra banda, com preveu l'article 84 de l'Estatut d'autonomia de Catalunya, també les lleis són les que estableixen les competències pròpies dels ens locals.

En definitiva, la regulació de l'ús de mitjans electrònics davant l'Administració requereix una llei que estableixi el primer marc normatiu, el qual dota d'estabilitat i de previsibilitat les normes inferiors que l'han d'executar, a més de complir amb les reserves funcionals i materials exigides. En efecte, ja s'ha dit que l'ordenament jurídic exigeix, per a una regulació completa i estable d'aquesta matèria, una llei prèvia, la qual és la cridada a perfilar les bases del model d'administració electrònica a aplicar, a desenvolupar el contingut i l'exercici dels drets dels ciutadans en la relació amb l'Administració i a vincular, si fos el cas, amb obligacions concretes, les administracions locals quant a l'ús de mitjans electrònics en les seves relacions internes i les comunicacions recíproques amb altres administracions.

Aquesta funció és la que desenvolupa la Llei 11/2007, sens perjudici que les comunitats autònomes, com és el cas de Catalunya, a l'empara de la previsió de l'article 111 de l'Estatut d'autonomia,[9] pugui desenvolupar polítiques pròpies i, fins i tot, establir-les com a aplicables en relació amb totes les administracions públiques catalanes.

[9] «En les matèries que l'Estatut atribueix a la Generalitat de forma compartida amb l'Estat, corresponen a la Generalitat la potestat legislativa, la potestat reglamentària i la funció executiva, en el marc de les bases que fixi l'Estat com a principis o mínim comú normatiu en normes amb rang de llei, excepte en els supòsits que es determinin d'acord amb la Constitució i amb aquest Estatut. En exercici d'aquestes competències, la Generalitat pot establir polítiques pròpies. El Parlament ha de desplegar i concretar per mitjà d'una llei les dites disposicions bàsiques.»

En qualsevol cas, aquesta extensió de la norma no és il·limitada, sinó que resta condicionada a una sèrie de límits, un dels quals és el de l'autonomia local.[10]

El principi constitucional d'autonomia implica que els municipis i les províncies han de tenir un mínim de competències que es pot considerar irreductible en la mesura que, si bé es poden reordenar, no poden ser eliminades completament (STC 32/1981, FJ 3r). A més, «*esa reordenación no puede afectar al contenido competencial mínimo* [...] *garantizado como imperativo de la autonomía local*» [STC 214/1989, FJ 4t b)]. En aquest sentit, «*el legislador puede disminuir o acrecentar las competencias hoy existentes, pero no eliminarlas por entero, y, lo que es más, el debilitamiento de su contenido sólo puede hacerse con razón suficiente y nunca en daño del principio de autonomía*» [STC 32/1981, FJ 3r; STC 214/1989, FJ 13 c)].

La STC 32/1981 ja va establir una doctrina que el Tribunal Constitucional ha recollit reiteradament en pronunciaments posteriors: «*Como titulares de un derecho a la autonomía constitucionalmente garantizada, las comunidades locales no pueden ser dejadas en lo que toca a la definición de sus competencias y la configuración de sus órganos de gobierno a la interpretación que cada comunidad autónoma pueda hacer de ese derecho* [...] *La garantía constitucional es de carácter general y configuradora de un modelo de Estado, y ello conduce, como consecuencia obligada, a entender que corresponde al mismo la fijación de principios o criterios básicos en materia de organización y competencia de general aplicación en todo el Estado.*»

Tanmateix, la normativa estatal bàsica, per aplicació de l'article 149.1.18 CE, s'articula en relació amb dos elements fonamentals que integren aquesta garantia institucional, que són l'estructura organitzativa i el règim de competències. En definitiva, com assenyala reiteradament el Tribunal Constitucional, el que és materialment bàsic són totes aquelles qüestions relacionades amb l'autonomia consagrada constitucionalment, és a dir, estructura orgànica i, especialment, competencial de les entitats locals.

Així mateix, com aprecia la STC 27/1987, l'autonomia local no impedeix establir fórmules de relació interadministrativa que comportin la coordinació dels ens locals en l'àmbit autonòmic que, sense menyscabar les competències de les entitats locals, suposin un límit d'aquestes quan es fixin mitjans o sistemes de relació que facin possible la informació recíproca, l'homogeneïtat tècnica en determinats aspectes i l'acció conjunta i, en definitiva, s'evitin contradiccions i es redueixin disfuncions. Per aquesta raó, la

[10] Cal recordar que l'article 159.2 de l'Estatut d'autonomia de Catalunya atribueix a la Generalitat la competència compartida en matèria de règim jurídic i procediment de les administracions públiques catalanes i, d'acord amb l'apartat 6 del mateix article, les competències de la Generalitat especificades als apartats 1, 3, 4 i 5 s'han d'exercir respectant el principi d'autonomia local.

coordinació pot constituir igualment un límit al ple exercici de les competències pròpies de les corporacions locals.

Traslladant aquests principis a l'àmbit de l'administració electrònica i, en particular, a l'actuació administrativa automatitzada, hem de concloure que cada Administració pública —estatal, autonòmica o local— ha de tenir un marge d'autonomia ampli a l'hora de configurar els criteris d'automatització i, amb rang de llei, els únics límits a establir serien aquells que facin possible l'homogeneïtat tècnica en determinats aspectes i la interoperabilitat.

2.1.7. *Els drets dels ciutadans com a límit de l'automatització*

Naturalment, hi ha altres límits que s'han de respectar, com ara els drets que reconeix l'ordenament jurídic als ciutadans en les seves relacions amb les administracions públiques. Respecte a aquests drets, la Llei 11/2007 recull, a l'article 4, dins els principis generals, el «principi de legalitat quant al manteniment de la integritat de les garanties jurídiques dels ciutadans davant les administracions públiques establertes a la Llei 30/1992, de règim jurídic de les administracions públiques i del procediment administratiu comú», cosa que comporta una reserva de llei pel que fa al manteniment d'aquestes garanties de què ha de gaudir la ciutadania.

S'hi han d'afegir igualment els principis que la Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, al seu article 4, reconeix i que informen la incorporació dels mitjans electrònics en les actuacions del sector públic de Catalunya. Aquests principis, tot i que no són exclusius de l'automatització dels processos, són aplicables a aquesta, atès que l'automatització és una manifestació més de la incorporació dels mitjans electrònics a l'actuació administrativa.

En resum, l'automatització de processos, com una manifestació més de l'adaptació dels procediments presencials a la seva tramitació electrònica, requereix una norma habilitadora, amb rang de llei, que així ho possibiliti. A més, aquesta habilitació ha de contenir les especificacions necessàries que estableixin les condicions d'exercici i que, simultàniament, garanteixin els drets dels ciutadans.

Aquests drets dels ciutadans resultarien garantits amb la possibilitat de reaccionar contra l'acte administratiu emès, ja sigui per raons de caràcter substantiu, relacionades amb el contingut intrínsec de l'acte produït, ja sigui per raons de caràcter formal, relatives al procés d'automatització mateix.

2.1.8. *Control de l'automatització*

Ja hem indicat que aquest procés d'automatització és una decisió discrecional i, com a tal, susceptible de control d'acord amb els paràmetres que es detallen tot seguit.

1) L'existència i l'extensió de la potestat.

No hi hauria problemes jurídics quan existís la norma habilitadora. Actualment es pot considerar que l'article 39 de la Llei 11/2007 no és suficient, per tal com requereix que se'n desenvolupi o se'n concreti el contingut.

2) La competència, la forma i el procediment.

Es tractaria d'elements de l'acte administratiu que respondrien al que hauria de ser una programació adequada, amb coherència entre els aspectes tècnics i els jurídics.

3) La finalitat a perseguir en l'actuació administrativa.

És evident que l'actuació administrativa ha de respondre a una persecució de l'interès general, sens perjudici de les finalitats particulars o els béns jurídics que ha de protegir l'actuació administrativa concreta.

En principi, l'actuació administrativa automatitzada no plantejaria cap diferència respecte a una actuació administrativa no automatitzada, exceptuant el cas que s'aprofités aquesta automatització per alterar les condicions d'exercici, en perjudici de l'administrat o l'administrada.

6) Els supòsits fàctics o de fet.

En el cas de l'actuació administrativa automatitzada, respondrien a un supòsit doble: en primer lloc, els supòsits fàctics o de fet que justifiquen l'actuació administrativa pròpiament dita, al marge de la seva forma de realització; en segon lloc, des d'un punt de vista més tècnic, hi hauria la comprovació de les condicions de programació que han condicionat o predeterminat un resultat o una resposta automàtica de la màquina.

7) Els principis generals del dret.

Com a criteri general, els principis generals del dret administratiu són aplicables i, en el cas que ens ocupa, tindrien, en particular, la seva manifestació en el respecte a tots i cadascun dels principis generals que la utilització dels mitjans electrònics requereix amb

caràcter específic,[11] i, en general, el respecte a tots els drets que, amb caràcter general, reconeix l'ordenament jurídic als administrats en les seves relacions amb l'Administració.

2.1.9. *La planificació de l'actuació administrativa*

Un altre element a considerar és la possibilitat que l'Administració planifiqui o programi l'actuació administrativa. Aquesta potestat planificadora, essencialment discrecional, significa l'establiment d'un programa o d'una planificació que predeterminarà el contingut dels actes administratius emesos pels òrgans administratius.

Això suposa la transformació d'una potestat discrecional en reglada, que és justament el que es produeix amb l'automatització de processos, en què potestats originàriament discrecionals passen a ser reglades com a conseqüència d'una planificació determinada o, fins i tot, en sentit estricte, d'una programació determinada.

Aquesta diferència no és merament aparent, ja que mentre que en les potestats discrecionals existeixen diferents possibilitats, totes igual de vàlides, en les potestats reglades hi ha una única possibilitat, perquè la programació informàtica realitzada haurà de respondre de manera idèntica a totes les situacions en què concorrin els requisits establerts jurídicament i tècnicament.

Això ens portaria, amb una automatització de processos duta a terme adequadament, a un compliment molt més estricte del principi d'igualtat, que garanteix el tracte igual als iguals. No obstant això, és evident que el límit es trobarà en la base de la programació, atès que existeix un nucli dur de les decisions administratives que difícilment es podrà automatitzar.

En qualsevol cas, tal com exposem, les previsions legals relatives a l'automatització dels actes administratius són genèriques, pel que fa a la tipologia d'actes susceptibles d'automatitzar, la qual cosa permet un marge ampli de discrecionalitat a l'hora de prendre aquesta decisió, sempre amb el necessari compliment de tots els paràmetres i les condicions prèvies que la justifiquin i amb ple respecte als principis i les garanties a observar.

[11] Es tractaria, fonamentalment, dels principis generals enumerats a l'article 4 de la Llei 11/2007.

2.2. La programació de l'actuació administrativa automatitzada

Ja hem comentat que els requeriments jurídics i els tècnics són essencials a l'hora d'articular el procediment administratiu electrònic. Pel que fa a l'automatització, la programació tracta de donar resposta a dos plantejaments: el derivat de la tramitació electrònica pròpiament dita i el derivat de l'automatització en la producció de l'acte administratiu estrictament.

2.2.1. *L'aprovació dels programes i les aplicacions*

En tots dos casos, s'ha de plantejar si es requereix l'aprovació i la publicació dels programes i les aplicacions tal com s'exigia abans que entrés en vigor la Llei 11/2007 o si, contràriament, l'aprovació i la publicació ja no són necessàries.

Podem avançar que l'aprovació dels programes i les aplicacions és necessària, perquè, malgrat el silenci de la Llei 11/2007,[12] la normativa pot exigir aquesta aprovació (com passa en determinats àmbits) i, independentment que aquesta previsió acabi sent superada, sempre haurà d'existir un acte aprovatori, més o menys formal, per part de l'òrgan administratiu competent, d'aquests programes i aplicacions. Una qüestió diferent serà la publicitat i la transparència que es puguin exigir a aquests actes aprovatoris.

Com a plantejament previ, la Llei 11/2007 ha derogat alguns preceptes de la Llei 30/1992. Entre aquests hi ha l'article 45.4, que deia el següent: «Els programes i les aplicacions electròniques, informàtiques i telemàtiques que hagin de ser utilitzats per les administracions públiques per a l'exercici de les seves potestats han de ser prèviament aprovats per l'òrgan competent, el qual n'ha de difondre públicament les característiques.»

No obstant això, la Llei 11/2007 no indica si, a partir d'aquesta derogació, s'han fet innecessàries l'aprovació i la publicació dels programes. Tan sols tracta la qüestió a l'article 39, relatiu a l'actuació administrativa automatitzada, de conformitat amb el qual hi haurà un òrgan regulador «[...] per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema

[12] El Reial decret 1671/2009, de 6 de novembre, pel qual es desplega parcialment la Llei 11/2007, no conté cap previsió sobre aquesta qüestió, tot i que deroga el Reial decret 263/1996, de 16 de febrer, que regulava la utilització de tècniques electròniques, informàtiques i telemàtiques per part de l'Administració general de l'Estat, que exigia amb caràcter general l'aprovació i la publicació dels programes i les aplicacions.

d'informació i del seu codi font. Així mateix, s'ha d'indicar l'òrgan que ha de ser considerat responsable als efectes d'impugnació».

Això significaria que, al marge del que es pugui entendre amb caràcter general en l'àmbit dels procediments administratius tramitats electrònicament, en l'àmbit de l'actuació administrativa automatitzada no s'ha eliminat l'obligació d'aprovació, sens perjudici que siguin els òrgans corresponents els que regulin el sistema d'aprovació i difusió dels programes i les aplicacions utilitzats en cada cas. Sigui com sigui, es tractaria d'una qüestió lligada a la potestat autoorganitzativa de cadascuna de les administracions.

Evidentment, aquesta aprovació ha de disposar prèviament dels informes tècnics pertinents que assegurin la legalitat de l'aplicació, la seguretat, la normalització dels mitjans d'accés i la conservació dels suports emprats.

Si analitzem altres normatives, comprovem que, en l'àmbit del Principat d'Astúries, per adaptar-se a la Llei 11/2007 es va aprovar el Decret 115/2008, de 20 de novembre, de modificació del Decret 111/2005, de 3 de novembre, sobre registre telemàtic.

No obstant això, la qüestió és tractada tan sols tangencialment:

«*El registro telemático recibirá las solicitudes, escritos y comunicaciones que le sean presentados siempre que se cumplan las siguientes condiciones*:
a) Que las solicitudes, escritos y comunicaciones se soporten en los formularios electrónicos habilitados al efecto para cada uno de los trámites, servicios o procedimientos.
b) Que se utilicen los sistemas de identificación electrónica y de firma electrónica admitidos en cada caso en la norma reguladora del registro.
Para cada servicio, procedimiento o trámite podrá admitirse más de un sistema de identificación electrónica y, en su caso, de firma electrónica.»

Més endavant es defineix el formulari electrònic com «u*n documento electrónico estructurado, con campos de información predefinidos, que sirve de soporte para la carga de las solicitudes, escritos y comunicaciones referidas a trámites o procedimientos administrativos susceptibles de recepción y remisión mediante registro telemático y que se encuentra disponible a tal efecto en el portal o la intranet corporativos de la Administración del Principado de Asturias*».

Així doncs, a pesar de la derogació expressa de l'article 45.4 de la Llei 30/1992 i el silenci de la Llei 11/2007, s'indica que els tràmits, els serveis o els procediments es duran a terme en els «*formularios habilitados al efecto*» i disponibles en «*el portal o la intranet corporativos de la Administración del Principado de Asturias*».

Pel que fa a Catalunya, el Decret 56/2009 preveu l'aprovació del procediment i, implícitament, dels programes i les aplicacions que hi donen suport. No obstant això, s'estableix que sigui el director o la directora de serveis de cadascun dels departaments, o òrgans equivalents, qui determini o acrediti el compliment del protocol corresponent a l'hora d'autoritzar la incorporació d'un procediment o d'un servei determinat a la tramitació electrònica i la seva utilització per part del ciutadà.

Jutgem correcte aquest criteri de la necessària aprovació dels programes i les aplicacions: d'una banda, en la mesura que respecta l'existència necessària d'un acte administratiu aprovatori, d'acord amb la doctrina de les potestats administratives i de la vinculació positiva; i, d'altra banda, perquè inclou l'existència necessària d'un informe tècnic favorable del Centre de Telecomunicacions i Tecnologies de la Informació, fet que garanteix igualment el compliment de les garanties tècniques.[13]

Igualment, en el camp de la contractació administrativa, el Decret 96/2004, de 20 de gener, pel qual es regula la utilització dels mitjans electrònics, informàtics i telemàtics en la contractació de l'Administració de la Generalitat, preveu l'aprovació de programes i aplicacions, a l'article 12.1.[14]

Al marge del que estableixin —o no estableixin— amb caràcter general l'Administració general de l'Estat i les comunitats autònomes, cal esmentar, igual que en el cas de la contractació pública, àmbits específics de regulació en què la matèria està regulada de manera que es podria qualificar de completa.

---

[13] L'article 10 del Decret 56/2009 disposa: «1. La tramitació electrònica de qualsevol servei requereix l'avaluació i aprovació del compliment del protocol de serveis i tràmits electrònics, pel que fa als aspectes tècnics i de gestió dels programes i aplicacions que l'executin. Aquesta aprovació la fa l'òrgan competent, amb l'informe previ tècnic favorable a què es refereix l'apartat 3, així com el corresponent informe organitzatiu.
2. És competent per a l'aprovació dels programes i aplicacions el director o directora de serveis de cada departament o òrgan equivalent. En el cas dels organismes autònoms, entitats de dret públic vinculades o dependents i altres ens inclosos en l'àmbit d'aplicació d'aquest Decret, s'ha de tenir en compte el que disposen les seves normes reguladores.
3. Els programes i les aplicacions que donen suport a la tramitació electrònica requereixen un informe tècnic favorable del Centre de Telecomunicacions i Tecnologies de la Informació, mitjançant les àrees TIC de cada departament, en relació amb les especificacions sobre l'adequació del programa o l'aplicació a aquest Decret i les disposicions dictades en el seu desplegament, i en particular:
a) La seguretat de l'aplicació: preservació de la disponibilitat, de la confidencialitat i de la integritat de les dades tractades per l'aplicació.
b) La normalització dels sistemes d'accés: especificacions tècniques sobre els mitjans, codis i formats d'accés.
c) La conservació dels formats utilitzats: proporció entre la durabilitat dels formats i el temps en què les dades s'han de mantenir incloses.
d) La interoperabilitat i reutilització de l'aplicació.
4. Una vegada complerts els requisits de l'apartat 1, el servei s'incorpora a la seu electrònica corporativa i està a disposició dels ciutadans i ciutadanes.»

[14] «Els programes i les aplicacions informàtiques per a la gestió de la contractació dels departaments, organismes autònoms i empreses públiques han de ser objecte d'aprovació per Ordre del/de la conseller/a d'Economia i Finances, previs els informes tècnics de la Comissió de Coordinació Interdepartamental de Gestió i de Tecnologies de la Informació i Comunicacions i de l'Agència Catalana de Certificació i l'informe de la Junta Consultiva de Contractació Administrativa. Aquests programes i aplicacions han de contenir les polítiques de seguretat i les especificacions tècniques que assegurin l'efectivitat dels controls criptogràfics de signatura electrònica exigits per l'article 7 i els controls criptogràfics de xifratge exigits per l'article 8 d'aquest Decret, així com els mecanismes de seguretat, algorismes, longituds de claus i procediments d'auditoria del sistema que permetin certificar el secret de les proposicions fins al moment en què sigui procedent la seva obertura.»

Aquest és el cas de l'àmbit tributari, en el qual la Llei 58/2003, general tributària, de 17 de desembre, indica, a l'article 96 («Utilització de tecnologies informàtiques i telemàtiques»): «1. L'Administració tributària ha de promoure la utilització de les tècniques i els mitjans electrònics, informàtics i telemàtics necessaris per al desenvolupament de la seva activitat i l'exercici de les seves competències, amb les limitacions que la Constitució i les lleis estableixin.»

El mateix precepte estableix, a continuació, el següent: «2. Quan sigui compatible amb els mitjans tècnics de què disposi l'Administració tributària, els ciutadans s'hi poden relacionar per exercir els seus drets i complir les seves obligacions a través de tècniques i mitjans electrònics, informàtics o telemàtics amb les garanties i els requisits previstos en cada procediment.
3. Els procediments i les actuacions en què s'utilitzin tècniques i mitjans electrònics, informàtics i telemàtics han de garantir la identificació de l'Administració tributària actuant i l'exercici de la seva competència. A més, quan l'Administració tributària actuï de forma automatitzada es garanteix la identificació dels òrgans competents per a la programació i supervisió del sistema d'informació i dels òrgans competents per resoldre els recursos que es puguin interposar.
4. Els programes i les aplicacions electrònics, informàtics i telemàtics que hagin de ser utilitzats per l'Administració tributària per a l'exercici de les seves potestats han de ser aprovats prèviament per aquesta en la forma que es determini per reglament.
5. Els documents emesos, sigui quin sigui el seu suport, per mitjans electrònics, informàtics o telemàtics per l'Administració tributària, o els que aquesta emeti com a còpies d'originals emmagatzemats per aquests mateixos mitjans, així com les imatges electròniques dels documents originals o les seves còpies, tenen la mateixa validesa i eficàcia que els documents originals, sempre que en quedi garantida l'autenticitat, integritat i conservació i, si s'escau, la recepció per part de l'interessat, així com el compliment de les garanties i els requisits exigits per la normativa aplicable.»

El Reial decret 1065/2007, de 27 de juliol, pel qual s'aprova el Reglament general de les actuacions i els procediments de gestió i inspecció tributària i de desplegament de les normes comunes dels procediments d'aplicació dels tributs, estableix, a l'article 85 («Aprovació i difusió d'aplicacions»):

«1. En els supòsits d'actuació automatitzada a què es refereix l'article anterior, les aplicacions informàtiques que efectuïn tractaments d'informació el resultat dels quals sigui utilitzat per l'Administració tributària per a l'exercici de les seves potestats i per les quals es determini directament el contingut de les actuacions administratives, han de ser prèviament aprovades mitjançant una resolució de l'òrgan que ha de ser considerat responsable als efectes de la impugnació dels corresponents actes administratius. Quan

es tracti de diferents òrgans de l'Administració tributària no relacionats jeràrquicament, l'aprovació correspon a l'òrgan superior jeràrquic comú de l'Administració tributària de què es tracti, sense perjudici de les facultats de delegació establertes en l'ordenament jurídic.
2. Els interessats poden conèixer la relació de les esmentades aplicacions mitjançant consulta en la pàgina web de l'Administració tributària corresponent, que han d'incloure la possibilitat d'una comunicació segura de conformitat amb el que preveu l'article 83.3.»

En aquesta línia, la Resolució de 16 d'abril de 2004, de la Direcció General de l'Agència Estatal d'Administració Tributària, regula la generació i l'arxivament de documents electrònics a partir de documents en suport paper, així com l'emissió de còpies en paper d'aquests documents electrònics, i aprova els programes i les aplicacions a utilitzar, a l'empara del Reial decret 263/1996, com indica la seva exposició de motius. Caldrà veure en quina mesura el Reial decret 1671/2009 afecta aquesta normativa.

Existeixen altres àmbits jurídics en què també es regula l'aprovació d'aplicacions, com el trànsit i la Seguretat Social.

Tocant al trànsit, cal fer esment de la Resolució de 27 de març de 2006, de la Direcció General de Trànsit, per la qual s'aproven les aplicacions dels registres en suport informàtic de la Direcció General de Trànsit utilitzats per a l'exercici de potestats administratives i es regula la conservació permanent de les dades dels registres de vehicles i de conductors i infractors amb finalitats històriques, científiques i estadístiques.[15]

En l'àmbit de la Seguretat Social, la Resolució de 18 de setembre de 2007, de la Tresoreria General de la Seguretat Social, aprova determinades aplicacions informàtiques per a la gestió d'inscripció d'empreses, d'afiliació de treballadors i de recaptació de

[15] L'article 1 disposa: «La presente Resolución tiene por objeto la adecuación de las aplicaciones de los Registros en soporte informático de la Dirección General de Tráfico, utilizados para el ejercicio de potestades administrativas, a lo dispuesto en el artículo 9 del Real Decreto 263/1996, así como regular la conservación permanente de los datos que obran en los Registros de Vehículos y de Conductores e Infractores.
En consecuencia, se aprueban las siguientes aplicaciones utilizadas para el ejercicio de potestades administrativas:
o Registro de Vehículos.
o Registro Central de Infractores.
o Manipuladores de placas de matrícula.
o Centros autorizados de reciclado y descontaminación (CARD).
o Autorizaciones complementarias y especiales de circulación.
o Personas.
o Centros de Reconocimiento.
o Escuelas de Conductores.
o Expedientes de sanción."
o […]
Los órganos competentes para la resolución de los procedimientos adoptados mediante estas aplicaciones son las Jefaturas Provinciales y Locales de Tráfico o el órgano que se determine en su caso, en virtud de lo dispuesto en el Reglamento General de Conductores, el Reglamento General de Vehículos y el artículo 5.h del Texto Articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. Los usos y accesos de estas aplicaciones serán los previstos para cada fichero en la Orden INT/3764/2004, de 11 de noviembre.»

recursos del sistema de la Seguretat Social. En aquesta mateixa línia es manifesta la Resolució de 3 d'agost de 2006, de l'Institut Nacional de la Seguretat Social, per la qual s'aproven determinades aplicacions informàtiques per a la gestió de les prestacions del sistema de la Seguretat Social.

Aquest és el marc normatiu vigent, en relació amb el qual es podria plantejar si la Llei 11/2007 ha modificat aquesta obligació d'aprovació i difusió pública.

Cal tenir present que autors com Valero Torrijos[16] fan esment de la defectuosa tècnica legislativa emprada per la Llei 11/2007 respecte a la derogació de l'aprovació dels programes i les aplicacions. A més, assenyalen que, al marge de la naturalesa jurídica de l'aprovació dels programes i les aplicacions, es tracta d'un requisit essencial per assegurar la subjecció plena a la llei i al dret de les aplicacions i els serveis de l'administració electrònica des d'una perspectiva material, de tal manera que existeixi un control efectiu sobre el funcionament d'aquestes eines i s'asseguri plenament que els òrgans administratius són els que actuen i controlen les seves decisions, sense que això impliqui renunciar a l'ús de les noves tecnologies.

Tanmateix, l'aprovació dels programes i les aplicacions es pot analitzar igualment des del punt de vista de la teoria general de l'acte administratiu i l'exercici de potestats administratives, basat en la doctrina de la vinculació positiva.

L'article 56 de la Llei 30/1992 estableix: «Els actes de les administracions públiques subjectes al dret administratiu són executius d'acord amb el que disposa aquesta Llei.» L'article 57, per la seva banda, diu així: «1. Els actes de les administracions públiques subjectes al dret administratiu es presumeixen vàlids i produeixen efectes des de la data en què es dicten, llevat que s'hi disposi altrament.»

Tot i el silenci de la Llei 11/2007, sembla evident que sempre haurà d'existir un acte administratiu en què el funcionari o la funcionària competent prengui la decisió de posar en producció un programa o una aplicació determinats a l'efecte que el puguin fer servir els administrats mitjançant l'accés al tràmit o el servei de què es tracti a la seu electrònica corresponent. Lògicament, aquest personal ha d'estar habilitat a l'efecte, és a dir, facultat per raó de la seva competència per dur a terme aquesta aprovació.

[16] Valero Torrijos, J. *Op. cit*., pàg. 79.

2.2.2. *La difusió pública de l'aprovació*

En qualsevol cas, malgrat que podem entendre que sempre serà necessària l'aprovació dels programes o aplicacions —al marge de l'element o el criteri formal que es requereixi per a aquesta aprovació—, el que s'ha comentat fins ara no resol la qüestió relativa a la difusió pública de les característiques d'aquest programari.

Amb caràcter general, l'article 58.1 de la Llei 30/1992 indica que «s'han de notificar als interessats les resolucions i els actes administratius que afectin els seus drets i interessos, en els termes que preveu l'article següent».

Per aquesta raó, si l'Administració ha d'utilitzar uns programes i unes aplicacions determinats, hi ha d'haver un acte aprovatori i, en la mesura que això afecta els administrats, s'hauria de plantejar si és necessària una notificació i si, pel fet que es tracta d'un acte adreçat a una pluralitat indeterminada d'interessats, caldria la publicació al Butlletí Oficial corresponent o bé n'hi hauria prou amb una difusió pública de les seves característiques, tal com es preveu en l'àmbit tributari.

En aquest sentit, existiria la possibilitat que l'aprovació no porti aparellada la publicació subsegüent. A més, fins i tot en la regulació fins fa poc vigent, amb referència als actes que no incideixen de manera directa en la resolució, l'article 5 del Reial decret 263/1996, ja no vigent, preveia un segon supòsit davant la regla general d'aprovació de programes. En aquell supòsit s'assenyalava que fins i tot no era necessària l'aprovació dels programes de caràcter instrumental que efectuessin tractaments d'informació auxiliars o preparatoris de decisions administratives sense determinar-ne el contingut.

Independentment de la manca de vigència d'aquest Reial decret i de la manca de concreció del que s'havia d'entendre per aquells actes administratius interns, la realitat és que aquells actes administratius tenien un caràcter residual i, pel que fa al seu àmbit d'aplicació, havien de ser objecte d'una interpretació restrictiva, ja que difícilment ens trobarem amb actes que, encara que sigui indirectament, determinin el contingut de la decisió administrativa.

Ja hem manifestat que quan l'article 39 de la Llei 11/2007 parla de l'actuació administrativa automatitzada es limita a indicar que «s'ha d'establir prèviament l'òrgan o òrgans competents, segons els casos, per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema d'informació i del seu codi font». Per tant, no inclou cap referència ni menció a una publicació posterior, la qual cosa podria conduir a pensar que aquesta no és necessària.

A més, és important assenyalar que la Llei 11/2007 recull igualment el principi de neutralitat tecnològica. Això fa convenient l'existència d'un òrgan que, a l'hora d'aprovar els programes i les aplicacions corresponents, verifiqui, entre d'altres, el compliment del principi esmentat.

Aquest principi apareix recollit a l'article 4.i) de la Llei 11/2007, que estableix el següent: «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 han d'utilitzar estàndards oberts així com, si s'escau i de forma complementària, estàndards que siguin d'ús generalitzat pels ciutadans.»

Així doncs, en compliment d'aquest principi general, seria exigible que es compleixi la garantia de la independència de l'alternativa tecnològica escollida i que la discrecionalitat que pugui tenir l'Administració a l'hora de determinar aquestes solucions tecnològiques es trobi limitada per la tendència a utilitzar estàndards oberts o, si s'escau, programes i aplicacions en què la interoperabilitat estigui garantida.

Cal tenir present que la interoperabilitat, l'intercanvi de dades i la col·laboració són molt importants: si no hi ha entesa entre les aplicacions que facin servir les administracions públiques, el desenvolupament dels mitjans electrònics es pot veure afectat. A més, l'automatització de processos pot partir moltes vegades de la comunicació de dades entre administracions públiques, en el marc del dret reconegut a l'article 6.2.b) de la Llei 11/2007, de no exigir dades i documents que estiguin en poder de les administracions públiques.[17] En aquests casos, la interoperabilitat és essencial, i restarà garantida dissenyant els programes de la manera més estàndard possible i amb els requisits de compatibilitat que possibilitin el compliment d'aquest principi.

Hi ha altres articles de la Llei 11/2007 que regulen aspectes relacionats amb l'aprovació i la difusió pública. És el cas dels esquemes nacionals d'interoperabilitat i de seguretat, previstos a l'article 42, els quals han d'establir les regles que ha de respectar qualsevol

[17] Article 6.2.b): «A més, els ciutadans, en relació amb la utilització dels mitjans electrònics en l'activitat administrativa, i en els termes que preveu aquesta Llei, tenen els drets següents:
[...]
b) A no aportar les dades i documents que estiguin en poder de les administracions públiques, les quals han d'utilitzar mitjans electrònics per obtenir la informació esmentada sempre que, en el cas de dades de caràcter personal, tinguin el consentiment dels interessats en els termes que estableix la Llei orgànica 15/1999, de protecció de dades de caràcter personal, o una norma amb rang de Llei ho determini, llevat que hi hagi restriccions d'acord amb la normativa aplicable a les dades i documents recollits. El consentiment es pot emetre i acceptar per mitjans electrònics.»

sistema posat a disposició per qualsevol Administració pública. En el mateix sentit, és important la reutilització de sistemes que estableix l'article 45.[18]

En aquesta mateixa línia, la Llei 29/2010, de 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, al seu article 25, regula la reutilització de les aplicacions i els serveis.[19]

Cal tenir present, també en aquest sentit, el Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'administració electrònica, i el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en el mateix àmbit. Tots dos reials decrets són dictats amb caràcter bàsic, a l'empara de l'article 149.1.18 de la Constitució.

Quan aquests esquemes estiguin aprovats, caldrà que qualsevol aplicació els respecti, circumstància que caldrà comprovar a l'hora d'aprovar l'aplicació corresponent per tal de garantir que es compleixen els estàndards que estableixen aquests esquemes.

Finalment, cal tenir present un precepte de la Llei 11/2007, l'article 27.4, en seu de comunicacions electròniques: «Les administracions han de publicar, en el corresponent diari oficial i a la mateixa seu electrònica, els mitjans electrònics que els ciutadans poden utilitzar en cada cas en l'exercici del seu dret a comunicar-s'hi.»

Realment, aquest precepte distorsiona la qüestió, sobretot si partim del concepte omnicomprensiu de *mitjà electrònic* que utilitza la Llei 11/2007 al seu annex.[20] En qualsevol cas, hem d'interpretar aquest article d'acord amb la ubicació on es troba —comunicacions electròniques— i en el context de l'article —referent als canals de comunicació que pot emprar el ciutadà a l'hora de relacionar-se amb l'Administració pública quan aquesta exerceix potestats administratives. No obstant això, la mateixa

[18] «1. Les administracions titulars dels drets de propietat intel·lectual d'aplicacions, desenvolupades pels seus serveis o el desenvolupament de les quals hagi estat objecte de contractació, les poden posar a disposició de qualsevol Administració sense contraprestació i sense necessitat de conveni.»

«2. Les aplicacions a què es refereix l'apartat anterior poden ser declarades de fonts obertes, quan d'això derivi una transparència més gran en el funcionament de l'Administració pública o es fomenti la incorporació dels ciutadans a la societat de la informació.»

[19] «1. Les entitats que integren el sector públic, per a prestar llurs serveis, han de potenciar l'ús de les aplicacions que han estat desenvolupades per altres entitats del sector públic.

2. Les entitats que integren el sector públic han de vetllar perquè les aplicacions que desenvolupen es basin en criteris i estàndards que facilitin la interoperabilitat i que puguin ésser reutilitzades per altres entitats del sector públic.

3. Les entitats del sector públic han d'impulsar la creació de bancs de recursos i aplicacions de les administracions públiques que puguin ésser reutilitzats per a facilitar l'aprofitament de les aplicacions, i també llur desenvolupament col·laboratiu»

[20] «Mitjà electrònic: mecanisme, instal·lació, equip o sistema que permet produir, emmagatzemar o transmetre documents, dades i informacions; incloent qualssevol xarxes de comunicació obertes o restringides com Internet, telefonia fixa i mòbil o altres.»

Comissió Jurídica Assessora, en el Dictamen 22/2009, esmentat més amunt, ha interpretat aquesta previsió com la subsistència de l'obligació de publicar oficialment els procediments i els serveis que es poden tramitar de manera electrònica.

2.3. L'automatització de processos i l'exercici de la competència

L'existència d'una pluralitat d'ens en el si de cadascuna de les administracions públiques exigeix que es distribueixi entre elles la titularitat de les funcions públiques. Però, a més, l'existència de diversos òrgans dins un ens públic obliga a distribuir igualment entre ells les funcions a realitzar en relació amb les particularitats atribuïdes a l'ens sobre la base del principi de legalitat i potestat autorganitzativa.

2.3.1. *La competència administrativa*

Podem definir el concepte de *competència administrativa* com ho fa García de Enterría: com «la mesura de la potestat que correspon a cada òrgan».

Quant a la naturalesa del concepte, la competència administrativa no obeeix tan sols a la necessitat de distribuir el treball, sinó també a la voluntat de ser una garantia per als administrats. Tant la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, com la Llei 13/1989, de 14 de desembre, d'organització, funcionament i règim jurídic de l'Administració de la Generalitat, disposen, com a regla general, que la competència és irrenunciable i l'ha d'exercir l'òrgan que la té atribuïda, llevat de determinades excepcions (com l'avocació o la delegació).

Cal tenir present que els conceptes de *competència* i de *potestat* són usats habitualment de manera indiferenciada. En aquest sentit, és paradigmàtic l'article 2.4 de la Llei 6/1997, d'organització i funcionament de l'Administració general de l'Estat (LOFAGE), quan indica que «*las potestades y competencias administrativas que, en cada momento, tengan atribuidas la Administración General del Estado y sus Organismos Públicos por el ordenamiento jurídico, determinan la capacidad de obrar de una y de otros*».

En qualsevol cas, podem entendre per *potestats* un concepte més ampli, referit a poders d'actuació de caràcter més genèric no identificats amb la matèria sobre la qual recauen o el sector en el qual operen. Per contra, la *competència* és un concepte més concret, referit a un sector o un àmbit d'actuació específic.

Quant a les classes, es distingeixen les següents:

1) Una competència subjectiva, o conjunt de funcions la titularitat de les quals s'atribueix a un ens amb preferència als altres.
2) Una competència orgànica, com aquella part de les funcions d'un ens l'exercici de les quals s'atribueix a un dels òrgans de l'ens.

Finalment, pel que fa als criteris de delimitació, es distingeix:

- Competència jeràrquica.
- Competència material.
- Competència territorial.

El criteri jeràrquic es refereix a la preferència d'un òrgan concret per exercir la funció en relació amb els seus superiors o inferiors. Els altres dos criteris atenen al pla horitzontal, això és, entre òrgans d'un mateix nivell jeràrquic, ja sigui en relació amb la matèria o amb l'àmbit territorial d'actuació.

La determinació competencial és una manifestació de la potestat autoorganitzativa, que s'entén com el conjunt de facultats que té cada Administració per configurar la seva estructura (és a dir, la possibilitat d'autoorganitzar-se).

Quant a la titularitat, caldrà acudir a la normativa reguladora de cada Administració. En particular, en l'àmbit de l'Administració general de l'Estat s'ha imposat la reserva de llei per a la regulació del Govern, del Consell d'Estat i dels organismes públics. No obstant això, per reial decret el president o la presidenta pot variar el nombre, la denominació i les competències dels ministeris i les secretaries l'Estat (articles 61 i 8.3 de la LOFAGE).

Així mateix, l'article 10 de la LOFAGE disposa que les subsecretaries, les secretaries generals, les secretaries generals tècniques, les direccions generals, les subdireccions generals i els òrgans similars es creen, es modifiquen i se suprimeixen per reial decret del Consell de Ministres. Per la seva banda, els òrgans de nivell inferior a subdirecció general es creen, es modifiquen i se suprimeixen per ordre del ministre respectiu.

En l'àmbit de l'Administració de la Generalitat, tant la Llei 13/1989 com la Llei 13/2008, de 5 de novembre, de la presidència de la Generalitat i del Govern, reconeixen al Govern responsabilitats organitzatives àmplies, com ara crear comissions dins el mateix govern; crear, agrupar, modificar, dividir o suprimir els departaments fixats per la llei, i realitzar les modificacions i les innovacions organitzatives en els diversos nivells. Paral·lelament, atribueix als consellers potestat reglamentària en matèria d'organització dels seus departaments.

En l'àmbit local, els òrgans polítics bàsics dels municipis i les províncies estan regulats a la Llei de bases de règim local. Els òrgans inferiors, de nivell administratiu, els regulen cada corporació —que ha d'aprovar un reglament orgànic— i les normes supletòries que dictin les comunitats autònomes.

Quant als principis de la potestat organitzativa, aquesta s'ha d'inspirar i ha de respectar l'article 103 de la Constitució, que estableix: «L'Administració pública serveix amb objectivitat els interessos generals i actua d'acord amb els principis d'eficàcia, jerarquia, descentralització, desconcentració i coordinació, amb submissió plena a la llei i al Dret.» Aquests principis han estat reiterats per l'article 3 de la Llei 30/1992, la qual hi afegeix tres principis més:

1) La distinció entre governs i administracions.
2) El principi de cooperació.
3) El principi de personalitat jurídica única, d'acord amb el qual l'article 3.4 de la Llei 30/1992 estableix el següent: «Cadascuna de les administracions públiques actua, per al compliment de les seves finalitats, amb personalitat jurídica única.» (Així mateix ho recull l'article 2 de la Llei 13/1989.)

2.3.2. *La competència i l'actuació administrativa automatitzada*

D'acord amb el que hem exposat, el concepte de *competència* és essencial a l'hora de tractar l'actuació administrativa, i, en el cas de l'actuació administrativa automatitzada, hi ha d'haver igualment una atribució expressa de competències.

De la mateixa manera, ja hem indicat que cada Administració pública gaudeix d'una autonomia molt gran a l'hora de crear, modificar i extingir els seus òrgans, cosa que es manifestarà també en l'actuació administrativa automatitzada, en un nivell doble:

- El primer nivell (tractat prèviament) seria la decisió discrecional d'automatitzar un procediment determinat, cosa que exigirà una actuació d'adequació jurídica i tècnica als condicionants que l'actuació administrativa concreta requereix.
- El segon nivell, relacionat directament amb l'anterior, té a veure amb la vessant jurídica: consistiria en l'adequació de la seva estructura organitzativa a l'existència d'un òrgan que, programat degudament, produís actes administratius de manera automatitzada.

En qualsevol cas, com indica l'article 44.3 de la Llei 26/2010, «l'actuació administrativa automatitzada no afecta la titularitat de la competència dels òrgans administratius ni les competències atribuïdes per a resoldre els recursos administratius».

A títol d'exemple, la normativa tributària preveu, per exemple, que l'automatització haurà de partir de l'òrgan administratiu responsable a efectes d'impugnació, que és el que comprovaria, en última instància, la regularitat de l'actuació administrativa emesa.

En qualsevol cas, el concepte de *competència* és bàsic a l'hora de parlar d'actuació administrativa per mitjans electrònics. Cal recordar que aquesta figura està recollida a la normativa tributària, en particular als articles 96.3 i 100.2 de la Llei 58/2003, de 17 de desembre, general tributària. A més, s'ha previst, amb caràcter general, la possible automatització dels processos als articles esmentats.

El primer d'aquests articles assenyala: «Els procediments i les actuacions en què s'utilitzin tècniques i mitjans electrònics, informàtics i telemàtics han de garantir la identificació de l'Administració tributària actuant i l'exercici de la seva competència. *A més, quan l'Administració tributària actuï de forma automatitzada es garanteix la identificació dels òrgans competents per a la programació i supervisió del sistema d'informació i dels òrgans competents per resoldre els recursos que es puguin interposar.*»

El segon d'aquests articles estén la possible utilització de l'actuació administrativa automatitzada als actes resolutoris. En particular, estableix: «Té la consideració de resolució la resposta efectuada de forma automatitzada per l'Administració tributària en els procediments en què estigui prevista aquesta
forma d'acabament.»

Certament, la figura ha estat usada en l'àmbit tributari amb certa profusió, sense que el segell d'òrgan hagi presentat problemes especials en les relacions juridicotributàries. Tanmateix, aquest fet no ens pot portar a entendre que l'experiència es pot traslladar fàcilment a qualsevol esfera de l'actuació administrativa. D'una banda, que el seu ús no hagi generat problemes també prové del fet que fins i tot la seva utilització en l'esfera tributària és, ara com ara, reduïda, per la qual cosa la casuística pel que fa al nombre de problemes encara no és rellevant. D'altra banda, el concepte essencialment de deure que caracteritza l'obligació tributària, l'actuació en massa i reiterada en el temps, signifiquen uns pressupòsits de fet que no es poden traslladar a la resta de les relacions juridicoadministratives, atès que els caràcters esmentats anteriorment presenten matisos significatius en el procediment administratiu comú.

Al marge de la normativa tributària, ens hem de plantejar la viabilitat de la figura al si del procediment administratiu, com també els problemes que pot generar.

Finalment, cal afegir que la mateixa Llei 11/2007 recull l'exigència general del respecte a la competència a l'article 33.1.[21]

2.3.3. *La identificació i l'autenticació en l'actuació administrativa automatitzada*

A banda de la competència configurada de manera abstracta, cal parlar també de la titularitat d'aquesta, que es manifesta mitjançant l'exercici de la competència per part del seu titular, la qual cosa requereix igualment la seva identificació i autenticació.

El capítol II de la Llei 11/2007 (articles 13 i següents) regula la identificació i l'autenticació, tant dels ciutadans com de les administracions públiques (seccions 2a i 3a), mentre que la secció 4a es refereix a la interoperabilitat i a l'acreditació i la representació dels ciutadans.

Aquesta regulació parteix del principi de lliure prestació de serveis de certificació, que deriva de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i de la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la qual s'estableix un marc comunitari per a la signatura electrònica. Alhora, la Llei 11/2007 aposta clarament pel DNI electrònic, que s'admet fins i tot com a mitjà d'acreditar l'exercici de la competència per part del personal al servei de les administracions públiques.

D'altra banda, el segell d'òrgan es recull a l'article 18 de la Llei 11/2007, sota la rúbrica «Sistemes de signatura electrònica per a l'actuació administrativa automatitzada». En aquests casos, se segueix la regla general d'exigir «la identificació i l'autenticació de l'exercici de la competència», exigible en tota actuació administrativa, amb el benentès que en l'actuació automatitzada es pot dur a terme mitjançant dos sistemes:

«a) Segell electrònic d'una administració pública, òrgan o entitat de dret públic, basat en certificat electrònic que reuneixi els requisits exigits per la legislació de signatura electrònica.

[21] Article 33.1: «La gestió electrònica de l'activitat administrativa ha de respectar la titularitat i l'exercici de la competència per l'administració pública, òrgan o entitat que la tingui atribuïda i el compliment dels requisits formals i materials establerts en les normes que regulin la corresponent activitat. A aquests efectes, i en tot cas sota criteris de simplificació administrativa, s'ha d'impulsar l'aplicació de mitjans electrònics als processos de treball i la gestió dels procediments i de l'actuació administrativa.»

b) Codi segur de verificació vinculat a l'administració pública, òrgan o entitat i, si s'escau, a la persona signant del document; en tot cas s'ha de permetre la comprovació de la integritat del document mitjançant l'accés a la seu electrònica corresponent.»

De tot allò exposat amb anterioritat deriva que, des de la vessant tècnica, cal fer una determinació doble: d'una banda, la programació dels programes i les aplicacions que duguin a terme aquesta actuació administrativa automatitzada, i, d'altra banda, l'existència de trets bàsics del procediment (com la delimitació dels mitjans d'identificació) que s'hauran de concretar o definir en el marc de la llei reguladora.

A més, no es pot deixar de banda el canvi significatiu que ha comportat la Llei 11/2007 en matèria d'identificació. A diferència de la Llei 59/2003, de 19 de desembre, de signatura electrònica, en què s'optava clarament per la signatura electrònica reconeguda, la Llei 11/2007 canvia radicalment aquesta concepció: atorga la possibilitat d'escollir el tipus de signatura a emprar per a cada procediment o tràmit i admet criteris de riscos a l'hora de determinar quina signatura s'haurà d'utilitzar.

En definitiva, la Llei 11/2007 consagra el criteri de determinació de mesures de seguretat pels procediments administratius basat en l'anàlisi de riscos i en l'ús de múltiples sistemes tècnics. Aquesta circumstància implica, primer, una certa continuació dels criteris continguts a la Llei 30/1992, i, després, representa el final de la tendència a l'adopció de la signatura electrònica reconeguda com a paradigma de la identificació i l'autenticació.

Així, les lleis de signatura estableixen la validesa legal de la signatura electrònica, a la qual no es podrà negar efectes únicament pel fet de trobar-se en forma electrònica. Tanmateix, això no vol dir que es pugui fer servir qualsevol signatura, en qualsevol entorn, sense suport jurídic addicional.

També cal tenir present que la normativa permet la construcció i l'operació de sistemes tancats d'usuaris i aplicacions basats en contractes de signatura electrònica (signatura electrònica convencional o contractual) o normatives específiques de signatura electrònica (signatura electrònica normativa), cosa que es pot traslladar a l'actuació administrativa automatitzada en funció del procediment, el tràmit o l'actuació que sigui objecte del procés d'automatització, els destinataris de l'acte i la finalitat última d'aquest.

2.4. L'òrgan administratiu i la competència envers l'automatització

Si parlem d'actuació administrativa automatitzada, i en la mesura que l'article 5 de la Llei 11/2007 ens remet a l'annex per determinar el sentit dels termes utilitzats, cal dir que aquest annex defineix l'actuació administrativa automatitzada com l'«actuació administrativa produïda per un sistema d'informació adequadament programat sense necessitat d'intervenció d'una persona física en cada cas singular. Inclou la producció d'actes de tràmit o resolutoris de procediments, així com de mers actes de comunicació».

Ja hem posat de manifest el caràcter omnicomprensiu de la definició. No obstant això, aquesta definició tan àmplia no es pot adoptar: caldrà delimitar-la per la simple raó que existeixen determinats tipus d'actes administratius que haurien de quedar exclosos de l'actuació administrativa automatitzada.

Prima facie, parlar de segell d'òrgan fa que ens plantegem dos conceptes: *competència administrativa* i *òrgan administratiu*.

2.4.1. *La superació del concepte tradicional d'òrgan administratiu*

Ja hem indicat que la competència és irrenunciable i l'exerceix l'òrgan que la té atribuïda legalment (article 12 de la Llei 30/1992). Aquesta atribució legal ens condueix al concepte d'*òrgan administratiu*, concebut tradicionalment com una pluralitat de llocs de treball que depenen d'una mateixa direcció.

El concepte legal d'*òrgan administratiu* s'ha equiparat tradicionalment amb el d'*unitat administrativa*, igual que ho fa la mateixa Llei 30/1992 en diferents articles (articles 11, 14.2, 16.1, 38, 70.1 i 110.1). El primer d'aquests preceptes, relatiu a la creació d'òrgans administratius, al·ludeix, a l'apartat segon, als requisits de creació d'un òrgan administratiu, entre els quals hi ha la forma d'integració en l'Administració pública de què es tracti i la seva dependència jeràrquica.

La Llei 6/1997, de 14 d'abril, d'organització i funcionament de l'Administració general de l'Estat (LOFAGE), a l'article 5.2, parla dels òrgans administratius en els termes següents: «*Tendrán la consideración de órganos las unidades administrativas a las que se les atribuyan funciones que tengan efectos jurídicos frente a terceros*, o cuya actuación tenga carácter preceptivo.»

L'article 7 precisa: «*Las unidades administrativas son los elementos organizativos básicos de las estructuras orgánicas. Las unidades comprenden puestos de trabajo o dotaciones de plantilla vinculados funcionalmente por razón de sus cometidos y orgánicamente por una jefatura común. Pueden existir unidades administrativas complejas, que agrupen dos o más unidades menores.*»

L'òrgan administratiu ha estat configurat tradicionalment entorn de dos elements: un de subjectiu (persones físiques integrades a l'òrgan) i un altre d'objectiu (mitjans materials de què disposa), necessaris per al compliment de les atribucions o competències de l'òrgan.

Això ens porta a avaluar si serien vàlides les actuacions administratives sense aquest element personal, és a dir, dutes a terme directament per mitjans electrònics o informàtics programats degudament. En definitiva, es tracta de discernir si la voluntat humana és essencial per a la producció d'actes administratius o si, al contrari, en podem prescindir.

La resposta, òbviament, ha de ser positiva: hi ha actes administratius que, per la seva singularitat, són susceptibles d'automatització, per raons d'interès general, i eliminen la voluntat humana. En qualsevol cas, ja hem indicat que aquesta eliminació és relativa, perquè ha estat manifestada prèviament mitjançant la programació realitzada.

No obstant això, alguns autors rebutgen la possibilitat d'automatització perquè consideren que els actes administratius, en tant que són declaracions de voluntat, no poden provenir de les màquines.[22]

Avui dia aquesta concepció s'ha d'entendre superada, ja que els avenços tecnològics fan viable —i fins i tot recomanable des del punt de vista de l'eficiència administrativa— que puguin ser automatitzades decisions administratives que, malgrat que impliquen una declaració de voluntat *ex novo*, s'integren per la comprovació del compliment d'uns requisits o condicionants establerts de manera clara i concreta.

Prèviament hem esmentat supòsits en què l'automatització resultaria pacífica —és a dir, no plantejaria situacions d'inseguretat jurídica— i permetria alliberar nombrosos recursos personals i materials que es podrien adreçar a l'exercici o el compliment d'altres funcions administratives (no cal sinó pensar en l'automatització de la notificació dels actes administratius a partir de les dades existents a l'expedient administratiu i, evidentment, amb compliment de tots els requisits que la normativa exigeix per a la notificació electrònica, o bé en els actes de certificació.)

[22] Parada, J.R. *Régimen jurídico de las administraciones públicas y del procedimiento administrativo común*. Madrid: Marcial Pons, 2a edició, 1999, pàg. 194.

L'article 44.1 de la Llei 26/2010 enumera una sèrie de supòsits o actuacions administratives automatitzables.[23] Si els analitzem, podem veure que són supòsits certament amplis que permeten traslladar l'automatització a molts àmbits de l'actuació administrativa.

Especialment significatius serien la comunicació o certificació de dades, i la constatació de la concurrència de requisits, declarant les conseqüències que es deriven.

Sobre aquesta base, existirien supòsits que serien susceptibles ~~igualment~~ d'automatització, com ara la denegació de subvencions per manca de compliment dels elements reglats establerts per a l'atorgament o bé la suspensió d'actes administratius de contingut econòmic en l'àmbit tributari per la comprovació de la prestació de la garantia.

En aquests casos, la inexistència de la intervenció humana no pot portar a negar la possibilitat d'automatització. Hem de reiterar que la intervenció humana existeix, en primer lloc, en la decisió d'automatització; en segon lloc, en l'establiment de les condicions informàtiques de producció de l'acte, i, en tercer lloc, en la supervisió del compliment o el funcionament adequat d'aquestes condicions. A més, es poden afegir sistemes d'auditoria informàtica que garanteixin el funcionament adequat de les aplicacions.

Per tot el que hem exposat, quan parlem de segell d'òrgan estem introduint un nou element en els conceptes esmentats més amunt, atès que aparentment hem de prescindir de l'element personal.

2.4.2. *El segell d'òrgan*

L'article 18.2 de la Llei 11/2007 estableix que «els certificats electrònics a què es fa referència a l'apartat 1.a) [segell d'Administració pública, òrgan o entitat de dret públic] han d'incloure el número d'identificació fiscal i la denominació corresponent, i poden contenir la identitat de la persona titular en el cas dels segells electrònics d'òrgans administratius».

D'una banda, veiem que al costat del segell d'òrgan s'admet el segell d'Administració pública i el d'entitat de dret públic, com també que, en el cas del segell d'òrgan, encara

[23] «[...] constatar la concurrència dels requisits que estableix l'ordenament jurídic, declarar les conseqüències previstes, adoptar les resolucions i comunicar o certificar les dades, els actes, les resolucions o els acords que constin en llurs sistemes d'informació [...].»

que sigui amb caràcter potestatiu, es parla de la identitat de la persona titular, cosa que ens porta a plantejar-nos si aquesta persona titular haurà d'existir necessàriament o no.

La Llei 11/2007 no resol aquesta qüestió d'una manera directa, si bé sembla admetre la possibilitat que el segell d'òrgan no estigui lligat a un titular determinat a la vista del que disposa l'article 39, d'acord amb el qual «en cas d'actuació automatitzada s'ha d'establir prèviament l'òrgan o òrgans competents, segons els casos, per a la definició de les especificacions, programació, manteniment, supervisió i control de qualitat i, si s'escau, auditoria del sistema d'informació i del seu codi font. *Així mateix, s'ha d'indicar l'òrgan que ha de ser considerat responsable als efectes d'impugnació*».

S'ha de destacar que estableix la indicació de l'òrgan que ha de ser considerat responsable als efectes d'impugnació. Això suposa l'establiment d'una ficció jurídica que permeti l'exercici del dret de reacció contra un acte produït mitjançant una actuació administrativa automatitzada, a través de la interposició del recurs corresponent.

2.4.3. *El segell d'òrgan i l'acte administratiu: principals problemes*

El segell d'òrgan trenca la concepció tradicional de l'acte administratiu com a declaració de voluntat, de judici, de coneixement o de desig, dut a terme per un òrgan administratiu a l'exercici d'una potestat administrativa (Zanobini), ja que la declaració que deriva d'un segell d'òrgan difícilment pot rebre algun dels qualificatius esmentats anteriorment.

En una primera aproximació, les declaracions de voluntat i de coneixement poden ser susceptibles d'automatització. Per contra, les declaracions de judici o de desig difícilment es poden predeterminar o programar i, consegüentment, la seva automatització es podria considerar no viable.

En resum, el segell d'òrgan obliga a replantejar-se el concepte d'acte administratiu i tota la cadena de producció d'aquesta mena d'actes. Cal afegir a això que la convivència del segell d'òrgan amb el segell d'Administració pública i el segell d'entitat de dret públic planteja problemes addicionals en cadascun d'aquests supòsits.

En relació amb el segell d'Administració pública, cal tenir present la diferenciació entre actes polítics i administratius —d'especial transcendència pel que fa a la seva revisió—,[24] la competència per executar els actes exterioritzats de forma automàtica, el control d'aquests actes i les responsabilitats que se'n poguessin derivar.

[24] El control dels actes polítics ho és tan sols en relació amb la tutela dels drets fonamentals i les llibertats públiques i l'existència d'elements reglats (article 2 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa).

En qualsevol cas, per la naturalesa mateixa dels actes polítics, que són manifestació d'una voluntat política, diferenciada de la voluntat administrativa, que lliga amb el funcionament ordinari de l'Administració, els primers difícilment es podrien automatitzar.

En definitiva, l'automatització de processos i decisions administratius lligaria més amb el concepte d'activitat administrativa estrictament dita, deixant de banda l'actuació política.

Un altre dels aspectes a considerar quan ens trobem amb l'actuació administrativa automatitzada i el segell d'òrgan és de la motivació dels actes administratius, ja que a ningú no se li escapa que els supòsits taxats de motivació dels actes administratius de l'article 54 de la Llei 30/1992 suposen, en la pràctica, configurar la motivació com la regla general.

En el cas de l'automatització administrativa, desapareix la motivació de l'acte configurada tradicionalment, perquè aquesta passa a integrar-se en el mecanisme de producció de l'actuació administrativa.

En aquest sentit, una programació concreta determina un resultat concret, i és en funció d'aquesta programació que l'acte administratiu es configura amb un contingut determinat. En definitiva, la motivació té una finalitat molt concreta, que és conèixer la raó de ser de l'actuació administrativa, i possibilitar en segona instància que l'administrat o l'administrada reaccioni davant aquesta actuació, en cas que no s'hagi adequat a les finalitats d'interès general a què les administracions públiques han d'atendre.

Per aquest motiu, si la motivació de l'acte administratiu automatitzada s'integra per una programació adequada, tan sols mitjançant la revisió d'aquesta programació es podrà reaccionar davant l'acte administratiu emès.

Aquesta possibilitat de reaccionar està condicionada pel fet que la presumpció de validesa de l'acte administratiu, aplicable igualment en l'àmbit de l'automatització, trasllada la càrrega de reaccionar a l'administrat o l'administrada. Així doncs, tractant-se de programes i aplicacions, haurem d'atenir-nos a una prova pericial tècnica que acrediti que la programació no ha estat efectuada degudament, ja que si bé la Llei d'enjudiciament civil admet qualsevol mitjà de prova que resulti útil i pertinent,[25] serà una prova pericial informàtica la més idònia per acreditar una programació adequada. Respecte a aspectes concrets (com una signatura electrònica concreta), també es podria emprar una certificació de producte o servei.

[25] Article 326.2 de la Llei d'enjudiciament civil.

Cal recordar que aquest és el criteri que recull, en matèria de signatura electrònica, l'article 3.8 de la Llei 59/2003, en redacció que hi dóna la Llei 56/2007, de 28 de desembre, de mesures d'impuls de la societat de la informació.[26]

Tots aquests elements (tipologia de l'acte, contingut de l'acte, plasmació documental), així com els subjectes que intervenen en la seva realització, són, entre d'altres, elements que integren o configuren l'acte i han de ser presos en consideració a l'hora de plantejar-ne l'automatització.

És cert que existeixen supòsits en què el segell d'òrgan pot ser d'aplicació, sense presentar problemes en la pràctica —com podria ser la foliació de l'expedient administratiu que es conté a l'article 32.2 de la Llei 11/2007—, però s'ha d'utilitzar de manera moderada i d'acord amb el principi de proporcionalitat que estableix l'apartat g) de l'article 4 de la Llei 11/2007, que exigeix «les garanties i mesures de seguretat adequades a la naturalesa i circumstàncies dels diferents tràmits i actuacions».

En aquest mateix sentit, resulta notable que l'única referència expressa a l'ús del segell per a un acte concret que fa la Llei 11/2007 al·ludeixi a la possibilitat d'automatitzar el procés de digitalització de documents en suport paper i a l'obtenció de les còpies electròniques corresponents, que es conté a l'article 30.3 de la Llei, potser amb la intenció d'evitar la necessitat que un funcionari hagi de confrontar la còpia amb l'original, un altre ús que pot resultar pacífic.

No podem desdenyar que, des del punt de vista de la responsabilitat, podria temptar el fet de deixar de banda la firma del funcionari competent a favor del segell d'òrgan o d'Administració, però el seu ús generalitzat produiria inseguretat jurídica. Això, d'altra banda, ens obliga a plantejar-nos el tipus de signatura electrònica a emprar, que, com a regla general, serà la signatura electrònica reconeguda.

[26] Article 3.8: «El suport en què estiguin les dades signades electrònicament és admissible com a prova documental en judici. Si s'impugna l'autenticitat de la signatura electrònica reconeguda amb la qual s'hagin signat les dades incorporades al document electrònic s'ha de comprovar que es tracta d'una signatura electrònica avançada basada en un certificat reconegut, que compleix tots els requisits i les condicions establerts en aquesta Llei per a aquest tipus de certificats, així com que la signatura s'ha generat mitjançant un dispositiu segur de creació de signatura electrònica.

La càrrega de realitzar les esmentades comprovacions correspon a qui hagi presentat el document electrònic signat amb signatura electrònica reconeguda. Si les esmentades comprovacions obtenen un resultat positiu, es presumeix l'autenticitat de la signatura electrònica reconeguda amb la qual s'hagi signat l'esmentat document electrònic en què les costes, despeses i drets que origini la comprovació són exclusivament a càrrec de qui hagi formulat la impugnació. Si, segons el parer del tribunal, la impugnació ha estat temerària, li pot imposar, a més, una multa de 120 a 600 euros.

Si s'impugna l'autenticitat de la signatura electrònica avançada, amb la qual s'hagin signat les dades incorporades al document electrònic, cal atenir-se al que estableix l'apartat 2 de l'article 326 de la Llei d'enjudiciament civil.»

Igualment, caldrà tenir present si l'actuació administrativa es produeix en entorns tancats o si, contràriament, produeix una eficàcia externa en relació amb el ciutadà. En cadascun d'aquests casos s'haurà d'actuar de manera diferenciada.

Tornant a la regulació legal, l'article 38.2 de la Llei 11/2007 limita l'adopció i la notificació de resolucions de forma automatitzada als procediments en què així estigui previst, però no s'estableix cap condicionant material a aquesta possibilitat, tot i que podem entendre que, com a regla general, la resolució automatitzada dels procediments administratius s'ha de justificar degudament —raó per la qual tindrà caràcter excepcional.

En qualsevol cas, caldrà atenir-se a la naturalesa dels actes i al seu contingut, i fins i tot a la regulació legal d'aquests.

A títol d'exemple, la suspensió dels actes administratius arran de la interposició d'un recurs es produeix de manera automàtica si, transcorregut el termini de trenta dies des de la sol·licitud, aquesta no ha estat resolta. A partir d'aquesta previsió legal, res no impedeix la configuració informàtica de la suspensió d'un acte administratiu en el supòsit que no s'hagi produït la resolució en el termini esmentat.

Més encara, en alguns àmbits —com el tributari— la suspensió s'entén atorgada automàticament per la simple prestació de la garantia corresponent, sense necessitat de justificar cap raó o motiu per tal de suspendre l'executivitat dels actes administratius.

D'acord amb aquesta previsió, res no impediria articular un procediment automatitzat en què, un cop constatada la prestació de la garantia esmentada, la mateixa màquina, programada degudament per la comprovació de la identitat entre la quantia objecte de reclamació i la que és objecte de garantia (amb una possible comprovació en línia), dictés una resolució que atorgués aquesta suspensió.

En aquesta línia, podem fer esment de la Resolució de 12 de juliol de 2010, de l'Instituto Social de la Marina y del Servicio Público de Empleo Estatal, per la qual es regula la tramitació electrònica automatitzada de diversos procediments en matèria de protecció per desocupació del règim especial dels treballadors del mar (BOE núm. 225, de 16 de setembre de 2010), que preveu l'automatització de determinats processos administratius no complexos.[27]

A banda dels actes resolutoris, els actes de tràmit constitueixen un àmbit de l'actuació administrativa en què l'automatització presenta múltiples possibilitats.

[27] «[...] *a) Solicitudes de alta y reanudación de las prestaciones contributivas por desempleo y de los subsidios por desempleo* [...]. *b) Solicitudes de prórrogas de los subsidios por desempleo* [...] *c)* [...] *suspensiones o extinciones del derecho*.»

Així, existeixen els actes de tràmit que, malgrat la seva naturalesa, s'adrecen de manera directa a la persona interessada (com l'acte d'incoació d'un procediment sancionador, amb la notificació corresponent), els quals, moltes vegades, tot i no ser susceptibles de recurs, requereixen una automatització complexa pel fet que es tracta de decisions de judici de l'Administració. Cal diferenciar aquests actes de tràmit dels anomenats *de direcció i impuls*, que es duen a terme a l'efecte de garantir el desenvolupament del procediment en tots els seus tràmits; sovint aquests actes no tenen una eficàcia directa envers els ciutadans, sinó que limiten els seus efectes al que seria l'esfera més interna.

Cal tenir present que en molts àmbits de l'actuació administrativa relacionada amb l'exercici de potestats ablatòries o sancionadores, en què l'exercici de l'activitat de policia està condicionada al compliment estricte de terminis per dictar i notificar l'acte, i en què el transcurs del temps determina moltes vegades la caducitat del procediment i la consegüent impunitat de la persona responsable, s'articulen sistemes de control de l'activitat amb alarmes que pretenen assegurar que la persona responsable dicti la resolució corresponent o posi fi al procediment i practiqui la notificació corresponent dins el termini establert a l'efecte.

En resum, l'automatització es podria traslladar a les actuacions reglades, fins i tot en els supòsits d'actes de caràcter constitutiu. Tanmateix, aquesta automatització només seria viable quan la decisió que cal prendre es pogués deduir d'un procés de tractament de dades programat degudament i sotmès a mesures de control i supervisió adients.

2.5. Límits de l'actuació administrativa automatitzada

No es pot deixar de banda que l'actuació administrativa ha de respondre sempre a raons d'interès general i que un límit de l'actuació administrativa, sobretot en relació amb els actes discrecionals, es configura per la prohibició de la desviació de poder, que suposa la prohibició de l'exercici de potestats administratives per a finalitats diferents de les previstes a l'ordenament jurídic.

L'existència de desviació de poder i la manca de motivació són supòsits d'anul·labilitat dels actes administratius dictats. Aquesta previsió és important, ja que l'Administració de vegades aplica l'actuació administrativa automatitzada a determinats processos i estableix models de resposta en què es preveuen totes les possibilitats. Això passa, per exemple, en les resolucions dels procediments sancionadors en matèria de trànsit, en què s'al·ludeix al fet de les al·legacions formulades, si s'escau, i el que denoten és que aquest model es pot traslladar al supòsit en què s'hagin formulat al·legacions o no o, el que és el mateix, establint una presumpció del fet que, en definitiva, l'Administració no ha tingut

en compte el contingut de les al·legacions —si han estat formulades—, sinó que practica un automatisme absolut en la decisió del procediment.

És evident que l'Administració pública ha de cercar criteris d'eficiència, però no a qualsevol preu, i menys encara quan poden resultar perjudicats drets o garanties dels administrats en el procediment administratiu en què tenen la condició de persones interessades.

D'altra banda, tal com hem subratllat, l'actuació administrativa automatitzada es pot definir com la produïda per un sistema d'informació programat adequadament sense necessitat d'intervenció d'una persona física en cada cas singular.

Això ens portaria a excloure l'actuació administrativa automatitzada de tots aquells supòsits en què hi ha discrecionalitat per part de l'Administració i a aplicar-la sols a supòsits clarament reglats. Tanmateix, no es pot ignorar que, avui dia, els actes administratius contenen diferents elements reglats i discrecionals que han de ser valorats conjuntament, la qual cosa dificulta encara més la predeterminació informàtica de la decisió administrativa.

Cal tenir en compte que els actes administratius s'han de vincular a un responsable, que pot ser objecte, arribat el cas, d'haver-se de sotmetre a responsabilitats disciplinàries. El mateix concepte de funcionari que conté l'article 24 del Codi penal no concorda amb l'admissió genèrica del segell d'òrgan ni amb les diferents tipificacions penals existents.

El segell d'òrgan també obliga a revisar el règim de recursos administratius i els mitjans d'impugnació, atès que el recurs d'alçada o de reposició, admesos com a mitjans d'impugnació, no poden ser utilitzats de manera automàtica i, en el cas del recurs de reposició, mai no seria una reposició per part del mateix "òrgan" que va decidir l'acte impugnat.

A més, ja hem comentat que el criteri general per a l'automatització de processos, en els supòsits en què està regulat actualment, passa per la decisió prèvia de l'òrgan administratiu responsable als efectes de recursos. Això comporta, en la pràctica, traslladar al mateix òrgan que ha pres la decisió d'automatitzar una actuació administrativa determinada la resolució dels recursos que es puguin interposar i, al mateix temps, deixar sense respondre què és el que passaria en els casos dels actes susceptibles de recurs d'alçada, en què l'automatització hauria estat decidida per l'òrgan que coneix del recurs d'alçada i, si s'impugnés aquesta automatització, ens trobaríem en la pràctica davant un recurs que, sent aparentment d'alçada, és objecte de coneixement per part del mateix òrgan que, pel fet que acorda l'automatització i com a responsable de la decisió, es podria considerar responsable de l'acte.

Així mateix, l'admissió del segell d'òrgan és una manifestació que la informàtica mana o pot manar i en què la persona física perd o pot perdre el control. Per aquesta raó, el règim de recursos és —o ha de ser— una garantia mínima per tal que els drets dels ciutadans en les seves actuacions davant les administracions públiques no quedin perjudicats.

Igualment, el segell d'òrgan ha de quedar exclòs de tots aquells supòsits en què hi hagi un element subjectiu, valoració o motivació en l'actuació administrativa. Altrament, s'estarien vulnerant els principis generals del procediment administratiu i, d'altra banda, es produiria una rebaixa dels drets dels ciutadans no emparada per la Llei 11/2007. Aquest seria el cas de les declaracions de judici que hem esmentat abans, com ara l'emissió d'un informe jurídic, que, òbviament, mai no podrà ser automatitzada.

A banda d'aquestes previsions relatives al contingut material o substantiu de l'acte administratiu i la viabilitat de l'automatització d'aquest, resulta necessari considerar els problemes de l'aplicació de la legislació vigent en matèria de signatura electrònica al cas particular del segell d'òrgan. En efecte, tot i que no es pot considerar que un segell d'òrgan sigui una signatura electrònica (ni avançada ni reconeguda, perquè senzillament és una institució nova i completament diferent de la firma), l'article 18 de la Llei 11/2007 determina que el segell d'òrgan ha d'estar «basat en certificat electrònic que reuneixi els requisits exigits per la legislació de signatura electrònica».

Aquesta manifestació genera alguns problemes d'aplicació pràctica, ja que la normativa de signatura electrònica està orientada a la documentació electrònica dels actes jurídics per persones físiques, per la qual cosa pot resultar complex determinar-ne l'aplicació directa.

Com a exemples particulars de problemes a resoldre en aquesta aplicació de la Llei 59/2003 podem citar els següents:

- La necessitat o no d'emprar un dispositiu segur de creació de segell (per aplicació analògica de la necessitat d'ús de dispositiu segur de creació de signatura electrònica, ex article 24 de la Llei 59/2003).
- El tractament dels límits d'ús dels certificats de segell d'òrgan, possibilitat que ens sembla, més que convenient, absolutament necessària per evitar possibles abusos del segell, especialment en cas de robatori d'aquest.
- El tractament de la representació legal tenen determinats òrgan, que, en el cas del segell, potser s'hauria de limitar de manera expressa.

En resum, correspon a cada Administració determinar els supòsits i els tràmits en què es pot aplicar el segell d'òrgan, si bé aquesta determinació no es pot dur a terme indiscriminadament, sinó a partir d'una valoració adequada dels actes administratius que es poden fer de forma automatitzada, d'acord amb el principi de proporcionalitat, i sense que es produeixi una minva de garanties de l'administrat o l'administrada.

Una qüestió que també cal considerar respecte a l'actuació administrativa automatitzada és la que deriva del tractament de dades de caràcter personal. Tal com assenyala Valero Torrijos,[28] en relació amb els actes administratius discrecionals l'automatització ha de tenir en compte el marge de decisió de què disposa l'òrgan administratiu per adoptar la decisió. També s'ha de tenir present la previsió de l'article 13 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, conforme al qual es reconeix el dret dels ciutadans «a no estar sotmesos a una decisió amb efectes jurídics, sobre ells o que els afecti de manera significativa, que es basi únicament en un tractament de dades destinades a avaluar determinats aspectes de la seva personalitat», legitimant-los per impugnar els actes administratius que impliquin una valoració del seu comportament, el fonament únic del qual sigui un tractament de dades de caràcter personal que ofereixi una definició de les seves característiques o de la seva personalitat.

2.6. Nul·litat o anul·labilitat de l'actuació administrativa automatitzada

Fins ara hem tractat els diferents elements o criteris jurídics que s'han de considerar a l'hora d'automatitzar els processos. La manca de compliment d'aquests criteris significa un vici o un defecte que, en funció dels supòsits, pot afectar l'acte emès, la qual cosa ens porta a analitzar la invalidesa dels actes jurídics.

La teoria de la invalidesa dels actes jurídics és pròpia de la part general del dret civil i comuna per a totes les branques jurídiques. Així, l'article 6.3 del Codi civil estableix que «*los actos contrarios a las normas imperativas y a las prohibitivas son nulos de pleno derecho, salvo que en ellas se establezca un efecto distinto para el caso de contravención*».

Aquesta disconformitat respecte a la llei o aquesta invalidesa pot provenir:

1) De la manca d'algun element essencial per a la formació de l'acte o el negoci jurídic (inexistència).

[28] Valero Torrijos, J. *El régimen jurídico de la e-Administración*. Granada: Ed. Comares, 2a edició, 2007, pàg. 75.

2) De la celebració d'un acte viciant, un mandat o una prohibició legal (nul·litat de ple dret).
3) De l'existència d'un vici o un defecte de l'acte (nul·litat relativa o anul·labilitat).

Podem traslladar aquesta distinció a l'àmbit administratiu, amb alguns matisos:

1) En primer lloc, en dret administratiu la teoria de la invalidesa s'esgota en l'estudi de dues úniques categories: nul·litat absoluta i anul·labilitat. Així, autors com Garrido Falla assenyalen que el tractament jurídic de la inexistència no s'ha de diferenciar del de la nul·litat absoluta.

2) En segon lloc, a diferència del que passa en el dret comú, en dret administratiu la regla general està constituïda, doncs, per la presumpció de validesa de totes les actuacions administratives, i per això mateix l'acte administratiu invàlid està dominat per la regla bàsica de l'anul·labilitat, mentre que la nul·litat de ple dret es reserva als supòsits indicats taxativament a l'article 62 de la Llei 30/1992 o en una disposició de rang legal que la reguli expressament amb aquest caràcter.

3) En tercer lloc, existeixen vicis que ni tan sols no donen lloc al vici de l'anul·labilitat, com ara les irregularitats no invalidants (article 63.2 de la Llei 30/1992).

4) Finalment, el principi del *favor acti* no solament limita la nul·litat i crea les irregularitats no invalidants, sinó que facilita tècniques de garantia de conservació de l'acte.

En aquest sentit, ja hem indicat que la regla general és l'anul·labilitat. La nul·litat s'aplica exclusivament en els supòsits que fixa taxativament la llei, que són els enumerats a l'article 62.1 de la Llei 30/1992.[29]

Si traslladem els conceptes de la invalidesa dels actes administratius a l'actuació administrativa automatitzada, hem de distingir els supòsits que es poden produir, ja que la conseqüència jurídica que deriva de cadascun també és diferent.

[29] Article 62.1 de la Llei 30/1992:
«Els actes de les administracions públiques són nuls de ple dret en els casos següents:
a) Els que lesionin els drets i les llibertats susceptibles d'empara constitucional.
b) Els que dicti un òrgan manifestament incompetent per raó de la matèria o del territori.
c) Els que tinguin un contingut impossible.
d) Els que siguin constitutius d'infracció penal o es dictin com a conseqüència d'aquesta.
e) Els que es dictin prescindint totalment i absolutament del procediment establert legalment o de les normes que contenen les regles essencials per a la formació de la voluntat dels òrgans col·legiats.
f) Els actes expressos o presumptes contraris a l'ordenament jurídic per part dels quals s'adquireixen facultats o drets quan no es tinguin els requisits essencials per a la seva adquisició.
g) Qualsevol altre que estableixi expressament una disposició de rang legal.»

Ja hem advertit que, d'acord amb la doctrina de les potestats administratives, qualsevol actuació ha d'estar emparada en una norma habilitadora, la qual en un primer nivell es configura per una norma amb rang de llei habilitadora i una norma de segon nivell que en concreta les condicions d'aplicació.

Aquest principi, aplicable amb caràcter general a la realització d'actes administratius per mitjans electrònics, es pot traslladar igualment a l'actuació administrativa automatitzada. Per això cal que l'actuació administrativa automatitzada estigui emparada en una habilitació suficient: si aquesta no es produeix, es trenca la regularitat del mecanisme de producció d'actes administratius.

Aquest vici entraria en la consideració d'invalidesa absoluta i, traslladada a l'àmbit del dret administratiu, determinaria un supòsit de nul·litat absoluta, ja sigui per considerar que es tracta d'un acte dictat per un òrgan manifestament incompetent (lletra b de l'article 62.1), ja sigui per un supòsit de prescindir totalment del procediment (lletra e del mateix article).

Tot plegat significa que una automatització de processos feta al marge dels criteris establerts per la normativa habilitadora o que no s'adeqüés a aquesta normativa seria incardinable en un supòsit de nul·litat de ple dret.

Aquesta nul·litat de ple dret suposa:

1) La impossibilitat de convalidació, ja que aquesta només és predicable dels actes anul·lables.

2) La suspensió automàtica de l'executivitat de l'acte nul de ple dret quan és impugnat al·legant aquesta nul·litat (article 111 de la Llei 30/1992).

3) La possibilitat que l'Administració declari d'ofici la nul·litat, previ dictamen favorable del Consell d'Estat o òrgan consultiu equivalent de la comunitat autònoma. En canvi, si es tracta d'actes anul·lables, l'Administració els haurà de declarar lesius per a l'interès públic i, posteriorment, els haurà d'impugnar davant l'ordre jurisdiccional contenciós administratiu.

4) Els efectes de la declaració són *ex tunc*, és a dir, des de la data en què es dicta l'acte. Per contra, l'anul·labilitat produeix efectes *ex nunc*, és a dir, des de la data en què es declara.

Així doncs, la regla general seria la nul·litat de ple dret, vici determinant de l'actuació administrativa que, en l'àmbit de la utilització dels mitjans electrònics, és especialment significatiu atesa la manca de confiança que la utilització d'aquests mitjans encara genera actualment entre els administrats.

D'altra banda, ens podríem plantejar la possibilitat d'anul·labilitat de les actuacions administratives dutes a terme, la qual es podria produir en els supòsits d'una programació inadequada. Això deriva del caràcter restrictiu que es predica de la nul·litat de ple dret, aplicable exclusivament als supòsits abans esmentats. Per contra, una programació inadequada es consideraria o es podria considerar una causa d'anul·labilitat, recollida a l'article 63 de la Llei 30/1992.[30]

En canvi, una programació indeguda o qualsevol altre defecte no es podria considerar actuació administrativa irregular, ja que difícilment es produirien els supòsits legalment previstos a aquest efecte.[31]

Finalment, es podria produir una desviació informàtica de poder, cosa que implicaria traslladar al camp de la informàtica decisional la doctrina de la desviació de poder.[32] En aquest sentit, la desviació de poder, configurada com a supòsit d'anul·labilitat, tindria lloc quan la programació dels programes i les aplicacions que han de dur a terme l'actuació administrativa automatitzada corresponent, tot i que aparentment s'adequa a la legalitat aplicable, s'ha realitzat per a una finalitat o persegueix una finalitat diferent de la que preveu l'ordenament jurídic.

Aquesta finalitat que esdevindria desviació de poder pot ser privada, però també pública: seria pública quan la finalitat perseguida fos diferent de la prevista i fixada per la norma que atribueix la potestat corresponent. Seria el cas, per exemple, en què una automatització determinada no perseguís una millora en la prestació dels serveis envers els ciutadans, sinó privar-los de l'exercici de drets o de garanties que els reconeix l'ordenament jurídic.

En aquests casos, ja hem indicat que la sanció seria la de l'anul·labilitat. No obstant això, pel fet que es tracta de l'element psicològic o volitiu que guia l'actuació administrativa,

---

[30] Article 63 de la Llei 30/1992*:* «1. Són anul·lables els actes de l'Administració que incorren en qualsevol infracció de l'ordenament jurídic, fins i tot la desviació de poder.
2. No obstant això, el defecte de forma només determina l'anul·labilitat quan l'acte no té els requisits formals indispensables per a aconseguir el seu fi o dóna lloc a la indefensió de les persones interessades.»

[31] Serien: 1) Actes mancats dels requisits formals no indispensables per tal d'assolir la seva finalitat i que no originin indefensió. 2) Actuacions administratives realitzades fora del temps establert, que només implicaran l'anul·labilitat de l'acte quan així ho imposi la naturalesa del terme o termini. 3) Actuació d'autoritats i personal al servei de les administracions públiques quan concorrin motius d'abstenció, que no implicarà necessàriament la invalidesa dels actes en què hagin intervingut (article 28.3 de Llei 30/92), sens perjudici, quan escaigui, de la responsabilitat.

[32] Cal recordar que la desviació de poder es defineix com l'exercici de les potestats administratives per a finalitats diferents de les previstes a l'ordenament jurídic. En definitiva, es tracta d'aquells supòsits en què l'Administració se separa de la persecució de l'interès general que ha de guiar la seva actuació.

acreditar-ne l'existència és certament dificultós, malgrat que no s'exigeix jurisprudencialment una prova plena.

3. TÈCNIQUES DE DETERMINACIÓ DE LA VIABILITAT INFORMÀTICA DE L'ACTUACIÓ ADMINISTRATIVA A AUTOMATITZAR

L'activitat de les administracions públiques s'ha de desenvolupar amb un grau elevat de garanties per als ciutadans, com a contrapunt dels poders exorbitants de què disposen per tal de poder complir amb la seva funció.

L'actuació administrativa automatitzada, com hem analitzat al capítol anterior, genera una sèrie de riscos particulars que cal adreçar suficientment per evitar que aquesta nova possibilitat esdevingui font de conflictes i problemes d'ineficàcia.

Cal recordar que l'annex de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, defineix l'actuació administrativa automatitzada com l'«actuació administrativa produïda per un sistema d'informació adequadament programat sense necessitat d'intervenció d'una persona física en cada cas singular. Inclou la producció d'actes de tràmit o resolutoris de procediments, així com de mers actes de comunicació».

Com hem vist, el requisit essencial per poder dur a terme una actuació administrativa automatitzada és la programació adequada del sistema d'informació, concepte jurídic indeterminat que cal omplir de contingut, ja que una programació inadequada podria implicar l'anul·lació —en el millor dels casos— d'un o de tots els actes singulars dictats de forma automatitzada.

En aquest sentit, també resulta convenient recordar que el *Gran diccionari de la llengua catalana* defineix el terme *adequat, -ada* com «apropiat, proporcionat, completament suficient, a un objecte, a un fi, a un propòsit». Així doncs, resultarà necessari, en principi, garantir que la interpretació de la norma que es codifica informàticament és prou completa per no produir discriminació al ciutadà afectat per l'acte singular, com veurem posteriorment.

Tot i que la Llei 11/2007 no defineix legalment el concepte de *sistema d'informació*, sí que aporta una definició d'*aplicació*, en el sentit de «programa o conjunt de programes l'objecte dels quals és la resolució d'un problema mitjançant l'ús d'informàtica» —en aquest cas, la necessitat d'efectuar un acte administratiu singular, sigui decisori, de constància, etc.

El primer pas per arribar a una programació adequada d'una aplicació és precisament la interpretació "informàtica" de la norma reguladora de l'actuació administrativa a automatitzar, aspecte del qual ens ocupem a continuació.

3.1. La interpretació de les normes jurídiques

El problema de la interpretació de les normes de dret privat ha estat abordat amb profunditat per Castán,[33] que, seguint Savigny, introdueix les modalitats principals de la interpretació i identifica els elements principals del procés d'interpretació:

- L'element literal o filològic, que constitueix el primer estadi del procés interpretatiu, perquè, en expressar la llei amb paraules,[34] cal obtenir el significat verbal que en resulti, d'acord amb les regles gramaticals.

  En cas de conflicte de possibles significacions, caldrà escollir, en general, el significat que es reputi més idoni per raó de connexió amb altres termes del precepte interpretat o de la matèria de què es tracti.

  Així mateix, tradicionalment s'ha considerat que quan un terme té un significat comú i un altre de tècnic, en general cal escollir el significat comú, atès que la norma s'adreça a una generalitat de persones. Aquest aspecte ha generat l'aparició de definicions «als efectes d'aquesta norma» de manera més o menys generalitzada, sobretot en els sectors de l'ordenament jurídic més tecnificats, com ara el dret administratiu —per contrast amb el dret privat, per exemple—, el dret tributari i la Seguretat Social.

- L'element lògic, racional o teleològic, que completa i controla els resultats de la interpretació gramatical. La interpretació lògica s'efectua atenent als elements de la fórmula legislativa (lògica interna) i als elements que formen el pressupòsit de la norma (lògica externa). Mentre que la lògica interna implica el conjunt de deduccions i induccions que permet comprendre la voluntat del legislador (*ratio legislatoris*), la lògica externa és un procés més profund orientat a comprendre el fonament i la finalitat essencial de la norma (*ratio legis*), així com l'oportunitat d'aquesta norma (*occasio legis*).

  Posteriorment abordarem amb més profunditat la interpretació lògica, per la seva íntima relació amb l'automatització de l'aplicació de la norma.

[33] José Castán Tobeñas. *Teoría de la aplicación e investigación del derecho. Metodología y técnica operatoria en derecho privado positivo*. Madrid: Instituto Editorial Reus, 1947.

[34] I, en concret, sovint en llenguatge natural, poc definit i que presenta possibles ambigüitats, vaguetats i altres problemes pel que fa a una interpretació adequada.

- L'element sistemàtic, que consisteix a relacionar la norma que cal interpretar amb aquelles altres que integren una institució jurídica, i cada institució amb la resta, fins a arribar als principis fonamentals del sistema jurídic.

- L'element històric, que permet millorar la comprensió de la norma en consideració als precedents històrics, siguin remots o immediats, així com als treballs preparatoris de la llei (encara que gairebé tota la doctrina considera que aquests darrers tenen un valor molt relatiu).

- L'element comparatiu, que consisteix a analitzar la norma d'acord amb el dret comparat sempre com a mitjà subsidiari en la interpretació.

- L'element sociològic, que permet considerar la norma a la llum de les exigències de la vida real i dels interessos i les necessitats de la col·lectivitat.

- L'element pràctic (tècnic i econòmic), que consisteix a analitzar la norma d'acord amb l'element de fet que la norma disciplina, i que tracta d'elements de naturalesa tècnica o del substrat econòmic de les relacions jurídiques. Es tracta d'un factor inclòs en els elements lògic i sociològic de la interpretació.

Quant a les regles d'interpretació, Castán diferencia les regles legals de les regles doctrinals, bo i advertint de la necessitat d'aplicar les regles doctrinals i, en particular, els aforismes jurídics amb molta cautela. Finalment, Castán identifica els quatre tipus d'interpretació que es detallen tot seguit, segons la funció que compleixen:

- Interpretació declarativa, que s'adreça a explicar el text de la llei, especialment quan presenta ambigüitats, obscuritats o vaguetats. Aquesta interpretació pot ser estricta o lata segons que es doni un sentit més limitat o més ampli a un terme concret, d'acord amb la resta de termes de la norma a interpretar.

- Interpretació restrictiva, que ofereix com a resultat restringir el significat dels termes legals quan expressen més del que va voler el legislador. Seria procedent en casos com els següents: si el text contradiu un altre text de la llei, si la llei conté una contradicció o si la norma, sense interpretació restrictiva, va més enllà de la finalitat per a la qual va ser ordenada.

- Interpretació extensiva, que amplia el significat natural dels termes legals quan expressen menys del que va voler el legislador. Escauria en casos com els següents: si la llei adopta una expressió concreta en lloc d'una expressió abstracta més adient per a la finalitat perseguida per la norma o si la llei enuncia un

concepte general que aplica per via indicativa o demostrativa a casos particulars (incloent-hi els arguments per identitat de raó i *a fortiori*).

- Interpretació modificativa, que opera quan l'expressió literal de la norma dóna a entendre quelcom qualitativament diferent d'allò volgut pel legislador, i que fonamentaria casos d'inaplicació legal o de desplaçament de l'aplicació de les normes en casos de conflicte. Val a dir que es tracta d'un tipus d'interpretació que la doctrina considera aplicable, en general, a la millora d'una expressió normativa concreta, igual que succeeix amb les interpretacions restrictiva i extensiva.

En paraules de Castán, la interpretació no és una operació mecànica en què no existeix un cert marge de llibertat i discrecionalitat, tot i que en qualsevol cas es tracta d'un acte de ciència, i no polític; una justa ponderació dels elements gramaticals, logicosistemàtic, històric i finalista o teleològic, que sembla la forma més segura d'arribar a una interpretació que posseeixi un valor de veritat i rectitud (Legaz).

Paral·lelament, Castán adverteix dels perills associats a una construcció purament lògica de les normes jurídiques, la qual podria arribar a reduir la ciència jurídica a una espècie de matemàtica del dret (Hernández-Gil), advertiment que compartim plenament i que la doctrina iusfilosòfica més autoritzada ha mostrat posteriorment.

3.2. La interpretació lògica de les normes

Ateses la importància de la interpretació lògica i la seva íntima connexió amb el llenguatge informatitzat, a continuació exposem algunes de les perspectives que ha treballat la doctrina científica més recent.

La lògica és la ciència que estudia sistemàticament els enunciats vàlids o formalment veritables (entenent que un enunciat és formalment veritable si són veritables tots els enunciats que tenen el mateix esquema lògic) o que tracta de la relació de conseqüència entre enunciats. A més, però, de la lògica pròpiament dita, actualment hom inclou dins el títol de lògica les investigacions metalògiques, les quals comprenen la teoria de la deducció o l'estudi de les propietats dels conjunts d'axiomes i la semàntica formal.

En altres paraules, podem dir que la lògica és l'estudi dels raonaments ben fets. La lògica analitza l'estructura dels raonaments i assenyala les condicions de la seva validesa. Per tant, és el procediment sistemàtic i fundat que ens permet diferenciar un raonament correcte, o vàlid, d'un altre d'incorrecte, o invàlid. Així doncs, és també l'estudi de la deducció lògica o de la inferència lògica.

Es pot parlar de l'inici de la lògica moderna a partir de l'àlgebra de Boole, interpretable com a lògica de classes i d'enunciats. De Morgan i Peirce crearen la lògica de relacions. Frege introduí els quantificadors, donà la primera versió sistemàtica i enterament formalitzada del càlcul de predicats i emprengué la reducció de l'aritmètica a la lògica. Russell i Whitehead imposaren, a *Principia mathematica* (1910-1913), el simbolisme més simple de Peano i evitaren la inconsistència del sistema de Frege amb la teoria dels tipus.

Quant a les investigacions metalògiques, és impossible d'exagerar la importància del descobriment de Gödel sobre la completesa del càlcul de predicats de primer ordre (1930) i la incompletesa de les lògiques d'ordre superior (1931). La resposta a la qüestió sobre la decidibilitat de la lògica, descrita per Hilbert com la més important, la va donar Churz (1936) com a negativa pel que fa a la lògica de predicats de primer ordre, però hom continua investigant, amb resultats positius, la decidibilitat de classes de fórmules.

Per *semàntica* hem d'entendre la part de la lògica que correspon a l'àmbit del que s'anomena *metalògica* i que estudia els sistemes lògics des del punt de vista de les seves possibles interpretacions, principalment la interpretació normal, o pensada en elaborar el sistema, si és que tal interpretació existeix. Anomenada també *teoria dels models*, la semàntica dels llenguatges formals s'ha de distingir de la *semàntica lingüística* o *semàntica dels llenguatges naturals*. Per bé que l'estudi sistemàtic de la semàntica lògica és posterior a l'estudi dels problemes sintàctics i és obra sobretot de Tarski i de Carnap, algunes nocions semàntiques són tan antigues com la mateixa lògica i es poden trobar ja en Aristòtil.

La semàntica moderna té els seus precedents en Bolzano i Frege, i és amb Tarski que assoleix els seus fonaments, per tal com aquest autor es proposa definir la noció de *veritat* només per als llenguatges formals d'estructura totalment explícita i, així, definir prèviament la noció de *compliment*, o *satisfacció*, per a les fórmules elementals, de donar després una definició recursiva de *satisfacció* per a tota classe de fórmules i d'oferir finalment la noció de *veritat* per a oracions o fórmules sense variables lliures. L'obra de Tarski va permetre emprendre amb rigor l'estudi del caràcter de satisfacció i de completesa, com també dels models, dels sistemes axiomàtics, com veurem més endavant.

Concretant una mica més, García González[35] indica que la lògica va ser desenvolupada en un intent de crear un llenguatge universal basat en principis matemàtics, de manera que es basa en principis formats que haurem de tenir en compte a l'hora de considerar si un

[35] Roberto García González. *A Semantic Web Approach to Digital Rights Management. Ph.Thesis*. Barcelona: Universitat Pompeu Fabra, 2005.

llenguatge de representació del coneixement (per exemple, d'un conjunt de normes que ordenen una actuació que automatitzem) és una lògica:

- Vocabulari: col·lecció de símbols representats com a caràcters, paraules, icones o sons, símbols que es divideixen en quatre grups:
    - Símbols lògics, que són independents del domini de coneixement, com poden ser qualificadors com "$\forall$" o connectives com "$\wedge$".
    - Constants, que són independents del domini de coneixement i identifiquen individus, propietats o relacions en aquest domini o univers de discurs, com per exemple "representant de".
    - Variables, que són símbols il·limitats aplicats d'acord amb els quantificadors.
    - Símbols de puntuació, que separen o agrupen altres símbols, com les comes i els parèntesis.

- Sintaxi: una lògica ha de tenir regles gramaticals que determinin com es combinen els símbols per formar sentències correctes.

- Semàntica: és necessari realitzar manifestacions amb significació, la qual cosa comprèn una teoria de referència que determini com es relacionen les constants i les variables amb els objectes en l'univers de discurs. A més, inclou una teoria de la veritat que permet diferenciar manifestacions veritables de manifestacions falses.

- Inferència: es duu a terme mitjançant regles que determinen com es generen uns patrons a partir dels altres, cosa que permet mecanismes de raonament i la generació de nou coneixement, a més de poder justificar com s'ha arribat a una conclusió.

Un llenguatge formal o un càlcul lògic permet decidir:

1. Si un símbol pertany al llenguatge.

2. Si una fórmula determinada és una expressió ben formada del llenguatge.

3. Si una seqüència sintàctica de fórmules constitueix una demostració o una deducció. En tot cas, un càlcul o un procediment de deducció posa de manifest que tot raonament vàlid equival a una expressió lògica que sempre és verdadera. Una expressió tal és una «veritat lògica» o una «veritat formal».

La lògica d'enunciats o proposicions i la lògica de predicats —coneguda també per *lògica de primer ordre*— són dos llenguatges lògics formals. La distinció entre l'un i l'altre es basa en la diferent capacitat expressiva del llenguatge. Els símbols (alfabet) del llenguatge de lògica proposicional es refereixen, bàsicament, a enunciats i a connexions entre enunciats, i deixen intacta la seva estructura interna, mentre que els símbols (alfabet) de la lògica de predicats penetren a l'interior dels enunciats i fan referència als termes de què es componen els enunciats.

3.3. Els llenguatges de la lògica

Avui dia, gairebé tots els llenguatges de la lògica s'ordenen al voltant de la lògica de primer ordre i es poden classificar d'acord amb sis paràmetres (García González):

- Sintaxi: la diferència més òbvia —però menys important— entre els diferents llenguatges lògics és la notació que fan servir, ja que, en termes de potència expressiva, les diferències sintàctiques no són rellevants.

  La lògica de primer ordre tipada és una extensió sintàctica de la lògica de primer ordre, té idèntica semàntica i existeixen substitucions sintàctiques directes per traduir entre elles:

  $(\forall x{:}t)\ \varphi(x) \equiv (\forall x)(t(x) \rightarrow \varphi(x))$ i $(\exists x{:}t)\ \varphi(x) \equiv (\exists x)(t(x) \wedge \varphi(x))$.

- Operadors: cada llenguatge lògic defineix un conjunt d'operadors permesos o de combinacions entre aquests.

  La lògica de primer ordre disposa dels operadors comuns de Boole: conjunció ($\wedge$), disjunció ($\vee$), negació ($\neg$), implicació ($\rightarrow$) i equivalència ($\equiv$), més els quantificadors universal ($\forall$) i existencial ($\exists$). També es poden introduir alguns quantificadors estesos:

  Exactament un quantificador: $\exists!$, $(\exists!x)\ \varphi(x) \equiv (\exists x)(\varphi(x) \wedge \neg(\exists y)(\varphi(y) \wedge y \neq x))$.
  Quantificador existencial únic: $\exists!!$, $(\forall x)(\exists!!y)\ \psi(x,y) \equiv (\forall x)(\exists!y)(\psi(x,y) \wedge \neg(\exists z)(\psi(z,y) \wedge z \neq x))$.

La lògica de Horn és un subconjunt de la lògica de primer ordre que no té disjunció ($\vee$) en les conclusions de la implicació ($\rightarrow$).

La lògica d'enunciats o proposicional també és un subconjunt de la lògica de primer ordre, sense quantificadors.

- Teoria demostrativa: diferents llenguatges lògics restringeixen o amplien les proves permeses. La lògica lineal restringeix la prova i permet que cada proposició només s'utilitzi un cop en una demostració; la lògica no monòtona, en canvi, estén els procediments de prova introduint assumpcions per defecte que resulten consistents amb el que es coneix en cada moment, i que podrien ser refutades. La lògica vencible (*defeasible logic*) n'és un bon exemple.

- Teoria del model: defineix de quina manera la lògica es relaciona amb el món, per exemple mitjançant els valors de veritat de les manifestacions lògiques. La lògica de primer ordre opera amb els valor veritat/fals, mentre que la lògica difusa és multivaluada i empra factors de certesa, des de 0.0, que és certament veritat, fins a 1.0, que és certament fals.

- Ontologia: una lògica no interpretada no té predicats predefinits per representar cap subjecte, sinó que només disposa de símbols i quantificadors, operadors de Boole i variables. En la pràctica, per facilitar-ne l'ús, alguns llenguatges lògics inclouen predicats i axiomes predefinits en forma d'ontologies natives. La teoria de conjunts s'utilitza per oferir fonaments matemàtics, mentre que la lògica temporal i la lògica dinàmica ofereixen ontologies temporals.

- Metallenguatge: és un llenguatge sobre el llenguatge. Es pot fer servir per definir, modificar o estendre qualsevol altre llenguatge.

  La lògica de primer ordre es pot fer servir com a metallenguatge de qualsevol altre llenguatge lògic, incloent-hi la mateixa lògica de primer ordre.

  La lògica modal és una extensió metalingüística de la lògica de primer ordre. Introdueix verbs auxiliars que, en lloc de descriure el món tal com és, descriuen el món tal com ha de ser o hauria de ser o bé com pot ser o podria ser. Els operadors modals s'interpreten com obligació ($\Box$) i permís ($\Diamond$).

  La lògica modal bàsica assumeix dos modes:

  p ha de ser necessàriament cert (ha de): $\Box p \equiv \neg \Diamond \neg p$.
  p pot ser possiblement cert (pot): $\Diamond p \equiv \neg \Box \neg p$.

La lògica deòntica s'enquadra dins la lògica modal i resulta, com veurem, particularment apropiada per als entorns normatius, com el sistema legal. A causa del fet que les lleis poden ser infringides (tot i que existeixin sancions previstes), no es pot considerar que res obligatòriament veritat sigui veritat, de forma que cal assumir el mode següent:

Qualsevol cosa obligatòriament certa és permissivament certa; és a dir, qualsevol cosa obligatòria està permesa: $\Box p \rightarrow \Diamond p$.

Pel que fa a la lògica com a mètode d'interpretació objectiu de la norma jurídica, hem de presentar breument la temàtica de la inferència lògica, que es pot dur a terme mitjançant deduccions, abduccions, induccions i analogies, com exposem a continuació:

- La deducció —anomenada també *inferència lògica* perquè és un tipus de raonament que tracta de capturar la lògica— té com a principal característica que preserva la veritat tal com determina la semàntica, de forma que, de premisses veritables, garanteix una conclusió també veritable. Les lògiques que permeten aquest tipus de raonament s'anomenen *lògiques consistents*.

  Els tests semàntics, establerts per l'operador d'implicació lògica o conseqüència lògica $\models$, ofereixen criteris per avaluar les regles d'inferència. La conseqüència lògica opera en el nivell notacional, mentre que la inferència opera en el nivell referencial. Les regles d'inferència defineixen l'operador de demostrabilitat $\vdash$, que indica que alguna cosa es pot provar.

  La implicació lògica és més fonamental que la demostrabilitat, perquè deriva la veritat de les fórmules dels fets sobre el món. La demostrabilitat depèn de les regles d'inferència d'una versió particular de la lògica, i aquestes regles han de ser justificades en termes d'implicació lògica. Així, les propietats desitjables de la inferència són:

  - La satisfacció, que significa que tot allò demostrable és veritat. Les regles d'inferència són consistents si la demostrabilitat $\vdash$ preserva la veritat com determina la implicació lògica semàntica $\models$.

    $(\forall s{:}\text{Situació})(\forall p,q{:}\text{Proposició})\ (s \models p \rightarrow (p \vdash q \rightarrow s \models q))$.

  - La completesa, que és el revers de la satisfacció, de manera que tot el que és veritat es pot demostrar.

$(\forall s{:}\text{Situació})(\forall p,q{:}\text{Proposició})\ ((s \models p \rightarrow s \models q) \rightarrow p \vdash q))$.

Les regles d'inferència en lògica proposicional, sense quantificadors, són les següents:

Modus ponens: de p i p→q, en deriva q.
Modus tollens: de ¬q i p→q, en deriva ¬p.
Sil·logisme hipotètic: de p→q i q→r, en deriva p→r.
Sil·logisme disjuntiu: de p $\vee$q i ¬p, en deriva q.
Conjunció: de p i q, en deriva p $\wedge$q.
Addició: de p, en deriva p $\vee$q.
Sostracció: de p $\wedge$q, en deriva p.

Les regles d'inferència per a la deducció amb quantificadors són les que mostrem tot seguit. Juntament amb les anteriors, conformen les regles deductives de la lògica de primer ordre:

Instanciació universal: de $(\forall x)\ \varphi\ (x)$, en deriva $\varphi\ (c)$, on c és qualsevol constant.
Instanciació existencial: de $\varphi\ (c)$, en deriva $(\exists x)\ \varphi\ (x)$.
Retirada de quantificadors: si x no està lliure en φ, aleshores de $(\exists x)\ \varphi$ deriva φ, i de $(\forall x)\ \varphi$ deriva φ.
Addició de quantificadors: de φ deriva $(\forall x)\ \varphi$ o $(\exists x)\ \varphi$, on x és qualsevol variable.
Substitució d'iguals per iguals: dels termes s i t on s = t, en deriva φ (t) de φ (s).

- L'abducció és un procés de generació d'explicacions possibles, i no es pot considerar un mètode vàlid d'inferència perquè permet conclusions falses. Es podria resumir amb la fórmula següent: de b $\wedge$ a → b aleshores potser a.

- La inducció és un procés d'inferència involucrat en l'aprenentatge que tracta d'anticipar com es comportarà un sistema. D'una sèrie d'actes, en produeix una generalització. No es pot considerar tampoc un mètode vàlid d'inferència perquè no garanteix la veritat, i requereix la retracció de proposicions quan es troben contradiccions. Es pot expressar amb la fórmula següent: de P (a), P (b)… conclou $(\forall\ x)\ P\ (x)$.

- L'analogia és una combinació d'inducció de segon ordre amb la deducció que no preserva la veritat ni la falsedat. Tot i això, resulta molt útil per a la l'argumentació o el raonament basat en casos. Es pot expressar amb la fórmula següent: de $P(a) \rightarrow P(b) \wedge R(a) \rightarrow R(b)$ potser $Q(a) \rightarrow Q(b)$.

Resulta evident anticipar la importància de l'aspecte lògic i semàntic en relació amb els sistemes d'actuació administrativa automatitzada, en consideració a les necessitats de satisfacció i completesa en la interpretació de la norma o conjunt de normes a aplicar de forma automàtica, per tal de complir el criteri de programació adequada.

En l'àmbit informàtic en general i, per tant, en el que ara ens interessa, el llenguatge lògic de base a emprar és la lògica de predicats de primer ordre, si bé veurem que s'han definit també altres llenguatges lògics d'aplicació més específica a la comprensió de la norma (lògica deòntica) o del procés de raonament jurídic argumentador no monòton (lògica refutable), que en general són representables mitjançant lògica de primer ordre. Així mateix, quant a la representació del coneixement jurídic, la lògica descriptiva serà un aspecte de rellevància notable, a més d'una eina molt eficient per descriure els elements del problema jurídic que tracta el sistema d'actuació administrativa automàtica.

3.4. La lògica en la doctrina jurídica recent

Malgrat que al final de la primera meitat del segle XX la doctrina jurídica parlava de manera general d'una crisi important del dret i, com a connexió amb aquesta, del descrèdit de totes les formes de positivisme i, per tant, de la lògica jurídica, alguns desenvolupaments de la teoria del dret a partir de la Segona Guerra Mundial han implicat un nou interès pels estudis de lògica jurídica, partint de la filosofia analítica i, en particular, de la problemàtica de l'anàlisi del llenguatge de l'Escola d'Oxford, en el context més general de l'estudi de la lògica de la ciència tractada en el Cercle de Viena fundat per Moritz Schlick, com exposa Beuchot.[36]

Fassò[37] ha detallat el ressorgiment de l'interès per l'anàlisi lògica del llenguatge, incloent-hi el llenguatge jurídic. Kelsen —en la seva darrera etapa—, Ross i Hart són bons exemples de la recepció parcial de la filosofia analítica, la qual es mostra en la seva preocupació per clarificar el funcionament dels instruments lingüístics de la recerca i determinar l'ús correcte d'aquests instruments. La filosofia analítica i del llenguatge ha

[36] Mauricio Beuchot. *Historia de la filosofía del lenguaje*. Mèxic: Fondo de Cultura Económica, 2006.
[37] Guido Fassò. *Historia de la filosofía del derecho (3). Siglos XIX y XX*. Madrid: Pirámide, 1988.

tingut un impacte considerable en la metodologia de la interpretació del dret i de la mateixa teoria del dret.

Després del seu contacte amb els neopositivistes dels Estats Units d'Amèrica, Kelsen arribarà a reconèixer que entre l'acte de voluntat —que és un fet i, doncs, un ésser— i la validesa de la forma —que és un haver d'ésser— existeix un nexe, i que la validesa és el significat de l'acte de voluntat, cosa que implica que la norma és la forma lògica d'un mandat.

Com indica Pérez Luño,[38] Kelsen distingeix la proposició normativa de la norma jurídica: mentre que aquesta darrera suposa una prescripció establerta per l'autoritat jurídica, la proposició jurídica és un judici formulat per la doctrina en què es descriu la norma. L'"haver d'ésser" que hi ha en tots dos termes (proposició normativa i norma jurídica) és diferent: prescriptiu en la norma jurídica i simplement descriptiu en la proposició normativa. Això implica que una proposició normativa pugui ser considerada veritable o falsa en funció de la correspondència del seu contingut amb la realitat normativa descrita, i que la norma jurídica només pugui ser vàlida o invàlida, però que no tingui sentit predicar d'una norma el caràcter de veracitat o falsedat, cosa que implicaria la impossibilitat d'una lògica de les normes.

Ross considera la normativitat del dret una classe de llenguatge que constitueix un fenomen real: així, un sistema de normes és vàlid si és idoni per funcionar com un esquema d'interpretació del conjunt d'accions socials corresponent, de tal manera que sigui possible comprendre aquest conjunt d'accions com un tot coherent de significats i motivació, i que dins aquest conjunt sigui possible, amb certs límits, la previsió. Per ser vàlida, l'asserció de la norma ha de ser verificable empíricament, amb referència a fets socials.

Hart, representant de la jurisprudència analítica d'Austin, prendrà de Kelsen el concepte de *norma* com a concepte central del dret, i distingirà normes primàries —que imposen obligacions— de normes secundàries —de reconeixement. Les normes secundàries proporcionen als particulars i als funcionaris públics el mitjà per individualitzar les normes obligatòries.

Partint també de la concepció neopositivista, Bobbio planteja el problema de la cientificitat jurisprudencial entenent la jurisprudència com anàlisi del llenguatge del legislador, que confereix a aquest llenguatge el caràcter de discurs rigorós en relació amb

[38] Antonio-Enrique Pérez Luño. *Manual de informática y derecho*. Barcelona: Ariel, 1996.

tot enunciat que sigui coherent amb la resta d'enunciats del sistema. Això circumscriu la teoria de Bobbio a la teoria general del dret normativista i formalista.[39]

Frosini[40] sosté que, tot i el ressorgiment del dret natural després de la Segona Guerra Mundial, s'ha pogut advertir un canvi en els interessos de la literatura jurídica pel que fa als aspectes semàntics, lògics i tecnològics del dret. Frosini denomina *dret artificial* aquesta orientació, una nova perspectiva que s'obre de la possibilitat de fer servir les invencions electròniques per solucionar problemes d'ordre jurídic.

Per a Frosini, el punt de mediació que ha permès associar la cibernètica a la jurisprudència ha estat la possibilitat d'usar la lògica simbòlica en l'àmbit cultural dels estudis jurídics, als quals ha arribat des dels estudis de filosofia matemàtica. El jurista ha d'efectuar una tasca de reducció del problema jurídic a la seva dimensió lògica per tal de sotmetre aquest problema a un procés de transformació que es duu a terme de manera rigorosament tecnològica; això ens dóna un producte de dret artificial, produït per un raonament perfectament objectiu o, millor, totalment tecnificat.

Fassò identifica la renovació de l'interès pels estudis de lògica jurídica precisament com a conseqüència de la mateixa actitud racionalista que informa el moviment de la filosofia analítica, com a evolució i concreció de l'ús general de la lògica jurídica que en general s'ha pogut trobar en les teories generals del dret.

En aquest sentit, es pot observar un important interès pels següents tipus de lògica i la seva aplicació al domini legal:

- La lògica deòntica, com a subespècie de lògica modal.
- La lògica refutable.
- La lògica descriptiva.

3.5. La lògica deòntica

[39] Tot i que sense rendir-se al reduccionisme que implicaria limitar-se a l'anàlisi formal de les normes, en perjudici del valor del dret, que correspondrà a la filosofia del dret, o de la seva eficàcia, que correspondrà a la sociologia del dret.
[40] Vittorio Frosini. *Cibernética, derecho y sociedad*. Madrid: Tecnos, 1982.

La lògica del dret ha estat considerada inicialment lògica de les normes, o del llenguatge normatiu,[41] que s'anomena *lògica deòntica*, i en són exponents destacats Von Wright i Kalinowski, així com Alchourrón i Bulygin.[42]

Més enllà de la pluralitat i l'heterogeneïtat de les accepcions de la lògica deòntica, Pérez Luño[43] assenyala que implica precisament la possibilitat d'estendre les inferències lògiques no tan sols a les descripcions, sinó també a les prescripcions, cosa que permet la construcció d'una lògica de les normes, una "lògica sense veritat" aplicable a les conseqüències i les relacions lògiques de les normes en funció del seu ús sintàctic en un context de deducció.

Com exposa Alarcón,[44] l'expressió *lògica deòntica* va ser emprada per primer cop en el sentit actual el 1951 per Georg H. Von Wright.[45] Juntament amb els conceptes modals alètics (necessitat, possibilitat, contingència), amb els conceptes modals existencials (universalitat, existència, vacuïtat) i amb els conceptes modals epistèmics (allò verificat, allò indeterminat, allò falsat), va introduir els conceptes modals deòntics: allò obligatori, allò permès, allò prohibit.

Els pressupòsits de la lògica deòntica inicial de Von Wright, de caire monàdic, són els següents: 1) les coses que anomenem *obligatòries*, *permeses* o *prohibides* són actes entesos no en sentit individual, sinó com a propietat que els qualifica; 2) respecte a qui realitza l'acte (l'agent), existeix un valor d'execució de l'acte i un valor de no execució de l'acte, anàlegs als valors clàssics de la veritat i la falsedat.

En aquesta primera conceptualització de la lògica deòntica, que hom anomena *sistema estàndard de lògica deòntica*, les variables i les constants són anàlogues a les emprades en la lògica d'enunciats, amb algunes particularitats: les variables incorporen les lletres O (de manera que Op vol dir que és obligatori fer p) i P (de manera que Pp vol dir que està permès o no està prohibit fer p), i les constants reben el significat deòntic corresponent: " - " es refereix a la negació deòntica, de manera que "-Op" vol dir que no és obligatori fer p; " ^ " es refereix a la conjunció deòntica, de manera que "O (p ^ q) vol dir que és obligatori fer p i q, i Op ^ Oq vol dir que és obligatori fer p i és obligatori fer q; " v " es refereix a la disjunció deòntica, de manera que O (p v q) vol dir que és obligatori fer p o q, i Op v Oq vol dir que és obligatori fer p i és obligatori fer q; " ↔ " es refereix a la

[41] Guido Fassò. *Historia de la filosofía del derecho*… , *op. cit*.

[42] Carlos E. Alchourrón i Eugenio Bulygin. *Introducción a la metodología de las ciencias jurídicas y sociales*. Buenos Aires: Astrea, 1987.

[43] Antonio-Enrique Pérez Luño. *Manual de informática*…, *op. cit.*

[44] Carlos Alarcón Cabrera. «Las lógicas deónticas de Georg H. Von Wright», Revista DOXA, núm. 26, 2003.

[45] Tot i que existeixen antecedents de sistemes deòntics des de l'obra d'Ernst Mally de 1926 anomenada *The Basic Laws of Ought: Elements of the Logic of Willing*, com reporta Gert-Jan Lokhorst, «Mally's Deontic Logic», *The Stanford Encyclopedia of Philosophy (Winter 2008 edition)*.

coimplicació o equivalència deòntica, de manera que Op ↔ Oq vol dir que si i només si és obligatori fer p aleshores és obligatori fer q, i finalment " → " es refereix a la implicació deòntica, de manera que O (p → q) vol dir que és obligatori p si es dóna p.

Addicionalment, Von Wright afegeix regles específiques d'inferència deòntica a les ja existents en la lògica proposicional ordinària. En primer lloc, afegeix dues regles sobre la interdefinibilitat: " OA → PA " indica que si és obligatori fer p, aleshores està permès fer p; " PA ↔ -O-A " indica que si està permès fer p, aleshores no és obligatori no fer p. En segon lloc, introdueix regles per a la distribució d'operadors semàntics. I, en tercer lloc, introdueix tres "lleis sobre el compromís": "OA ^ O (A → B) → OB " indica que si és obligatori fer p, i fer p implica obligació de fer q, aleshores també és obligatori fer q (que es considera tautològic); " PA ^ O (A → B) → PB " indica que si està permès fer p, i fer p obliga a fer q, aleshores també està permès fer q; " -PB ^ O (A → B) → -PA " indica que si no està permès fer q, i fer p obliga a fer q, aleshores p tampoc no està permès.

La lògica deòntica monàdica també va sorgir a partir dels treballs de Kanger i Anderson sobre la reducció de la lògica modal, amb característiques semblants al sistema deòntic estàndard.

Posteriorment, arran d'algunes paradoxes detectades en el sistema estàndard, Von Wright —i altres autors interessats en la lògica deòntica— hi introdueix diverses ampliacions afegint-hi operadors diàdics, que permeten expressar, de manera implícita o explícita, relacions entre dos arguments que constitueixen l'antecedent i la conseqüència de la implicació deòntica.

Els sistemes diàdics disposen de tres estrats: la lògica proposicional clàssica, basada en l'estudi formal de les expressions p, q...; la lògica del canvi, basada en l'estudi formal de les expressions T, en la qual el succés descrit per " pTq " és una transformació d'un estat inicial de coses descrites per p fins a un estat final de coses descrit per q; i la lògica de l'acció, basada en l'estudi formal de les expressions df, en la qual " d (-pTp) " indica que un agent, en una ocasió determinada, provoca l'estat de coses descrit per p, mentre que " f (-pTp) " indica que un agent, en una ocasió determinada, s'absté de provocar l'estat de coses descrit per q. D'altra banda, amb el símbol " / " s'introdueix la possibilitat de descriure mandats, com en el cas de " O (pTp) / qTpq) ".

Per a Pérez Luño,[46] la lògica deòntica —tot i que aquesta conclusió es pot predicar, en termes generals, de la resta de lògiques que presentem— resulta molt rellevant per a la informatització del llenguatge jurídic, per un motiu doble: perquè com més estructuració lògica tingui el llenguatge jurídic, més fàcil serà la seva formalització informàtica, i

[46] Antonio-Enrique Pérez Luño. *Manual de informática*…, *op. cit.*

perquè la possibilitat de projectar regles lògiques sintàctiques de les normes permet facilitar les operacions de l'ordinador.

Actualment la lògica deòntica és una de les branques importants d'estudi de la interpretació de les normes, tant legals com en altres sistemes normatius socials, juntament amb altres modalitats de lògica modal, com la lògica temporal o la lògica condicional, i altres reptes que ha presentat quant a la possibilitat de raonar es poden satisfer mitjançant sistemes de raonament no monòton, com la lògica refutable.

La seva aplicació pràctica als efectes d'aquest treball és que permet avaluar el conjunt de normes en termes modals monòtons i oferir una primera interpretació d'allò a què obliga una norma, d'allò que permet o que prohibeix, especialment en termes de la relació entre les diferents normes del sistema a automatitzar.

Un exemple d'aplicació jurídica basada en lògica deòntica el constitueix el sistema CLIME, segons reporten Boer, Hoesktra i Winkels.[47] Es tracta d'un sistema de consell legal basat en el web orientat a les normatives internacionals sobre classificació de vaixells, que realitza una gestió del coneixement de les normatives i, en el que ara ens interessa, implementa un control de consistència semiautomàtic relatiu a les mateixes normes. Aquesta experiència mostra com es pot aplicar la lògica deòntica a l'entorn de regulació típicament administrativa.

Malgrat que no es pot sostenir que la lògica deòntica sigui absolutament vàlida o útil per al raonament automatitzat per raó dels reptes que els sistemes deòntics encara afronten, sí que pot resultar útil per formalitzar la interpretació purament normativa de les normes a aplicar, cosa que permet guanyar objectivitat en el procés interpretatiu sense deixar de banda altres criteris lògics d'interpretació.

3.6. La lògica refutable

L'anomenada —amb una certa impropietat— *lògica d'argumentació* (anomenada *nova retòrica* per Frosini) ha aparegut amb força. Es preocupa per la lògica del procediment o del debat judicial (incloent-hi el "procediment administratiu"), amb una forta orientació a la lògica d'allò probable, tot i no ser absolutament i científicament "cert".

Aquesta concepció deriva de la constatació de l'operativa dels casos particulars la prova dels quals, com es mostra especialment en el moment del procés, s'efectua amb

[47] Alexander Boer, Rinke Hoekstra i Radboud Winkels. «The CLIME Ontology», *Second International Workshop on Legal Ontologies*, 2001.

argumentacions de probabilitat i versemblança, i no amb demostracions de veritat. Aquest corrent va ser iniciat per Perelman, i en són representants Toulmin i Viehweg (Fassò).

Entre nosaltres, Atienza[48] ha indicat que el dret és essencialment una activitat d'argumentació que té a veure amb el llenguatge, amb la lògica i amb altres formes d'argumentació poc tractades en la cultura jurídica contemporània, com la tòpica, la retòrica i la dialèctica.

L'anomenada *lògica d'argumentació* ha estat particularment desenvolupada mitjançant els sistemes de raonament no monòton, i en especial per la lògica refutable (*defeasible logic*).

Luger i Stubblefield[49] mantenen que la no-monoticitat és un aspecte important de la resolució de problemes i del raonament basat en sentit comú que realitzen les persones.

La lògica de predicats es basa en les assumpcions de suficiència en la descripció de predicats del domini de l'aplicació, de consistència en la base d'informacions (absència de contradiccions entre les informacions) i d'increment de la informació (mitjançant les regles d'inferència i, en concret, de la deducció, que augmenten la informació de forma monòtona), condicions que no es poden considerar en molts dominis, com ara en el cas jurídic.

Davant els sistemes monòtons, els sistemes no monòtons ofereixen mecanismes de raonar quan no disposem de prou coneixement sobre els predicats (per exemple, quan no es coneix la condició de veritat d'un predicat, sobre la innocència d'una persona) o considerant la informació com una assumpció vencible, és a dir, que es pot modificar en consideració a informació nova.

Seguint Koons,[50] podem indicar que les aproximacions lògiques al raonament vencible tracten aquesta matèria com l'estudi de les relacions de conseqüència no monòtona, en contrast amb la monoticitat de la lògica clàssica.

Una relació de conseqüència és una relació matemàtica que modela què se segueix lògicament a partir de què. Aquestes relacions es poden definir de diverses formes: com relacions de Hilbert, de Tarski o de Scott. Així, una relació de conseqüència de Hilbert és una relació entre parells de fórmules; una relació de Tarski és una relació entre conjunts

[48] Manuel Atienza. *El derecho como argumentación*. Barcelona: Ariel Derecho, 2006.

[49] George F. Luger i William A. Stubblefield. *Artificial Intelligence. Structures and strategies for complex problem solving*. Reading, Massachusetts: Addison-Wesley,1998.

[50] Robert Koons. «Defeasible reasoning», *The Stanford Encyclopedia of Philosophy (Spring 2009 edition)*.

de fórmules (possiblement infinites) i fórmules individuals, i una relació de Scott és una relació entre dos conjunts de fórmules.

En el cas de les relacions de Hilbert i Tarski, $A \vDash B$ o $\Gamma \vDash B$ significa que la fórmula B segueix de la fórmula A o del conjunt de fórmules Γ. En el cas de les relacions de Scott, $\Gamma \vDash \Delta$ signfica que la veritat conjunta de tots els membres de Γ implica (en algun sentit) la veritat d'almenys un membre de Δ. Fins aquest moment, els estudis de lògica no monòtona han definit relacions de conseqüència lògica de l'estil hilbertià o tarskià, més que en el sentit de Scott.

Una relació de conseqüència lògica de Tarski és monòtona només si satisfà la condició següent, per a totes les fórmules p i tots els conjunts Γ i Δ:

Si $\Gamma \vDash p$, aleshores $\Gamma \cup \Delta \vDash p$.

Qualsevol relació que no compleixi aquesta condició és no monòtona. Una relació de conseqüència vencible —és a dir, que es pot modificar en funció d'informació nova— ha de ser necessàriament no monòtona.

En la lògica no monòtona de McDermott-Doyle i en la lògica autoepistèmica de Moore, s'hi introdueix un operador modal M, que representa un tipus de possibilitat epistèmica. Les regles per defecte tenen la forma següent: $((p \& Mq) \rightarrow q)$; és a dir, si p és veritat i q és "possible" (en el sentit rellevant), aleshores q també és veritat.

Governatori i Rotolo[51] presenten el contingut d'una teoria refutable com una estructura $(F,R,\succ)$ on F és un conjunt finit de fets, R és un conjunt finit de regles, i $\succ$ és una relació acíclica de superioritat sobre R. Els fets s'identifiquen amb literals i són manifestacions indiscutibles. Una regla expressa una relació entre un conjunt de premisses i una conclusió.

La lògica refutable permet establir tres tipus de regles sobre la força de les relacions:

- Regles estrictes, amb la forma $A_1, ..., A_n \rightarrow B$, que són les més fortes, ja que quan les premisses són indisputables sempre es dóna la conclusió.

- Regles vencibles, amb la forma $A_1, ..., A_n \Rightarrow B$, que descriuen els casos en què la conclusió es dóna quan les premisses són temptativament certes.

[51] Guido Governatori i Antoni Rotolo. «Changing legal systems: abrogation and annulement. Part I: Revision of defeasible theories», *Deontic logic in computer science*. Berlín: Springer, 2008.

- Vencedors, amb la forma $A_1, ..., A_n \sim> B$, que consideren les situacions en què les premisses no garanteixen les conclusions, de manera que les premisses només impedeixen a una altra norma suportar una postura contrària.

Semblantment, una conclusió es pot etiquetar com a definitiva o refutable, i podria ser retractable si apareixen noves premisses. La lògica refutable es basa en una teoria demostrativa constructiva per a les conclusions, de manera que podem dir que existeix una derivació per a una conclusió i que no podem donar una derivació per a una conclusió. Això permet etiquetar les conclusions d'acord amb la notació següent:

- $+\Delta B$, que vol dir que disposem d'una demostració definitiva per a B, per a la qual només emprem fets i regles estrictes, com en el cas del raonament monòton propi de la lògica de predicats de primer ordre.

- $-\Delta B$, que vol dir que no és possible construir una demostració definitiva per a B.

- $+\delta B$, que vol dir que disposem d'una demostració refutable per a B.

- $-\delta B$, que vol dir que no és possible donar una demostració refutable per a B.

La lògica refutable és un formalisme escèptic, ja que, en cas de conflicte entre dues conclusions sobre un mateix cas, les considera totes dues poc probables —més que contradictòries entre elles— mentre no es disposi d'informacions addicionals, un problema que es pot superar mitjançant l'establiment de relacions de superioritat entre les diferents conclusions.

D'aquesta manera, la demostració refutable funciona a l'estil argumentador: primer es tracta de cercar un argument a favor de la conclusió que es vol provar; en segon lloc, un argument en contra de la conclusió que es tracta de provar, i en tercer lloc, una refutació de l'argument contrari, mostrant que aquest no està fonamentat (per exemple, no es donen les premisses) o refutant-lo (per exemple, perquè és més dèbil lògicament).

Com succeeix amb la lògica deòntica, a la qual ha ajudat a avançar en alguns dels reptes formals a què s'enfronta, la lògica vencible és objecte d'un estudi recent, teòric i pràctic, molt ampli. Això permet emprar-la com a eina en el procés interpretatiu de la norma jurídica a automatitzar, en aquest cas amb una visió menys normativa del sistema, en benefici de la dinàmica del descobriment de la solució legal, més adient per via d'argumentació lògica, proposicional i modal.

3.7. La lògica de descripció

Recentment, en el domini de la representació del coneixement, i com a evolució de diversos formalismes, trobem la lògica de descripció, que permet representar el coneixement d'un domini d'aplicació (el "món") definint els conceptes rellevants del domini (la terminologia) i després emprant-los per especificar propietats dels objectes i dels individus que ocorren en aquest domini (la descripció del món).

Les lògiques de descripció han permès avançar molt en la creació de sistemes de raonament aplicat a una àmplia varietat de domini, incloent-hi el domini legal, en conjunció amb la construcció d'ontologies. Per aquest motiu les presentem succintament, i d'aquesta manera tanquem la visió de conjunt dels formalismes per a la interpretació lògica de les normes jurídiques.

Seguint Baader i Nutt,[52] podem exposar les característiques principals de la lògica de descripció. En primer lloc, a diferència d'altres formalismes de representació del coneixement, les lògiques de descripció estan equipades —com el seu nom indica— amb una semàntica formal basada en lògica. En segon lloc, emfatitzen el raonament com a servei principal ofert: el raonament permet inferir coneixement representat implícitament a partir del coneixement explícit contingut a la base de coneixement.

Les lògiques de descripció suporten la classificació de conceptes i d'individus. La classificació de conceptes determina relacions de subconceptes i superconceptes entre els conceptes d'una terminologia concreta, també anomenades *relacions de subsumpció*, i d'aquesta manera permet estructurar la terminologia en forma de jerarquia de subsumpció. Aquesta jerarquia ofereix informació útil sobre la connexió entre diferents conceptes, i es pot emprar per accelerar altres sistemes d'inferència.

La classificació dels individus (o dels objectes) determina si un individu concret és sempre una instància d'un concepte determinat (per exemple, si aquesta relació d'instància ve donada per la descripció de l'individu i la definició del concepte), i aleshores ofereix informació útil sobre les propietats d'un individu.

Des de la perspectiva de la lògica, cal dir que les lògiques de descripció són subconjunts de la lògica de predicats de primer ordre, com mantenen Nardi i Brachman.[53] De fet, el llenguatge de lògica de descripció ALC correspon al fragment de lògica de primer ordre que s'obté restringint la sintaxi a fórmules que continguin dues variables. Així mateix, les

[52] Franz Baader i Werner Nut. «Basic description logics», *Description Logic Handbook*, editat per F. Baader, D. Calvanese, D.L. McGuinness, D. Nardi, P.F. Patel-Schneider. Cambridge University Press, 2002.

[53] Daniele Nardi i Ronald J. Brachman. «An introduction to description logics», *Description Logic Handbook*, editat per F. Baader, D. Calvanese, D.L. McGuinness, D. Nardi, P.F. Patel-Schneider. Cambridge University Press, 2002.

lògiques de descripció estan fortament relacionades amb les lògiques modals; específicament, els conceptes ALC són directament traduïbles a fórmules en lògica multimodal K.

Una aplicació d'aquests tipus de lògiques és la conceptualització del domini legal, per exemple de les tipologies de representants de les persones (representants legals, representants voluntaris) i dels rols definits normativament que els compleixen (de manera que el tutor és un representant legal d'una persona incapaç, o l'administrador únic és el representant legal d'una societat limitada), com en el cas del sistema PASSI desenvolupat per l'Agència Catalana de Certificació.[54]

A partir d'aquesta conceptualització o ontologia, es poden implementar els mecanismes de raonament que permeten les lògiques de descripció, que són força eficients a causa d'un equilibri entre expressivitat i tractabilitat, i es pot deixar a altres mecanismes lògics la resolució d'altres problemes.

[54] Ignacio Alamillo i Xavier Uriós. «La gestión de identidades y capacidades por las Administraciones Públicas». TECNIMAP, 2006.

4. ANÀLISI DE CASOS RELLEVANTS D'ÚS D'AUTOMATITZACIÓ

En aquesta secció presentem alguns casos rellevants d'ús d'automatització que, segons la nostra opinió, resulten idonis per aplicar aquesta nova possibilitat reconeguda legalment:

- L'expedició automàtica de rebut de registre electrònic.
- La comprovació automàtica de dades de sol·licitud.
- La digitalització automàtica de documents.
- L'impuls automàtic del procediment.
- L'acte automàtic de constància electrònica.
- L'expedició automàtica de còpia autèntica electrònica.
- L'obertura i el tancament automàtic de llibres electrònics.
- La foliació automàtica d'expedients.
- La migració automàtica de document electrònic.
- Els intercanvis automàtics de dades entre administracions públiques.
- La remissió automàtica de comunicació electrònica al ciutadà.

Respecte a la possibilitat d'automatitzar actes administratius de voluntat, certament dependrà de dos factors principals: d'una banda, la configuració de l'acte administratiu com a potestat reglada o la predeterminació raonable dels casos en què actua la discrecionalitat administrativa, i, d'altra banda, la correcta informatització de la norma aplicada, en especial en termes de la necessària motivació-justificació dels actes automàtics, que d'acord amb el nostre criteri s'haurà d'incorporar al text de la resolució de forma particularment detallada, sobretot en els actes de voluntat i en els actes de judici.[55]

García de Enterría i Fernández[56] sostenen que la motivació ha de ser suficient, ha de donar raó plena del procés lògic i jurídic que ha determinat la decisió. Aquest fet connecta amb la necessitat de codificar i poder reconstruir, per a cada cas singular, les regles lògiques —ja hem vist que en una aproximació híbrida, amb l'aplicació d'un mètode integrat per la lògica de predicats de primer ordre, per les lògiques modals, deòntica i refutable aplicables, i per la lògica descriptiva quant a la representació del domini de coneixement jurídic— que han estat aplicades en l'acte administratiu automàtic singular.

[55] En cas que els considerem de possible execució automàtica, ja que resulta més fàcil, fins i tot intuïtivament, admetre que es pot programar una màquina per prendre decisions, mentre que no sembla possible que una màquina tingui judici, encara que sigui capaç de realitzar inferències lògiques, com hem exposat.

[56] Eduardo García de Enterría i Tomás Ramón Fernández. *Curso de derecho administrativo I*. Madrid: Thomson-Civitas, 2008.

A continuació presentem una sèrie de taules analítiques que mostren l'avaluació dels actes anteriors.

4.1. L'expedició automàtica de rebut de registre electrònic

1. Quin és el contingut de l'acte?	- Descripció de l'acte. L'emissió de rebut de registre electrònic consisteix en la producció d'un document acreditatiu de la presentació a un registre electrònic d'una sol·licitud, escrit o comunicació. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu, a sol·licitud del ciutadà, que en pot disposar voluntàriament. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una prova documental sobre l'acte del ciutadà adreçat a l'Administració.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. L'article 35 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, indica que, entre d'altres, els ciutadans tenen dret a obtenir una còpia segellada dels documents que presentin, quan l'aportin juntament amb els originals, així com a la devolució dels documents originals, excepte quan aquests originals hagin de constar en el procediment, dret que es concreta en la corresponent obligació de l'Administració, prevista a l'article 38.5 de la mateixa Llei 30/1992. L'article 6.1 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, reconeix als ciutadans el dret a relacionar-se amb les administracions públiques utilitzant mitjans electrònics per a l'exercici dels drets que preveu l'article 35 de la Llei 30/1992, i concreta, a l'article 24.1, l'obligació de crear registres electrònics per a la recepció i la remissió de sol·licituds, escrits i comunicacions. L'article 25.3 de la Llei 11/2007 estableix que els registres electrònics han d'emetre automàticament un rebut consistent en una còpia autenticada de l'escrit, la sol·licitud o la comunicació de què es tracti, que ha d'incloure la data i l'hora de presentació i el número d'entrada de registre. Així mateix, l'article 25.4 de la Llei 11/2007 regula que es poden aportar documents que acompanyin la corresponent sol·licitud, escrit o comunicació, sempre que compleixin els estàndards de format i requisits de seguretat que determinin els esquemes nacionals d'interoperabilitat i de seguretat. Els registres electrònics han de generar rebuts acreditatius del lliurament d'aquests documents que garanteixin la integritat i el no-rebuig dels documents aportats.

	- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions). Es tracta d'un acte absolutament reglat que l'Administració ha de dur a terme sempre que ho sol·liciti el ciutadà, en el moment de presentar un escrit al registre, tot i que el ciutadà en pot disposar lliurement.
	- Condicions jurídiques necessàries perquè l'acte es pugui realitzar. Les condicions jurídiques són les aplicables a l'acte de presentació de la sol·licitud, escrit o comunicació al registre electrònic; és a dir, les generals de capacitat i legitimació per actuar.
	- Obligació legal o administrativa de documentar l'acte. Com hem indicat anteriorment, resulta exigible documentar l'acte quan ho sol·licita el ciutadà, tot i que de la lectura de l'article 25.3 de la Llei 11/2007 es podria considerar que l'obligació existeix sempre, fins i tot quan el ciutadà no ho sol·licita. Aquesta lectura no modifica el fet que el rebut està disponible per part del ciutadà, que pot decidir no conservar-lo.
3. Qui realitza l'acte?	- Persona física (ciutadà). No aplicable.
	- Treballador de l'Administració (si s'escau, funcionari). No aplicable.
	- Òrgan unipersonal de l'Administració. L'emissió del rebut de registre la duu a terme el registre, que té la consideració d'òrgan administratiu.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). En el cas de l'emissió de rebut de presentació a un registre presencial, el funcionari de registre actua en qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Podem avançar que aquesta actuació, es cas de ser realitzada de forma automàtica, no exigirà —lògicament— la determinació prèvia de la qualitat en què actua cap persona.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).

	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). En el cas de l'emissió de rebut de presentació a un registre presencial, qualsevol funcionari de registre pot executar l'acte. Podem avançar que aquesta actuació, es cas de ser realitzada de forma automàtica, no exigirà —lògicament— la determinació prèvia de la possibilitat de substitució personal.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. En el cas del registre electrònic, l'article 25.3 de la Llei 11/2007 exigeix la generació d'un document nou, consistent en la còpia autenticada de l'escrit, la sol·licitud o la comunicació de què es tracti, que ha d'incloure la data i l'hora de presentació i el número d'entrada de registre. Per la seva banda, l'article 25.4 de la Llei 11/2007 obliga a la generació de rebuts acreditatius del lliurament des documents complementaris aportats al procediment que garanteixin la integritat i el no-rebuig d'aquests documents. - Es plasma en un document existent. El rebut de registre, en el cas de la presentació presencial, es plasma en un document ja existent, que precisament és la còpia de la sol·licitud, l'escrit o la comunicació adreçada a l'Administració, i que ha d'aportar el ciutadà. - Es registra, sense generar manifestació documental. No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí, normalment l'aplicació de registre identifica el funcionari que actua. També caldrà identificar l'òrgan de registre quan actuï automàticament. - Determinació del mètode d'identificació i autenticació de la persona que actua. En principi, sembla que es pot identificar la persona que opera el registre mitjançant qualsevol sistema vàlid i, en concret, resulta habitual fer-ho mitjançant nom d'usuari i paraula de pas, identificació que no transcendeix a la gestió de l'aplicació de registre, i que per tant no és coneguda pel ciutadà. Podem avançar que aquesta actuació, es cas de ser realitzada de forma automàtica, haurà d'identificar el registre mitjançant el segell d'òrgan corresponent, a nom del mateix registre o de l'Administració que n'és titular.

	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Com hem indicat anteriorment, la identificació de la persona que opera el registre és de nivell 1 o superior, mentre que la identificació del registre electrònic automatitzat s'hauria de fer amb nivell 3 o superior.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. Sí, tot i que aquesta comprovació es realitza de forma interna a l'aplicació de registre i no és coneguda pel ciutadà. En el cas de l'actuació automatitzada, es considera necessari comprovar la correcció del segell a emprar, de manera que s'utilitzi el segell adequat per a la producció dels segells de registre. - Comprovació de la facultat d'actuació, orgànica o legal. Es comprova la condició de persona habilitada per operar el registre, quan s'escau. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. En general, no, però depèn del contingut de la còpia segellada de registre, ja que si conté dades personals de nivell alt (com ara una sol·licitud motivada per una discapacitat), aleshores caldrà garantir el secret de la comunicació de retorn del rebut. - Determinació del mètode de protecció emprat. El mètode de protecció a emprar depèn del mecanisme de comunicació utilitzat. Per exemple, si la comunicació amb el registre es produeix a través de la seu electrònica, com resulta convenient, aleshores probablement es faran servir els mateixos mecanismes de confidencialitat per protegir el lliurament del rebut.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. L'acte d'emissió de rebut es pot dur a terme de manera manual o automàtica indistintament. - Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació, el segellament i el lliurament al ciutadà del rebut de registre.

4.2. La comprovació automàtica de dades de sol·licitud

1. Quin és el contingut de l'acte?	- Descripció de l'acte. La comprovació automàtica de dades de sol·licitud consisteix en la verificació d'aquestes dades, emprant informacions emmagatzemades en sistemes propis o pertanyents a altres administracions, amb la possibilitat d'omplir, totalment o parcialment, el formulari amb la finalitat que el ciutadà verifiqui la informació i, si s'escau, la modifiqui i la completi. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu, si s'escau a sol·licitud del ciutadà. - Efectes que produeix dins el procés (inicia, acaba, altres). L'efecte d'aquest acte en el procés és detectar errors en les dades de la sol·licitud, d'una banda, i facilitar al ciutadà la tasca d'omplir el formulari, d'altra banda.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. L'article 35.3 de la Llei 11/2007 disposa que els sistemes normalitzats de sol·licitud poden incloure comprovacions automàtiques de la informació aportada respecte a dades emmagatzemades en sistemes propis o pertanyents a altres administracions i, fins i tot, poden oferir el formulari emplenat, totalment o parcialment, amb la finalitat que el ciutadà verifiqui la informació i, si s'escau, la modifiqui i la completi. - Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions). Es tracta d'un acte discrecional per a l'Administració que la llei autoritza amb vista a facilitar i promoure l'ús dels sistemes normalitzats de sol·licitud. - Condicions jurídiques necessàries perquè l'acte es pugui realitzar. Les condicions jurídiques són les aplicables a l'acte de presentació de la sol·licitud, l'escrit o la comunicació al registre electrònic; és a dir, les generals de capacitat i legitimació per actuar. - Obligació legal o administrativa de documentar l'acte. Segons la nostra opinió, caldrà documentar el resultat de la comprovació automàtica, i, en cas de detecció d'errors en la sol·licitud, comunicar-los en unitat d'acte al ciutadà perquè els corregeixi.
3. Qui realitza l'acte?	- Persona física (ciutadà). No aplicable. - Treballador de l'Administració (si s'escau, funcionari). No aplicable.

	- Òrgan de l'Administració. La comprovació es configura legalment com un acte automàtic. Per tant, l'ha de dur a terme l'òrgan corresponent, que cal identificar amb precisió, i que en general correspon a l'òrgan responsable del sistema normalitzat de tramitació.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Aplicable, ja que els actes de comprovació s'han d'imputar a l'òrgan responsable del sistema normalitzat de tramitació. - En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta). - No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. El resultat positiu de les comprovacions es pot plasmar en un document específic. - Es plasma en un document existent. El resultat positiu de les comprovacions es pot plasmar en la mateixa sol·licitud. - Es registra, sense generar manifestació documental. El resultat de les comprovacions es pot registrar en el sistema normalitzat de sol·licitud.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí. - Determinació del mètode d'identificació i autenticació de la persona que actua. Segell d'actuació administrativa automàtica o codi segur de verificació.

	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 3.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. No. - Determinació del mètode de protecció emprat. No aplicable.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí, tal com determina de manera expressa la llei. - Determinació dels tractaments automàtics o mecànics. L'automatisme consisteix en la comprovació d'informacions emmagatzemades en sistemes propis o pertanyents a altres administracions, cosa que implica els automatismes corresponents als intercanvis de les dades corresponents.

4.3. La digitalització automàtica de documents

1. Quin és el contingut de l'acte?	- Descripció de l'acte. La digitalització automàtica consisteix en el canvi de suport d'un document, del suport paper al suport electrònic, mitjançant tecnologia de captura i tractament posterior de la imatge. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu, si s'escau a sol·licitud del ciutadà. - Efectes que produeix dins el procés (inicia, acaba, altres). La digitalització automàtica no produeix cap efecte particular en un procediment, sinó que permet disposar d'un suport de substitució del paper (una còpia autèntica de l'original, que el pot substituir).
2. Quina és la normativa	- Identificació de les normes aplicables.

aplicable a l'acte?

L'article 30.2 de la Llei 11/2007 estableix que les còpies realitzades per les administracions públiques, utilitzant mitjans electrònics, de documents emesos originalment per les administracions públiques en suport paper tenen la consideració de còpies autèntiques sempre que es compleixin els requeriments i les actuacions que preveu l'article 46 de la Llei 30/1992, de règim jurídic de les administracions públiques i del procediment administratiu comú.

Per la seva banda, l'article 30.3 de la Llei 11/2007 determina que les administracions públiques poden obtenir imatges electròniques dels documents privats aportats pels ciutadans, amb la seva mateixa validesa i eficàcia, a través de processos de digitalització que garanteixin l'autenticitat, la integritat i la conservació del document imatge, del qual s'ha de deixar constància. Aquesta obtenció es pot fer de manera automatitzada, mitjançant el segell electrònic corresponent.

En tercer lloc, l'article 30.4 de la Llei 11/2007 estableix que, en els casos de documents emesos originalment en suport paper dels quals s'hagin efectuat còpies electròniques d'acord amb el que disposa aquest article, es poden destruir els originals en els termes i amb les condicions que estableixi cada Administració pública.

Finalment, l'article 31.1 de la mateixa Llei 11/2007 indica que es poden emmagatzemar per mitjans electrònics tots els documents utilitzats en les actuacions administratives, cosa que referma la noció de la digitalització de documents en expedients administratius.

- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

  Es tracta d'un acte discrecional per a l'Administració.

- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

  Les condicions inclouen el nomenament de l'òrgan competent i la determinació dels mecanismes que permeten acreditar la constància de la integritat i de l'autenticitat de la còpia produïda a partir de la digitalització.

- Obligació legal o administrativa de documentar l'acte.

  La digitalització produeix una còpia autèntica que documenta l'acte.

3. Qui realitza l'acte?

- Persona física (ciutadà).

  No aplicable.

- Treballador de l'Administració (si s'escau, funcionari).

  No aplicable.

- Òrgan de l'Administració.

  La digitalització es configura com un acte automàtic. Per tant, l'ha de dur a terme l'òrgan corresponent, que cal identificar amb precisió, i que en general correspon a l'òrgan responsable del sistema de digitalització o al titular de la

	documentació.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Aplicable, ja que els actes de digitalització s'han d'imputar a l'òrgan responsable que hagi estat nomenat. - En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta). - No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. La digitalització genera un document nou, una còpia autèntica. - Es plasma en un document existent. No aplicable. - Es registra, sense generar manifestació documental. La digitalització pot implicar l'extracció de dades del document, que es registraran en alguna aplicació, com ara l'aplicació de registre (en el cas de digitalització de documents d'entrada) o de gestió documental o d'arxiu (en el cas d'expedients ja existents).
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí. - Determinació del mètode d'identificació i autenticació de la persona que actua. Segell d'actuació administrativa automàtica o codi segur de verificació. - Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 4, ja que la còpia digitalitzada pot substituir l'original en paper, que eventualment serà destruït per

		l'Administració, d'acord amb el que determini la normativa reglamentària aplicable.
8.	Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9.	Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. No. - Determinació del mètode de protecció emprat. No aplicable.
10.	És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí, tal com determina de forma expressa la llei, com a mínim en el cas de l'article 30.3. - Determinació dels tractaments automàtics o mecànics. L'automatisme consisteix en la creació d'un document electrònic, amb la consideració de còpia, que representa de manera fidedigna la imatge del document original en suport paper.

4.4. L'impuls automàtic del procediment

1.	Quin és el contingut de l'acte?	- Descripció de l'acte. L'impuls automàtic del procediment consisteix en el conjunt d'actes de tràmit que permeten que avanci ordenadament la instrucció del procediment. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu. - Efectes que produeix dins el procés (inicia, acaba, altres). L'efecte d'aquest acte en el procés és fer avançar el procediment administratiu eliminant els obstacles que impedeixin, dificultin o endarrereixin l'exercici ple dels drets dels interessats o el respecte als seus interessos, disposant el que resulti necessari per evitar i eliminar tota anormalitat en la tramitació del procediment, i garantir el seu acabament dins el termini establert legalment.
2.	Quina és la normativa	- Identificació de les normes aplicables.

aplicable a l'acte?

L'article 41 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, determina la responsabilitat dels titulars de les unitats administratives i del personal al servei de les administracions públiques que tinguin a càrrec la resolució o el despatx dels assumptes.

Per la seva banda, l'article 74.1 de la Llei 30/1992 determina que el procediment, que se sotmet al principi de celeritat, s'ha d'impulsar d'ofici en tot els seus tràmits.

En aquest sentit, l'article 75.1 de la Llei 30/1992 disposa que cal acordar en un sol acte tots els tràmits que, per la seva naturalesa, admetin un impuls simultani i no sigui obligatori el seu compliment successiu.

L'article 78 de la Llei 30/1992 estableix que els actes d'instrucció necessaris per a la determinació, el coneixement i la comprovació de les dades en virtut de les quals s'hagi de pronunciar la resolució, els ha de realitzar d'ofici l'òrgan que tramiti el procediment, sens perjudici del dret dels interessats a proposar aquelles altres actuacions que requereixin la seva intervenció o constitueixin tràmits establerts legalment o reglamentàriament.

Finalment, l'article 36 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, determina, a l'apartat 1, que les aplicacions i els sistemes d'informació utilitzats per a la instrucció per mitjans electrònics dels procediments han de garantir el control dels temps i els terminis, la identificació dels òrgans responsables dels procediments i la tramitació ordenada dels expedients, i facilitar la simplificació i la publicitat dels procediments, mentre que l'apartat 2 indica que els sistemes de comunicació utilitzats en la gestió electrònica dels procediments per a les comunicacions entre els òrgans i les unitats interventors als efectes d'emissió i recepció d'informes o altres actuacions han de complir els requisits que estableix la Llei 11/2007.

- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

  No aplicable en general a la categoria d'actes d'impuls, ja que la significació jurídica serà predicable de cada acte concret.

- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

  Els actes d'impuls requereixen l'existència d'un procediment formalment obert.

- Obligació legal o administrativa de documentar l'acte.

  Segons la nostra opinió, caldrà documentar de manera suficient els actes d'impuls, d'acord amb la normativa aplicable a cada acte.

  Pot ser convenient, en relació amb la responsabilitat de l'òrgan instructor, documentar la seqüència d'actes d'instrucció a l'efecte de controlar els terminis, típicament mitjançant una eina de BPM (*business process*

	management, gestió de processos de negoci).
3. Qui realitza l'acte?	- Persona física (ciutadà). No aplicable. - Treballador de l'Administració (si s'escau, funcionari). Aplicable. - Òrgan de l'Administració. Aplicable.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Aplicable. - En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta). - No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). Aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. L'acte d'impuls es pot plasmar en un document específic. - Es plasma en un document existent. No aplicable. - Es registra, sense generar manifestació documental. L'acte d'impuls es pot registrar en l'aplicació de negoci que gestiona el procediment.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí. - Determinació del mètode d'identificació i autenticació de la persona que actua. Segell d'actuació administrativa automàtica o codi segur de verificació.

	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 3 o superior.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. No. - Determinació del mètode de protecció emprat. No aplicable.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí, sempre que l'acte concret d'impuls ho permeti. - Determinació dels tractaments automàtics o mecànics. Depèn de l'acte concret d'impuls del procediment.

4.5. L'acte automàtic de constància electrònica

1. Quin és el contingut de l'acte?	- Descripció de l'acte. L'acte automàtic de constància consisteix en una declaració de coneixement per part de l'Administració en relació amb una informació registrada en un document, un expedient o un llibre de l'Administració. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu, típicament a sol·licitud del ciutadà o d'una autoritat competent. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una prova documental sobre la informació manifestada.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. La Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, no estableix un règim concret per als actes de constància, que, per contra, es manifesten en altres actes,

	com l'expedició de certificacions i notes simples informatives, les quals normalment es reglamenten per la normativa sectorial o específica que els resulta d'aplicació.
	- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).
	Es tracta d'un acte absolutament reglat que l'Administració ha de dur a terme sempre que ho sol·liciti el ciutadà o l'autoritat competent.
	- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.
	Les condicions jurídiques necessàries per a la realització de l'acte les determina el tipus d'acte de constància.
	Resulten particularment rellevants les normes sobre expedició de certificats, ja que normalment es tracta d'una facultat reservada a un òrgan concret, en alguns casos amb la garantia de fe pública.
	- Obligació legal o administrativa de documentar l'acte.
	L'acte de constància es produeix habitualment mitjançant la forma documental escrita, en alguns casos amb rigoroses formalitats, com en el cas dels certificats emesos per les secretaries de les entitats locals.
3. Qui realitza l'acte?	- Persona física (ciutadà).
	No aplicable.
	- Treballador de l'Administració (si s'escau, funcionari).
	No aplicable.
	- Òrgan unipersonal de l'Administració.
	L'acte de constància l'ha de dur a terme l'òrgan administratiu competent.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi.
	No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica).
	Aplicable.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals.
	No aplicable.
	- Qualsevol representant.

	No aplicable.
	- Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
	No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou.
	Els actes de constància es manifesten en documents específics, com els certificats o les notes simples informatives. Així mateix, es poden plasmar en còpies autèntiques de documents en poder de l'Administració.
	- Es plasma en un document existent.
	No aplicable.
	- Es registra, sense generar manifestació documental.
	No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No.
	Sí.
	- Determinació del mètode d'identificació i autenticació de la persona que actua.
	Segell d'actuació administrativa automàtica o codi segur de verificació.
	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert.
	Nivell 3 per a les notes simples informatives i nivell 4 per a les certificacions.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No.
	No, ja que s'utilitza un segell d'actuació administrativa automàtica.
	- Comprovació de la facultat d'actuació, orgànica o legal.
	No aplicable.
	- Comprovació d'un apoderament o d'una autorització, en representació voluntària.
	No aplicable.
	- Comprovació de la condició de professional de col·lectiu autoritzat.
	No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No.
	En general, no, però depèn del contingut de l'acte de constància, ja que si conté dades personals de nivell alt, aleshores caldrà garantir el secret de l'acte de constància.
	- Determinació del mètode de protecció emprat.
	El mètode de protecció a emprar depèn del mecanisme de comunicació que s'utilitzi per lliurar el document de constància (nota simple o certificació).
10. És d'execució automàtica o mecànica, totalment o	- Sí/No.

parcialment?	Sí.
	- Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació, el segellament i el lliurament del document amb l'acte de constància.

4.6. L'expedició automàtica de còpia autèntica electrònica

1. Quin és el contingut de l'acte?	- Descripció de l'acte. L'expedició d'una còpia autèntica electrònica deriva d'un acte d'informació o d'accés a informació per part de l'Administració, en relació amb un document, típicament integrat en expedient de l'Administració. També es realitzen còpies automàtiques autèntiques per ingressar documents administratius o privats mitjançant la seva digitalització en paper, cas que no es tracta en aquest document, ja que s'analitza en un cas d'ús específic. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu, típicament a sol·licitud del ciutadà o d'una autoritat competent. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una prova documental sobre la informació manifestada.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. La Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, determina, a l'article 35.a), que els ciutadans tenen dret a conèixer en qualsevol moment l'estat de tramitació dels procediments en què tinguin la consideració d'interessats, i a obtenir una còpia dels documents continguts en aquests procediments. Per la seva banda, l'article 37.1 de la Llei 30/1992 determina que els ciutadans tenen dret a accedir als registres i als documents que formin part d'un expedient i romanguin en els arxius administratius, independentment de la seva forma d'expressió, gràfica, sonora o en imatge, o el tipus de suport material en què figurin, sempre que aquests expedients corresponguin a procediments finalitzats en la data de la sol·licitud. L'apartat 8 del mateix article 37 indica que el dret d'accés implicarà el d'obtenir còpies o certificacions dels documents l'examen dels quals sigui autoritzat per l'Administració. L'article 45.5 de la Llei 30/1992 estableix que els documents emesos, independentment del seu suport, per mitjans electrònics, informàtics i telemàtics per les administracions públiques, o els que aquestes emetin com a còpia d'originals emmagatzemats per aquests mateixos mitjans, han de gaudir de la validesa i l'eficàcia de

document original sempre que en quedi garantida l'autenticitat, la integritat i la conservació i, si s'escau, la recepció per part de la persona interessada, així com el compliment de les garanties i els requisits exigits per aquesta Llei o d'altres.

L'article 46 de la Llei 30/1992 disposa que cada Administració pública ha de determinar reglamentàriament els òrgans que tinguin atribuïdes les competències d'expedició de còpies autèntiques de documents públics i privats, i que les còpies de qualssevol documents públics han de gaudir de la mateixa validesa i eficàcia que aquests, sempre que existeixi constància de la seva autenticitat.

Per la seva banda, l'article 30.2 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, indica que les còpies realitzades per les administracions públiques, utilitzant mitjans electrònics, de documents emesos originalment per les administracions públiques en suport paper tenen la consideració de còpies autèntiques sempre que es compleixin els requeriments i les actuacions que preveu l'article 46 de la Llei 30/1992, de règim jurídic de les administracions públiques i del procediment administratiu comú.

L'article 30.4 de la Llei 11/2007 estableix que les còpies realitzades en suport paper de documents públics administratius emesos per mitjans electrònics i signats electrònicament tenen la consideració de còpies autèntiques sempre que incloguin la impressió d'un codi generat electrònicament o altres sistemes de verificació que permetin contrastar-ne l'autenticitat mitjançant l'accés als arxius electrònics de l'Administració pública, òrgan o entitat emissora.

Finalment, l'article 32.3 de la Llei 11/2007 determina que la tramesa d'expedients es pot substituir a tots els efectes legals per la posada a disposició de l'expedient electrònic, i l'interessat té dret a obtenir-ne una còpia.

- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

  Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho sol·liciti el ciutadà o l'autoritat competent.

- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

  Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i dels mecanismes de constància de l'autenticitat de la còpia.

- Obligació legal o administrativa de documentar l'acte.

  La còpia autèntica s'ha de documentar, normalment en forma de fotocòpia diligenciada, cosa que en cas de còpia electrònica serà una reproducció, amb o sense canvi de format, amb la diligència corresponent de ser còpia autèntica.

3. Qui realitza l'acte?

- Persona física (ciutadà).

	No aplicable.
	- Treballador de l'Administració (si s'escau, funcionari).
	No aplicable.
	- Òrgan unipersonal de l'Administració.
	La còpia autèntica l'ha de dur a terme l'òrgan administratiu competent.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi.
	No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica).
	Aplicable.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals.
	No aplicable.
	- Qualsevol representant.
	No aplicable.
	- Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
	No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou.
	Aplicable.
	- Es plasma en un document existent.
	No aplicable.
	- Es registra, sense generar manifestació documental.
	No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No.
	Sí.
	- Determinació del mètode d'identificació i autenticació de la persona que actua.
	Segell d'actuació administrativa automàtica o codi segur de verificació.
	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert.

		Nivell 4.
8.	Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9.	Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. En general, no, però depèn del contingut de la còpia autèntica, ja que si conté dades personals de nivell alt, aleshores caldrà garantir-ne el secret. - Determinació del mètode de protecció emprat. El mètode de protecció a emprar depèn del mecanisme de comunicació que s'utilitzi per lliurar la còpia autèntica.
10.	És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí. - Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació, el segellament i el lliurament de la còpia autèntica.

4.7. L'obertura i el tancament automàtic de llibres electrònics

1.	Quin és el contingut de l'acte?	- Descripció de l'acte. L'obertura i el tancament de llibres consisteix en la seqüenciació dels registres que formen part d'un llibre electrònic mitjançant l'encadenament criptogràfic dels registres o altres tècniques similars. L'acte d'obertura implica la creació i la signatura del primer registre, a partir del qual comença la cadena de registres, mentre que l'acte de tancament finalitza la cadena i protegeix tota la seqüència amb un segell de data i hora final. Els actes d'encadenament criptogràfic de registres, que es realitzen entre el segon registre (encadenat amb el primer) i el tancament (encadenat amb el darrer registre), es duen a terme sense nova identificació de l'òrgan. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu.

	- Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és formalitzar i protegir les insercions del llibre electrònic, ja que no es podran afegir ni retirar registres pel fet que estan encadenats criptogràficament.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. La normativa sectorial sovint identifica la necessitat de disposar de llibres legalitzats o diligenciats. - Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions). Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho determini la normativa aplicable. - Condicions jurídiques necessàries perquè l'acte es pugui realitzar. Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i del supòsit legal de l'obligació de legalitzar o diligenciar llibres, que indica la normativa sectorial, com ara la normativa de règim local. - Obligació legal o administrativa de documentar l'acte. Sí, mitjançant el sistema de llibre electrònic, amb encadenament criptogràfic dels registres.
3. Qui realitza l'acte?	- Persona física (ciutadà). No aplicable. - Treballador de l'Administració (si s'escau, funcionari). No aplicable. - Òrgan unipersonal de l'Administració. L'obertura i el tancament els ha de dur a terme l'òrgan administratiu competent, responsable del llibre.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Aplicable. - En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta). No aplicable.

5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. No aplicable. - Es plasma en un document existent. No aplicable. - Es registra, sense generar manifestació documental. Aplicable, ja que es registra en el mateix sistema de llibre electrònic.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí. Els actes concrets d'encadenament criptogràfic d'un registre amb l'anterior, que succeeix entre l'obertura i el tancament, no requereixen nova identificació. - Determinació del mètode d'identificació i autenticació de la persona que actua. Segell d'actuació administrativa automàtica. - Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 3 o superior.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. No, ja que l'índex no conté dades personals. - Determinació del mètode de protecció emprat. No aplicable.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí.

- Determinació dels tractaments automàtics o mecànics.

  L'automatisme possible consisteix en l'obertura i el tancament del llibre, com també l'encadenament criptogràfic dels registres.

4.8. La foliació automàtica d'expedients

1. Quin és el contingut de l'acte?
   - Descripció de l'acte.

     La foliació automàtica o electrònica d'expedients consisteix en la seqüenciació dels documents que formen part de l'expedient mitjançant un índex signat electrònicament.
   - Tipus d'acte (del ciutadà/de l'Administració, altres).

     Es tracta d'un acte administratiu.
   - Efectes que produeix dins el procés (inicia, acaba, altres).

     El seu efecte dins el procés administratiu és formalitzar i protegir l'expedient.
2. Quina és la normativa aplicable a l'acte?
   - Identificació de les normes aplicables.

     L'article 32.2 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, indica que la foliació dels expedients electrònics s'ha de dur a terme mitjançant un índex electrònic signat per l'Administració, l'òrgan o l'entitat actuant, segons escaigui. Aquest índex ha de garantir la integritat de l'expedient electrònic i permetre recuperar-lo sempre que calgui, i és admissible que un mateix document formi part de diferents expedients electrònics.
   - Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

     Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho determini la normativa aplicable.
   - Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

     Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i del supòsit legal de l'obligació de foliar, que indica la normativa sectorial, com ara la normativa de règim local.
   - Obligació legal o administrativa de documentar l'acte.

     La foliació obliga a generar l'índex de l'expedient.
3. Qui realitza l'acte?
   - Persona física (ciutadà).

     No aplicable.
   - Treballador de l'Administració (si s'escau, funcionari).

     No aplicable.
   - Òrgan unipersonal de l'Administració.

	La foliació l'ha de dur a terme l'òrgan administratiu competent, responsable de l'expedient.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. No aplicable. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). Aplicable. - En qualitat de representant legal d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. No aplicable. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta). No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. No aplicable. - Qualsevol representant. No aplicable. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup). No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. Aplicable. - Es plasma en un document existent. No aplicable. - Es registra, sense generar manifestació documental. No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. Sí. - Determinació del mètode d'identificació i autenticació de la persona que actua. Segell d'actuació administrativa automàtica o codi segur de verificació. - Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 3 o superior.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica.

	- Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. No, ja que l'índex no conté dades personals. - Determinació del mètode de protecció emprat. No aplicable.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí. - Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació i el segellament de l'índex.

4.9. La migració automàtica de document electrònic

1. Quin és el contingut de l'acte?	- Descripció de l'acte. La migració automàtica d'un document electrònic és un cas particular de l'expedició automàtica de còpia en què es produeix un canvi del format del document, per exemple de format ODF (ofimàtic) a format PDF (presentació). - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una prova documental sobre la informació manifestada.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. L'article 45.5 de la Llei 30/1992 indica que els documents emesos, independentment del seu suport, per mitjans electrònics, informàtics i telemàtics per les administracions públiques, o els que aquestes emetin com a còpia d'originals emmagatzemats per aquests mateixos mitjans, han de gaudir de la validesa i l'eficàcia de document original sempre que en quedi garantida l'autenticitat, la integritat i la conservació i, si s'escau, la recepció per l'interessat, així com el compliment de les garanties i els requisits exigits per aquesta llei o d'altres. L'article 46 de la Llei 30/1992 disposa que cada Administració pública ha de determinar reglamentàriament

		els òrgans que tinguin atribuïdes les competències d'expedició de còpies autèntiques de documents públics i privats, i que les còpies de qualssevol documents públics han de gaudir de la mateixa validesa i eficàcia que aquests, sempre que existeixi constància de la seva autenticitat. Per la seva banda, l'article 30.1 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, estableix que les còpies realitzades per mitjans electrònics de documents electrònics emesos pel mateix interessat o per les administracions públiques, mantenint o no el format original, tenen immediatament la consideració de còpies autèntiques amb l'eficàcia que preveu l'article 46 de la Llei 30/1992, de règim jurídic de les administracions públiques i del procediment administratiu comú, sempre que el document electrònic original estigui en poder de l'Administració i que la informació de signatura electrònica i, si s'escau, de segellament de temps permetin comprovar la coincidència amb el document esmentat. Finalment, l'article 31.2 de la Llei 11/2007 determina que els documents electrònics que continguin actes administratius que afectin drets o interessos dels particulars s'han de conservar en suports d'aquesta naturalesa, ja sigui en el mateix format a partir del qual es va originar el document o en un altre qualsevol que asseguri la identitat i la integritat de la informació necessària per reproduir-lo. S'ha d'assegurar en tot cas la possibilitat de traslladar les dades a altres formats i suports que garanteixin l'accés des de diferents aplicacions.
	-	Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions). Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho requereixi l'estratègia de preservació documental.
	-	Condicions jurídiques necessàries perquè l'acte es pugui realitzar. Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i dels mecanismes de constància de l'autenticitat de la còpia resultant de la migració.
	-	Obligació legal o administrativa de documentar l'acte. La còpia autèntica s'ha de documentar, normalment en un document amb canvi de format, amb la diligència corresponent de ser una còpia autèntica.
3. Qui realitza l'acte?	-	Persona física (ciutadà). No aplicable.
	-	Treballador de l'Administració (si s'escau, funcionari). No aplicable.
	-	Òrgan unipersonal de l'Administració. La còpia autèntica l'ha de dur a terme l'òrgan administratiu competent.
4. En quina qualitat realitza	-	En nom propi i per compte propi.

l'acte?	No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica).
	Aplicable.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals.
	No aplicable.
	- Qualsevol representant.
	No aplicable.
	- Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
	No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou.
	Aplicable.
	- Es plasma en un document existent.
	No aplicable.
	- Es registra, sense generar manifestació documental.
	No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No.
	Sí.
	- Determinació del mètode d'identificació i autenticació de la persona que actua.
	Segell d'actuació administrativa automàtica o codi segur de verificació.
	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert.
	Nivell 4.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No.
	No, ja que s'utilitza un segell d'actuació administrativa automàtica.
	- Comprovació de la facultat d'actuació, orgànica o legal.
	No aplicable.
	- Comprovació d'un apoderament o d'una autorització, en

	representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. En general, no, però depèn del contingut de la còpia autèntica, ja que si conté dades personals de nivell alt, aleshores caldrà garantir-ne el secret. - Determinació del mètode de protecció emprat. El mètode de protecció a emprar depèn del mecanisme de comunicació que s'utilitzi per lliurar la còpia autèntica.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí. - Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació, el segellament i el lliurament de la còpia autèntica.

4.10. Els intercanvis automàtics de dades entre administracions públiques

1. Quin és el contingut de l'acte?	- Descripció de l'acte. L'intercanvi automàtic entre administracions públiques consisteix en l'enviament o la posada a disposició d'un document per part d'una administració pública a una altra. L'acte d'intercanvi és molt semblant a l'acte de comunicació pel qual una administració sol·licita a una altra unes dades concretes, que són retornades per l'Administració requerida, típicament en substitució de certificats administratius de dades. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una prova documental sobre l'intercanvi efectuat.
2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. L'article 6.2.b) de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, consagra el dret dels ciutadans a no aportar les dades i els documents que estiguin en poder de les administracions públiques, les quals han d'utilitzar mitjans electrònics per obtenir la informació esmentada, sempre que, en el cas de dades de caràcter personal, tinguin el consentiment dels interessats en els termes que estableix la Llei orgànica 15/1999, de protecció de dades de caràcter personal, o una norma amb rang de llei ho determini, llevat que hi hagi restriccions

d'acord amb la normativa aplicable a les dades i els documents recollits. El consentiment es pot emetre i acceptar per mitjans electrònics.

Per la seva banda, l'article 9.1 de la Llei 11/2007 estableix que, per a un exercici eficaç del dret reconegut a l'apartat 6.2.b), cada Administració ha de facilitar l'accés de les administracions públiques restants a les dades relatives als interessats que figurin en poder seu i estiguin en suport electrònic, especificant les condicions, els protocols i els criteris funcionals o tècnics necessaris per accedir a les dades esmentades amb les màximes garanties de seguretat, integritat i disponibilitat, de conformitat amb el que disposa la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal i la seva normativa de desplegament. L'apartat 2 de l'article 9 especifica que la disponibilitat de les dades està limitada estrictament a les que les administracions restants requereixen als ciutadans per a la tramitació i la resolució dels procediments i les actuacions de la seva competència d'acord amb la seva normativa reguladora, i que l'accés a les dades de caràcter personal, a més, està sotmès al compliment de les condicions que estableix l'article 6.2.b) de la Llei 11/2007.

Finalment, l'article 13.3.d) de la Llei 11/2007 determina que les administracions públiques poden utilitzar, per a la seva identificació electrònica i per a l'autenticació dels documents electrònics que produeixin, sistemes d'intercanvi electrònic de dades en entorns tancats de comunicació, d'acord amb el que s'hagi acordat específicament entre les parts.

Aquesta previsió es desplega a l'article 20 de la Llei 11/2007, que a l'apartat 1 preveu que els documents electrònics transmesos en entorns tancats de comunicacions establerts entre administracions públiques, òrgans i entitats de dret públic es consideren vàlids als efectes d'autenticació i identificació dels emissors i els receptors en les condicions que estableix el present article, mentre que l'apartat 4 indica que en tot cas s'ha de garantir la seguretat de l'entorn tancat de comunicacions i la protecció de les dades que es transmetin.

- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

  Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho determini la normativa aplicable, per donar compliment al dret dels ciutadans.

- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

  Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i del supòsit legal de l'obligació d'efectuar l'intercanvi electrònic de dades.

- Obligació legal o administrativa de documentar l'acte.

  L'intercanvi s'ha de produir, normalment, en forma documentada, a l'efecte d'incorporar l'evidència de les dades a l'expedient.

3. Qui realitza l'acte?

- Persona física (ciutadà).

	No aplicable.
	- Treballador de l'Administració (si s'escau, funcionari).
	No aplicable.
	- Òrgan unipersonal de l'Administració.
	L'intercanvi l'ha de dur a terme l'òrgan administratiu competent.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi.
	No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica).
	Aplicable.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals.
	No aplicable.
	- Qualsevol representant.
	No aplicable.
	- Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
	No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou.
	Aplicable.
	- Es plasma en un document existent.
	No aplicable.
	- Es registra, sense generar manifestació documental.
	No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No.
	Sí.
	- Determinació del mètode d'identificació i autenticació de la persona que actua.
	En principi, sembla que hauria de ser el segell d'actuació administrativa automàtica o codi segur de verificació, però d'acord amb l'article 20 de la Llei 11/2007 s'han d'admetre, també, altres tipus de certificats de caràcter més tècnic que legal, com els sovint anomenats *certificats de component* o

	d'aplicació segura o *de servidor segur*, tot i que aquestes possibilitats hauran d'haver estat previstes expressament pel conveni regulador de l'intercanvi electrònic de dades.
	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert. Nivell 3 o superior, d'acord amb el que es determini al conveni regulador de l'intercanvi electrònic de dades.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. No, ja que s'utilitza un segell d'actuació administrativa automàtica o un mecanisme alternatiu de característiques similars. - Comprovació de la facultat d'actuació, orgànica o legal. No aplicable. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. No aplicable. - Comprovació de la condició de professional de col·lectiu autoritzat. No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. En general, no, però depèn del contingut de l'intercanvi electrònic de dades, ja que si conté dades personals de nivell alt, aleshores caldrà garantir-ne el secret. - Determinació del mètode de protecció emprat. El mètode de protecció a emprar depèn del mecanisme d'intercanvi que s'utilitzi.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. Sí. - Determinació dels tractaments automàtics o mecànics. L'automatisme possible consisteix en la generació, el segellament i el lliurament de l'intercanvi de dades.

4.11. La remissió automàtica de comunicació electrònica al ciutadà

1. Quin és el contingut de l'acte?	- Descripció de l'acte. La remissió automàtica de comunicació electrònica al ciutadà consisteix en l'enviament o la posada a disposició del ciutadà d'un document que instrumenta una comunicació entre l'Administració i el mateix ciutadà. - Tipus d'acte (del ciutadà/de l'Administració, altres). Es tracta d'un acte administratiu. - Efectes que produeix dins el procés (inicia, acaba, altres). El seu efecte dins el procés administratiu és generar una

prova documental sobre la comunicació efectuada.

2. Quina és la normativa aplicable a l'acte?

- Identificació de les normes aplicables.

  La Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú, determina, a l'article 34, que els òrgans administratius han d'anotar en el seu registre la sortida dels escrits i les comunicacions oficials adreçades a altres òrgans o particulars, previsió que troba el seu paral·lel a l'article 24.1 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, que estableix la necessitat de registrar la remissió de comunicacions electròniques.

  L'article 58.1 de la Llei 30/1992 imposa l'obligació de notificar als interessats les resolucions i els actes administratius que afectin els seus drets i interessos, d'acord amb el que determina l'article 59.

  Per la seva banda, l'article 27.2 de la Llei 11/2007 disposa que les administracions públiques han d'utilitzar mitjans electrònics en les seves comunicacions amb els ciutadans, sempre que així ho hagin sol·licitat o consentit expressament. La sol·licitud i el consentiment, en tot cas, es poden emetre i demanar per mitjans electrònics.

  L'apartat 3 de l'article 27 de la Llei 11/2007 indica que les comunicacions a través de mitjans electrònics són vàlides sempre que hi hagi constància de la transmissió i la recepció, de les dates i del contingut íntegre de les comunicacions, i s'hi identifiquin fidedignament el remitent i el destinatari.

  L'apartat 5 del mateix article 27 determina que els requisits de seguretat i integritat de les comunicacions s'han d'establir en cada cas de manera apropiada al caràcter de les dades que en són objecte, d'acord amb criteris de proporcionalitat, de conformitat amb el que disposa la legislació vigent en matèria de protecció de dades de caràcter personal.

  Com a norma especial, l'apartat 7 de l'article 27 estableix que les administracions públiques han d'utilitzar preferentment mitjans electrònics en les seves comunicacions amb altres administracions públiques. Les condicions que regeixen aquestes comunicacions s'han de determinar entre les administracions públiques participants.

  Finalment, l'article 38 de la Llei 11/2007 estableix minuciosament els requisits per a la realització de notificacions telemàtiques.

- Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions).

  Es tracta d'un acte absolutament reglat que l'Administració ha de realitzar sempre que ho determini la normativa aplicable.

- Condicions jurídiques necessàries perquè l'acte es pugui realitzar.

  Les condicions jurídiques necessàries per a la realització de l'acte són la determinació prèvia de l'òrgan competent i del

	supòsit legal de l'obligació d'efectuar la comunicació.
	- Obligació legal o administrativa de documentar l'acte.
	La comunicació s'ha de produir, normalment, en forma documentada, ja que el ciutadà l'ha de poder conservar pels seus propis mitjans.
3. Qui realitza l'acte?	- Persona física (ciutadà).
	No aplicable.
	- Treballador de l'Administració (si s'escau, funcionari).
	No aplicable.
	- Òrgan unipersonal de l'Administració.
	La comunicació l'ha de dur a terme l'òrgan administratiu competent o l'òrgan inferior, i s'hi ha d'indicar l'autoritat de què prové, d'acord amb l'article 55 de la Llei 30/1992.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi.
	No aplicable.
	- En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica).
	Aplicable.
	- En qualitat de representant legal d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant voluntari d'una persona física o jurídica, pública o privada.
	No aplicable.
	- En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
	No aplicable.
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals.
	No aplicable.
	- Qualsevol representant.
	No aplicable.
	- Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
	No aplicable.
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou.
	Aplicable.
	- Es plasma en un document existent.
	No aplicable.
	- Es registra, sense generar manifestació documental.
	No aplicable.
7. Requereix la comprovació prèvia de la identitat de qui	- Sí/No.

realitza l'acte?	Sí.
	- Determinació del mètode d'identificació i autenticació de la persona que actua.
	Segell d'actuació administrativa automàtica o codi segur de verificació.
	- Valoració del nivell d'evidència del mètode emprat, d'acord amb l'esquema de CATCert.
	Nivell 3 o superior.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No.
	No, ja que s'utilitza un segell d'actuació administrativa automàtica.
	- Comprovació de la facultat d'actuació, orgànica o legal.
	No aplicable.
	- Comprovació d'un apoderament o d'una autorització, en representació voluntària.
	No aplicable.
	- Comprovació de la condició de professional de col·lectiu autoritzat.
	No aplicable.
9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No.
	En general, no, però depèn del contingut de la comunicació, ja que si conté dades personals de nivell alt, aleshores caldrà garantir-ne el secret.
	- Determinació del mètode de protecció emprat.
	El mètode de protecció a emprar depèn del mecanisme de comunicació que s'utilitzi.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No.
	Sí.
	- Determinació dels tractaments automàtics o mecànics.
	L'automatisme possible consisteix en la generació, el segellament i el lliurament de la comunicació.

5. L'ACTUACIÓ ADMINISTRATIVA AUTOMATITZADA I EL CICLE DE VIDA DEL PROGRAMARI

Un cop presentada la nostra visió sobre la interpretació "informàtica" de la norma a automatitzar, en particular sobre la base dels diferents llenguatges lògics i la seva aplicació al domini jurídic, així com alguns casos rellevants per a l'automatització, cal entrar en la discussió sobre la naturalesa de l'aplicació o el programari que permet l'actuació administrativa automatitzada i sobre la idoneïtat de les metodologies d'enginyeria existents actualment per crear un producte amb prou qualitat per "delegar-hi" l'exercici de la potestat administrativa, que és el que en definitiva trobem en el cas de l'actuació administrativa sense intervenció humana en cada cas singular.

5.1. La naturalesa del tipus d'aplicació que ofereix suport a l'actuació administrativa automatitzada

Una qüestió sens dubte rellevant en el context analitzat és precisament la determinació de la naturalesa corresponent al tipus d'aplicació que ofereix suport a l'actuació administrativa automatitzada, és a dir, quina és la funcionalitat de l'aplicació.

Davant la concepció clàssica de l'aplicació informàtica com a auxiliar de la persona física que aplica el dret, trobem en aquestes aplicacions una orientació completament diferent, que es correspon, més que amb la informàtica documental o d'oficina, amb la que ha estat anomenada *informàtica jurídica de decisió*.

Frosini recull les primeres experiències en matèria d'automatització de problemes jurídics a partir de les propostes de Loevinger, que havia anomenat *jurimetria* a aquesta possibilitat, i de Hoffmann, que la va anomenar *lawtomation*, indicant un dels principis que posteriorment han estat recollits per la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

En efecte, s'indica que, per a la difusió de l'ús de les calculadores electròniques i dels procediments cibernètics en general —cal recordar que el treball de Frosini es remunta als anys seixanta— entre els juristes, es requereix, en general, fins i tot abans que una racionalització acabada en la producció jurídica, una simplificació dels conceptes, els mètodes i les tècniques tradicionals. Així mateix, Frosini recull la crítica ja inicial que Spengler realitzà a aquests tipus de sistemes, tot indicant que una «justícia feta a màquina» dóna lloc a un nou fetitxisme, augmenta la rigidesa conceptual dels juristes i afavoreix la pèrdua del sentit de la responsabilitat personal, en especial a partir d'una

conceptualització purament analítica que pot conduir a malentesos radicals de normes, sentències i documents jurídics.

Malgrat aquestes reserves inicials, l'any 1963 Kerimov[57] anunciava una planificació interessant —i, a parer nostre, força actual— dels objectius de recerca i aplicació de l'automatització legal a l'extinta Unió Soviètica. En aquesta obra apareix recollit explícitament l'objectiu d'analitzar les institucions de dret públic partint de la teoria dels jocs, amb simulacions electròniques per trobar els mitjans més eficaços i racionals per aplicar-les. Aquesta planificació es va concretar parcialment en experiències de càlcul de la possibilitat de jubilació de treballadors a petició pròpia.

Entre nosaltres, Pérez Luño[58] manté que la informàtica jurídica té com a objecte l'aplicació de la tecnologia de la informació al dret. Considera que es tracta d'una disciplina bifront de metodologia tecnològica i objecte jurídic, que precisament condiciona l'aplicació d'aquest mètode.

Pérez Luño distingeix tres grans tipus d'aplicacions d'informàtica jurídica:

- La informàtica jurídica documental, l'objecte de la qual és l'automatització dels sistemes d'informació relatius a les fonts del coneixement jurídic: legislació, jurisprudència i doctrina.

- La informàtica jurídica de gestió, que té com a objecte l'automatització de les tasques rutinàries que es desenvolupen en qualsevol oficina, incloent-hi el despatx jurídic o administratiu.

- La informàtica jurídica de decisió, integrada per procediments adreçats a la substitució o la reproducció, total o parcial, de les activitats del jurista mitjançant l'aplicació de la programació algebraica o lògica, en aquest cas, especialment des de la branca de la informàtica identificada amb l'expressió general d'intel·ligència artificial, i, en particular, des de la disciplina dels sistemes experts i de l'enginyeria del coneixement.

  En particular, l'autor esmenta l'aparició de projectes i prototipus de sistemes experts jurídics en liquidacions tributàries, càlcul d'indemnitzacions per accidents laborals o de trànsit, predicció de les conseqüències jurídiques en casos d'impacte mediambiental o condicions d'adquisició de la nacionalitat i dret de família.

[57] D.A. Kerimov. «Future applicability of cybernetics to jurisprudence in the U.S.S.R», *Modern Uses of Lovic in Law*, 1963, citat per Frosini.

[58] Antonio-Enrique Pérez Luño. *Manual de informática*…, *op. cit*.

En relació amb la informàtica jurídica de decisió, que seria el tipus dins el qual hem d'inscriure les aplicacions informàtiques que ofereixen suport a l'actuació administrativa automàtica, Pérez Luño adverteix, en la tradició general —a la qual ens adherim— que s'ha de considerar insuficient la inferència lògica —més o menys representativa, com hem vist anteriorment— ja què substitueix la interpretació del dret per part de les persones pel raonament subjacent.

En efecte, en la mesura que les màquines poden processar informacions i establir inferències lògiques, però no poden comprendre la multiplicitat de circumstàncies que concorren en les conductes humanes, no sembla adient la suplantació plena de l'intèrpret pel càlcul matemàtic de l'ordinador, sinó que només en aspectes de l'experiència rutinària, estandarditzats, formalitzables i amb variables predeterminades tancades és possible recórrer a sistemes completament automàtics.

Tanmateix, l'adopció d'aquesta posició no implica que l'abast de l'actuació administrativa automatitzada hagi de ser reduït: els casos avaluats al llarg d'aquest treball de recerca presentats anteriorment són excel·lents candidats a l'automatització.

Podem indicar que l'aplicació que permeti l'actuació administrativa automatitzada serà una aplicació d'informàtica jurídica de decisió que s'ha de basar intensament en l'anàlisi lògica de les proposicions normatives, tot i que serà potestat de cada Administració pública decidir el llenguatge a aplicar.

Mentre que en alguns casos s'optarà per una aproximació de sistema expert, basat en una representació plena del coneixement del domini jurídic involucrat i l'ús de llenguatges de programació lògica capaços de decidir en temps d'execució, en la majoria de casos existirà una primera fase d'anàlisi i disseny de l'aplicació que hauria de considerar les eines de formalització i d'interpretació lògica presentades anteriorment. Posteriorment es codificarà un programa emprant llenguatges i mètodes de computació tradicionals, sovint obeint a criteris d'eficiència computacional i cost.[59]

Sigui com sigui, a parer nostre és absolutament necessari gestionar adequadament el cicle de vida del programari o l'aplicació que implementa l'actuació administrativa automatitzada mitjançant metodologies de qualitat i seguretat, independentment de l'orientació escollida.

[59] En aquest sentit, George F. Luger i William A. Stubblefield. *Artificial Intelligence*…, *op. cit.*

5.2. La gestió del cicle de vida del programari

Cal remarcar que la referència a l'anàlisi i al disseny de l'aplicació d'actuació administrativa automatitzada, així com la resta d'aspectes identificats, de seguretat, d'auditoria del codi, etc., que deriven de la interpretació de l'article 39 de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, s'han d'entendre com a processos i interfícies del cicle de vida del programari, és a dir, com a fases d'un procés més ampli, que és el procés de desenvolupament de sistemes d'informació, el qual s'ha de definir i gestionar dins l'Administració pública que implementa l'actuació administrativa automatitzada.

Aplicar una metodologia —més o menys formalitzada i madura— per al desenvolupament del programari que suporta l'aplicació d'actuació administrativa automatitzada implica assumir una sèrie de riscos, especialment en relació amb possibles errors de programació, que es poden actualitzar en forma d'una programació inadequada del sistema i, per tant, en motiu d'impugnació de l'actuació per part dels afectats.

Resulta, per tant, necessari presentar de forma succinta una metodologia de cicle de vida del programari. A l'Estat espanyol, el Consell Superior d'Administració Electrònica del Ministeri d'Administracions Públiques (avui Ministeri de la Presidència) ha desenvolupat la metodologia MÉTRICA, que es descriu a continuació. Existeixen moltes altres metodologies de desenvolupament, algunes força més actualitzades que MÉTRICA, de manera que l'elecció de MÉTRICA es duu a terme a efectes purament didàctics i, sobretot, per la seva utilització en el sector públic estatal.

La metodologia MÉTRICA versió 3 ofereix a les organitzacions un instrument útil per a la sistematització de les activitats que donen suport al cicle de vida del programari dins el marc que permet assolir els objectius següents:

- Proporcionar o definir sistemes d'informació que ajudin a aconseguir les finalitats de l'organització mitjançant la definició d'un marc estratègic per al desenvolupament d'aquests sistemes.
- Dotar l'organització de productes de programari que satisfacin les necessitats dels usuaris concedint una major importància a l'anàlisi de requisits.
- Millorar la productivitat dels departaments de sistemes i tecnologies de la informació i les comunicacions permetent una major capacitat d'adaptació als canvis i tenint en compte la possible reutilització.
- Facilitar la comunicació i la comprensió entre els diferents participants en la producció de programari durant el cicle de vida del projecte tenint en compte el seu paper i la seva responsabilitat, així com les necessitats de tothom.

- Facilitar l'operació, el manteniment i l'ús dels productes de programari obtinguts.

Pel que fa a estàndards, s'ha considerat referència principal el model de cicle de vida de desenvolupament proposat a la norma ISO 12207 Information Technology / Software Life Cycle Processes. Seguint aquest model, s'ha elaborat l'estructura de MÉTRICA versió 3, en la qual es distingeixen processos principals (planificació, desenvolupament i manteniment) i interfícies (gestió de projectes, assegurament de la qualitat, seguretat i gestió de projectes) amb l'objectiu d'oferir suport al projecte en els aspectes organitzatius.

A més de la norma ISO 12207 —la primera publicació de la qual data de 1995—, entre els estàndards de referència cal destacar les normes ISO/IEC TR 15504/SPICE Software Process Improvement and Assurance Standards Capability Determination, UNE-EN-ISO 9001:2000 Sistemes de Gestió de la Qualitat. Requisits, UNE-EN-ISO 9000:2000 Sistemes de Gestió de la Qualitat. Fonaments i Vocabulari, i l'estàndard IEEE 610.12-1990 Standard Glossary of Software Engineering Terminology. Igualment, s'han considerat altres metodologies com ara SSADM, Merise, Information Engineering, MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información —promoguda pel Consell Superior d'Informàtica (avui Consell Superior d'Administració Electrònica)— i EUROMÉTODO.

Des d'una altra perspectiva, cal indicar que MÉTRICA descriu únicament els processos i les activitats del cicle de vida del programari, però no té en consideració aspectes de millora de capacitats ni de maduresa relatius a aquest cicle de vida.

Així mateix, cal tenir en compte que des de la publicació de MÉTRICA versió 3 ha tingut lloc una important evolució en els estàndards internacionals de referència, cosa que aconsella avaluar la conveniència de fer servir MÉTRICA o, per contra, d'adherir-se a les normes més recents, entre les quals podem esmentar les següents:

- ISO/IEC 12207:2008, que actualitza la versió anterior d'aquesta norma, així com les correccions tècniques dels anys 2002 i 2004.
- ISO/IEC 14764:2006, que amplia els detalls sobre el procés de manteniment de programari descrit a la ISO/IEC 12207 en relació amb la planificació, l'execució i el control, la revisió i l'avaluació, i el tancament del procés de manteniment.
- ISO/IEC 15288:2008, que estableix un marc de treball comú per descriure el cicle de vida dels sistemes creats per humans, de manera harmonitzada amb la norma ISO/IEC 12207 en el cas dels sistemes d'informació.

- ISO/IEC 15940:2006, que defineix els serveis d'un entorn d'enginyeria de programari que es poden emprar de manera genèrica o per a la producció automatitzada de programari.
- ISO/IEC 16085:2006, que defineix un procés per a la gestió del risc en el cicle de vida de sistemes o del programari, indistintament.

En el mateix sentit, sembla força necessari complementar la metodologia MÉTRICA amb un marc concret que permeti precisament avaluar, de manera continuada o per etapes, la implementació dels processos de desenvolupament de programari, com també altres processos relacionats, per a la qual cosa es podria fer servir, per exemple, el model CMMI for Development (Integració de Models de Maduresa de Capacitats per al Desenvolupament), publicat per l'Institut d'Enginyeria del Programari de la Universitat Carnegie Mellon, dels Estats Units d'Amèrica.

5.2.1. *Els processos de desenvolupament de sistemes d'informació*

MÉTRICA divideix el procés de desenvolupament de sistemes d'informació en cinc processos per facilitar-ne la comprensió i atenent a la seva amplitud i complexitat:

- Estudi de viabilitat del sistema.
- Anàlisi del sistema d'informació.
- Disseny del sistema d'informació.
- Construcció del sistema d'informació.
- Implantació i acceptació del sistema.

La necessitat de reduir el cicle de desenvolupament dels sistemes d'informació ha orientat moltes organitzacions cap a l'elecció de productes programari del mercat l'adaptació dels quals als seus requeriments significava un esforç força inferior al d'un desenvolupament a mida, per no parlar dels costos de manteniment.

Aquesta decisió, estratègica en moltes ocasions per a una organització, s'ha de prendre amb les precaucions necessàries, i és una realitat que està canviant l'escenari del desenvolupament del programari.

Una altra conseqüència d'aquest fet és la pràctica, cada cop més habitual en les organitzacions, de la contractació de serveis externs en relació amb els sistemes i les tecnologies de la informació i les comunicacions. Això condueix a la necessitat de

gestionar i controlar adequadament aquests serveis externs i el risc implícit[60] per tal que els resultats representin un benefici per a l'organització.

5.2.1.1. L'estudi de viabilitat del sistema

L'objectiu d'aquest procés és analitzar un conjunt concret de necessitats amb la idea de proposar una solució a curt termini. Els criteris amb què es fa aquesta proposta no han de ser estratègics, sinó tàctics i relacionats amb aspectes econòmics, tècnics, legals i operatius. Ja en aquest moment s'ha de considerar l'especial rellevància i els riscos particulars que pot implicar la realització d'actuacions administratives automatitzades, com desenvoluparem detalladament més endavant.

Els resultats de l'estudi de viabilitat del sistema han de constituir la base per prendre la decisió de tirar endavant o d'abandonar. Si es decideix tirar endavant, poden sorgir un o diversos projectes que afectin un o diversos sistemes d'informació. Aquests sistemes s'han de desenvolupar d'acord amb el resultat obtingut en l'estudi de viabilitat i tenint en compte la cartera de projectes per a l'estratègia d'implantació del sistema global.

S'ha considerat que aquest procés és obligatori, tot i que el nivell de profunditat amb què s'executi dependrà de cada cas. La conveniència de fer l'estudi de la situació actual depèn del valor afegit previst per a l'especificació de requisits i per al plantejament d'alternatives de solució. En les alternatives, es consideren típicament solucions "a mida", solucions basades en l'adquisició de productes programari del mercat o solucions mixtes.

5.2.1.2. L'anàlisi del sistema d'informació

El propòsit d'aquest procés es aconseguir l'especificació detallada del sistema d'informació a través d'un catàleg de requisits i una sèrie de models que cobreixin les necessitats d'informació dels usuaris per als quals s'ha de desenvolupar el sistema d'informació, i que han de ser l'entrada al procés de disseny del sistema d'informació.

En primer lloc, s'ha de descriure el sistema d'informació a partir dels productes generats en el procés d'estudi de viabilitat del sistema. Se'n delimita l'abast, es genera un catàleg de requisits generals i es descriu el sistema mitjançant uns models inicials d'alt nivell.

[60] En relació amb l'externalització, vegeu Carles Ramió, Miquel Salvador i Oriol Garcia, *Els determinants i la gestió de l'externalització a Catalunya. Món local i món autonòmic*. Barcelona: Escola d'Administració Pública de Catalunya, 2007.

Es recullen de manera detallada els requisits funcionals que el sistema d'informació ha de cobrir —cosa que resulta especialment sensible en el cas de l'actuació administrativa automatitzada, que ha d'interpretar d'una manera particularment completa i acurada la norma jurídica a aplicar— i es cataloguen, fet que permet establir la traça al llarg dels processos de desenvolupament. A més, s'identifiquen els requisits no funcionals del sistema, és a dir, les facilitats que ha de proporcionar el sistema i les restriccions a què es trobarà sotmès quant a rendiment, freqüència de tractament, seguretat, etc.

Per facilitar l'anàlisi del sistema, s'han d'identificar els subsistemes d'anàlisi i s'han d'elaborar els models de casos d'ús i de classes, en desenvolupaments orientats a objectes, i de dades i processos, en desenvolupaments estructurats. Cal desenvolupar una activitat específica per a la definició d'interfícies d'usuari a mesura que es van depurant els requisits i els models anteriors. Així mateix, cal especificar totes les interfícies entre el sistema i l'usuari, com ara formats de pantalles, diàlegs, formats d'informes i formularis d'entrada.

Un cop acabats els models, s'ha de dur a terme una anàlisi de consistència mitjançant una verificació i una validació, cosa que pot forçar la modificació d'alguns dels models obtinguts. Com també tractarem posteriorment, aquesta activitat adquireix una rellevància particular en el cas de la definició funcional d'un procediment administratiu que incorpori l'actuació administrativa automatitzada, ja que ofereix l'oportunitat de detectar carències i errors en la interpretació de la norma en què es basarà l'actuació administrativa automatitzada esmentada.

Després de fer aquesta anàlisi de consistència, s'elabora l'especificació de requisits de programari, que constitueix un punt de referència en el desenvolupament del programari i la línia base de referència per a les peticions de canvi sobre els requisits especificats inicialment.

En aquest procés s'inicia també l'especificació del pla de proves, que s'ha de completar en el procés corresponent al disseny del sistema d'informació.

En aquestes activitats és molt important la participació dels usuaris a través de tècniques interactives —com ara disseny de diàlegs i prototips—, les quals permeten que els usuaris es familiaritzin amb el nou sistema i col·laborin en la construcció i el perfeccionament d'aquest.

Tal com hem avançat, en el cas de l'actuació administrativa automatitzada cal involucrar intensament personal expert en l'àmbit legal en aquestes activitats per garantir una anàlisi adequada dels requisits funcionals, a partir d'una interpretació jurídica apropiada

de les normes en què es basaran els actes administratius i, molt especialment, els de naturalesa decisòria.

5.2.1.3. El disseny del sistema d'informació

El propòsit del disseny del sistema d'informació és obtenir la definició de l'arquitectura del sistema i de l'entorn tecnològic que li ha d'oferir suport, juntament amb l'especificació detallada dels components del sistema d'informació. A partir d'aquesta informació, es generen totes les especificacions de construcció relatives al sistema, així com l'especificació tècnica del pla de proves, la definició dels requisits d'implantació i el disseny dels procediments de migració i càrrega inicial, quan s'escaigui.

Aquest procés consta d'un primer bloc d'activitats, que es desenvolupen en paral·lel, amb l'objectiu d'obtenir el disseny de detall del sistema d'informació que comprèn la partició física del sistema d'informació (independent d'un entorn tecnològic concret), l'organització en subsistemes de disseny, l'especificació de l'entorn tecnològic sobre el qual es despleguen aquells subsistemes, i la definició dels requisits d'operació, administració del sistema, seguretat i control d'accés.

Igual que en el procés d'anàlisi del sistema d'informació, abans d'especificar els components s'ha de fer una verificació i una validació a fi d'analitzar la consistència entre els diferents models i formalitzar l'acceptació del disseny de l'arquitectura del sistema per part dels usuaris d'explotació i sistemes.

Com també hem indicat anteriorment, semblaria necessari involucrar en aquesta verificació i en aquesta validació personal expert que pugui garantir la consistència entre el disseny i la interpretació legal que es va fixar en les etapes anteriors, amb la finalitat d'evitar possibles errors.

A més, considerem que resulta particularment important establir controls tècnics que garanteixin la seguretat de les operacions, en el sentit que exposarem més endavant.

5.2.1.4. La construcció del sistema d'informació

La construcció del sistema d'informació té com a objectiu final la construcció i la prova dels diferents components del sistema d'informació a partir del conjunt d'especificacions lògiques i físiques corresponents, obtingut en el procés de disseny del sistema

d'informació. Es desenvolupen els procediments d'operació (no són necessaris en el cas de l'actuació administrativa automatitzada) i seguretat, i s'elaboren els manuals d'usuari final (tampoc no resulten necessaris en el cas de l'actuació administrativa automatitzada) i d'explotació, quan s'escaigui.

Per aconseguir aquest objectiu, s'ha de recollir la informació relativa al producte del disseny d'especificacions de construcció del sistema d'informació, preparar l'entorn de construcció, generar el codi de cadascun dels components del sistema d'informació i efectuar, a mesura que es vagi finalitzant la construcció, les proves unitàries de cadascun i les proves d'integració entre subsistemes.

Si calgués dur a terme una migració de dades, seria en aquest procés on s'executaria la construcció dels components de migració i els procediments de migració i càrrega inicial de dades.

5.2.1.5. La implantació i l'acceptació del sistema

Aquest procés té com a objectiu principal el lliurament i l'acceptació del sistema en la seva totalitat, que pot comprendre diversos sistemes d'informació desenvolupats de manera independent, segons s'hagi establert en el procés d'estudi de viabilitat del sistema. El segon objectiu és dur a terme les activitats oportunes per passar a la producció del sistema.

S'estableix el pla d'implantació, un cop revisada l'estratègia d'implantació, i es detalla l'equip que l'executarà.

Per a la iniciació d'aquest procés es prenen com a punt de partida els components del sistema provats de manera unitària i integrats en el procés construcció del sistema d'informació, així com la documentació associada.

El sistema s'ha de sotmetre a les proves d'implantació amb la participació de l'usuari d'operació, que té la responsabilitat, entre altres aspectes, de comprovar el comportament del sistema en les condicions més extremes. El sistema s'ha de sotmetre igualment a les proves d'acceptació que ha d'executar l'usuari final.

També en aquest cas podem cridar ja l'atenció sobre la necessitat d'establir controls propis en el cas de l'acceptació del sistema d'informació que ofereix suport a l'actuació administrativa automatitzada.

En aquest procés s'elabora el pla de manteniment del sistema, de tal manera que el responsable del manteniment conegui el sistema abans que passi a producció.

Finalment, s'estableix l'acord de nivell de servei requerit un cop s'iniciï la producció. Aquest acord fa referència als serveis de gestió d'operacions, de suport a usuaris, i al nivell d'acord amb què s'han de prestar aquests serveis.

5.2.2. *El procés de manteniment de sistemes d'informació*

L'objectiu d'aquest procés és obtenir una nova versió d'un sistema d'informació a partir de les peticions de manteniment que fan els usuaris amb motiu d'un problema detectat en el sistema o bé per la necessitat de millorar-lo.

Davant una petició de canvi d'un sistema d'informació ja en producció, s'efectua un registre de les peticions, es diagnostica el tipus de manteniment i es decideix si s'hi dóna resposta o no —en funció del pla de manteniment associat al sistema afectat per la petició—, i s'estableix amb quina prioritat.

La definició de la solució de la necessitat o el problema plantejat per l'usuari, que fa el responsable de manteniment, inclou un estudi d'impacte, la valoració de l'esforç i del cost, les activitats i les tasques del procés de desenvolupament a realitzar i el pla de proves de regressió.

En aquest procés també cal indicar la necessitat d'establir controls específics en el cas de l'actuació administrativa automatitzada, sobretot derivats de la necessitat de detectar i tractar correctament els canvis sobre el sistema d'informació motivats per una modificació (o derogació) de la norma jurídica. En efecte, es podria donar la situació que, un cop derogada una norma, el sistema automatitzat continués prenent decisions administratives d'acord amb la norma derogada, les quals resultarien incorrectes, lògicament.

Per tant, cal considerar amb especial cura el procediment de manteniment del programari, per exemple mitjançant un procés de registre en una base de dades de les normes que han estat objecte d'automatització. Una persona haurà de fer el seguiment de la normativa, de manera que, un cop hagi estat derogada una norma que doni suport a procediments automàtics, ho pugui detectar i en pugui avaluar l'impacte per tal d'aturar eventualment el sistema i obrir un procediment de manteniment.

Normalment hi haurà prou temps des de la publicació de la norma fins a l'entrada en vigència de la norma substitutiva. Això permetrà fer les modificacions oportunes, sempre que s'hagi previst aquest manteniment evolutiu.

El procés de registre i seguiment es podria automatitzar en la mesura que els editors de les fonts escrites del dret —en particular, els diaris oficials— adoptin estàndards de publicació de normes en XML, com ara MetaLex,[61] cosa que permetria identificar les normes derogatòries sense intervenció humana i generar l'alerta pertinent.

5.3. Alguns requisits específics de l'aplicació d'actuació administrativa automatitzada

En la fase d'anàlisi, MÉTRICA recull una sèrie de tècniques orientades a construir el model de casos d'ús i de classes, en desenvolupaments orientats a objectes, i de dades i processos, en desenvolupaments estructurats. En aquest punt cal garantir que la interpretació logicoinformàtica de la norma és completa i adequada, és a dir, que no queden casos vàlids no considerats, o que no es produeixen ambigüitats ni errors que impliquin discriminació per als ciutadans derivada d'una decisió inadequada. Aquí hem d'introduir la discussió sobre la interpretació lògica del dret (aplicant lògica deòntica, per exemple).

Cal remarcar la importància de l'anàlisi de consistència en la fase d'anàlisi funcional i de disseny tècnic (doble control), ja que representen punts de control per detectar problemes en la interpretació en lògica informàtica de la norma jurídica aplicable. Podem fer una certa crítica al model de rols participants en la gestió del projecte de desenvolupament, atès que MÉTRICA no considera la participació d'experts legals en cap fase de la metodologia.

Totes les lògiques jurídiques que hem presentat (deòntica, refutable i descriptiva), aplicades en forma de lògiques híbrides en un procés reglat i controlat d'interpretació normativa, ens poden ajudar a adquirir i formalitzar els coneixements jurídics de la norma a automatitzar, així com a establir mecanismes de validació; de retruc, això reduirà els riscos inherents a l'actuació administrativa automatitzada.

En particular, l'ús d'una lògica modal híbrida, amb elements de lògica deòntica i refutable, molt especialment en el context de la lògica de l'acció, constitueix un element molt potent per obtenir una interpretació objectiva i acurada dels aspectes estructurals de la norma i del seu comportament argumentador (la qual cosa permet una certa

[61] CEN CWA 15710:2007. MetaLex (Open XML Interchange Format for Legal and Legislative Resources).

previsibilitat de les possibles aplicacions de la norma en cas de conflicte, sigui judicial o administratiu, en termes de procés).

D'altra banda, l'ús de la lògica descriptiva i de les ontologies ens permet un formalisme de representació del coneixement jurídic que actua com a base per al disseny d'aplicacions jurídiques avançades.

En aquest sentit, la interpretació lògica pot quedar formalitzada en diversos moments al llarg del cicle de vida del programari que ofereix suport a l'actuació administrativa automatitzada:

- Una primera possibilitat és realitzar i formalitzar la interpretació lògica en la fase d'anàlisi funcional i disseny del programari. En aquest cas, la interpretació és un procés dut a terme per un intèrpret humà. El procés generarà un conjunt de casos que més tard han de servir per codificar informàticament el tractament d'aquests casos (la funcionalitat del programa que permet l'actuació administrativa automatitzada).

- Una segona possibilitat, complementària de l'anterior, consisteix a realitzar i formalitzar la interpretació lògica en el moment de construir el programari i, en concret, en el procés de codificació informàtica. Novament la interpretació es un procés dut a terme per un intèrpret humà, però en el mateix moment de produir el codi del programa.

- Una tercera possibilitat és realitzar i formalitzar la interpretació lògica en forma de regles a aplicar en el moment d'execució del programa, sense que en el codi del programa es trobi cap lògica de funcionament de l'aplicació. Constitueix un exemple d'aquesta tercera possibilitat l'anomenada *programació lògica*, basada en l'ús de programes raonadors, com succeeix en els anomenats *sistemes experts* i, més recentment, en la Web semàntica.

  En aquest cas, la interpretació és un procés realitzat només parcialment per un intèrpret humà, que col·labora en el procés de representació del coneixement jurídic i codifica les regles que després permetran al programa, mitjançant operacions lògiques, decidir els casos als quals resulta aplicable aquesta norma, en una mena d'interpretació purament logicista o mecànica.

- Una quarta possibilitat és dissenyar el sistema de tal manera que sigui ell mateix qui generi, a partir de la lectura i la comprensió de la norma jurídica, tant la representació del coneixement jurídic com les regles d'inferència lògica necessàries per aplicar les normes. Només en aquest cas podríem considerar que

existeix una veritable interpretació per part de la màquina, que, malgrat el volum d'experiències realitzades, especialment en el domini de la recerca de textos jurídics, no considerem practicable en l'actualitat.

- D'altra banda, s'ha de considerar la utilitat d'aquestes eines en els processos de verificació del programari produït. Efectivament, una de les possibilitats més interessants que ofereixen les eines lògiques que hem presentat és, precisament, la possibilitat d'avaluar formalment el programa que ofereix suport a l'actuació administrativa automatitzada, de forma integrada durant el procés de construcció o com a procediment d'avaluació de la idoneïtat del programa en moments posteriors, durant el procés natural de manteniment del programa, que en aquest cas esdevé particularment rellevant pel fet que el sistema experimentarà ordinàriament l'impacte dels canvis normatius.

Evidentment, el fet de no disposar —o de no fer ús— d'aquestes eines no vol dir en cap cas que el producte resultant —és a dir, el programa o l'aplicació que ofereix suport a l'actuació administrativa automàtica— sigui incorrecte o de baixa o poca qualitat, però és cert que amb l'actuació administrativa automatitzada es produeix una situació nova: és el mateix programa el que decideix sense la intervenció de cap persona concreta. Així, es podria donar el cas d'un òrgan administratiu concret (una direcció general, per exemple) que, tenint vacant la plaça per cessament del director o directora (motivat per un canvi electoral, posem per cas), continua prenent decisions administratives que produeixen efectes interns i externs.

Es tracta d'un escenari molt diferent de l'actual, en què l'ordinador senzillament assisteix o prepara una decisió humana, i que obliga a assolir una comprensió molt acurada de les normes a aplicar per via d'una interpretació que no pot quedar en mans de la figura de l'analista informàtic —ja ho podem avançar—, sinó que requereix el concurs i la participació dels experts en el domini legal i de la consciència de la persona titular de l'òrgan impulsor de l'automatització.

Aquesta necessitat —que, si és important en general, ens sembla extraordinàriament rellevant en el cas de l'actuació automatitzada— exigeix revisar les metodologies del cicle de vida del programari i establir requisits i condicions específics, ja que l'actuació administrativa automatitzada és resultat d'un producte d'enginyeria i ha de ser tractat com a tal.

5.4. La determinació dels requisits de formalització documental electrònica

A partir de l'anàlisi de la funcionalitat de l'aplicació, cal detallar els requisits de seguretat de l'aplicació en termes d'autenticitat, integritat i confidencialitat del producte documental que l'aplicació genera.

Per dur a terme aquesta tasca, disposem de diferents eines, entre les quals podem esmentar la metodologia PADS desenvolupada per l'Agència Catalana de Certificació.[62]

L'anàlisi PADS és una eina que es proposa per analitzar els requisits en relació amb els actes documentats que es produeixen dins els processos i els procediments de l'Administració i els seus organismes i entitats, públics o privats.

L'objectiu d'aquesta anàlisi és obtenir un catàleg de requisits dels actes documentats del procediment que descrigui les necessitats quant als nivells funcionals de seguretat de servei.

5.4.1. *L'anàlisi dels processos (P)*

Els processos són, en una visió molt simplificada, seqüències d'esdeveniments que condueixen a un resultat concret. Aquests esdeveniments poden consistir en fets o en accions que desencadenen un pas endavant o endarrere dins el procés.

El procediment administratiu és un bon exemple de procés regulat, totalment o parcialment, d'acord amb la llei, que en determina el flux, el contingut i els efectes.

Juntament amb els procediments administratius, podem trobar processos corresponents a la prestació de serveis públics o, fins i tot, a la prestació de serveis privats per part de les administracions públiques i els seus organismes.

La primera tasca a desenvolupar en l'anàlisi PADS és la definició del procés al qual es vol incorporar la signatura electrònica. Existeixen múltiples definicions de procediments, des

[62] Ignacio Alamillo, Daniel Martínez, Philip Seltsikas i Nikolaos Papas. «Designing a Modelling Methodology for Legal Workflows», *Legal Knowledge and Information Systems - JURIX 2007: The Twentieth Annual Conference on Legal Knowledge and Information Systems, Leiden, The Netherlands, 12-15 December 2007*. Frontiers in Artificial Intelligence and Applications 165. IOS Press. Amsterdam. 2007.

de les més informals en llenguatge natural fins a l'ús de llenguatges formals de definició i d'execució de processos.[63]

Aquesta guia no adopta cap model formal per a la definició dels processos, ja que aquesta anàlisi és instrumental pel que fa a la determinació dels documents generats en l'execució dels processos, i, en especial, dels requisits de signatura corresponents. Tanmateix, es recomana l'adopció d'un mètode formal, apropiat al tipus d'aplicació i entorn de negoci concret.

Els aspectes a considerar són els següents:

1. Quin és el contingut del procés?	- Descripció del procés. - Modalitat de gestió (servei en gestió privada, gestió pública, procediment administratiu). - Efectes que produeix el procés.
2. Quina és la normativa aplicable al procés?	- Identificació de les normes aplicables. - Significació jurídica del procés. - Condicions jurídiques necessàries perquè el procés es pugui realitzar.
3. Quin és el flux de treball?	- Llistat o gràfic dels esdeveniments que el conformen, incloent-hi els actes i els fets rellevants, així com les connexions corresponents.
4. Quins són els processos relacionats?	- Processos anteriors. - Processos coetanis. - Processos posteriors.

5.4.2. *L'anàlisi dels actes (A)*

Un cop hem identificat els processos, escau analitzar-ne els actes avaluant cada acte per separat.

Els actes són, en definitiva, els verbs corresponents a l'acció (del ciutadà, de l'Administració o de terceres persones o entitats) que inicia, impulsa o acaba el procés. Es diferencien dels fets o les omissions en què habitualment cal documentar-los.

[63] A aquest efecte, actualment existeixen iniciatives que treballen en la definició d'estàndards d'abast internacional en relació amb la notació de processos de negoci (BPMN), llenguatges de definició de processos de negoci (BPDL o XBPL) o execució de processos de negoci (WS BPEL).

Alguns exemples habituals són:

- Sol·licitar, presentar (sol·licituds, declaracions, documents complementaris, al·legacions, recursos). En aquest tipus d'acte és freqüent encabir una part important de la relació telemàtica amb les administracions públiques, bé directa amb la persona interessada o amb una tercera persona que presenta en nom seu.
- Registrar (d'entrada, de sortida, en un llibre o registre administratiu).
- Informar, donar vistiplau i altres actes semblants.
- Resoldre.
- Notificar, comunicar i altres actes semblants.

Captar la naturalesa exacta de cada acte resulta essencial per a les futures fases d'anàlisi:

- Per exemple, no tots els actes es manifesten en documents independents, sinó que resulta freqüent trobar diversos actes documentats al mateix instrument. Un cas paradigmàtic és un document d'autorització de pagament, que incorpora actes de diferents òrgans la plasmació dels quals es recull al mateix document. Per tant, caldrà distingir els actes dels documents.

- En alguns actes, pot resultar indiferent qui és la persona física que el produeix, tal com succeeix en alguns actes preparatoris d'una resolució administrativa, en què qualsevol treballador públic d'un grup concret podria preparar l'expedient pel fet que l'acte legalment vàlid el durà a terme un òrgan administratiu unipersonal, per exemple. Un altre cas semblant és el del simple impuls del procediment o els trasllats d'expedients, que no tenen rellevància externa i que, per tant, no han de revestir les formalitats dels actes administratius.

- Per contra, en altres actes precisament la persona que els realitza és absolutament essencial, així com la qualitat del procés d'actuació amb mitjans electrònics.

Els aspectes a considerar són els següents:

1. Quin és el contingut de l'acte?
   - Descripció de l'acte.
   - Tipus d'acte (del ciutadà/de l'Administració, altres).
   - Efectes que produeix dins el procés (inicia, acaba, altres).

2. Quina és la normativa aplicable a l'acte?	- Identificació de les normes aplicables. - Significació jurídica de l'acte (acte reglat/discrecional i altres consideracions). - Condicions jurídiques necessàries perquè l'acte es pugui realitzar. - Obligació legal o administrativa de documentar l'acte.
3. Qui realitza l'acte?	- Persona física (ciutadà). - Treballador de l'Administració (si s'escau, funcionari). - Òrgan unipersonal de l'Administració.
4. En quina qualitat realitza l'acte?	- En nom propi i per compte propi. - En qualitat d'òrgan d'una persona jurídica pública o privada (representació orgànica). - En qualitat de representant legal d'una persona física o jurídica, pública o privada. - En qualitat de representant voluntari d'una persona física o jurídica, pública o privada. - En qualitat de representant professional d'una persona física o jurídica (representació presumpta).
5. Existeix possibilitat de substitució personal?	- Actes estrictament personals. - Qualsevol representant. - Qualsevol persona física amb una qualitat concreta (p. ex., qualsevol treballador públic d'un grup).
6. Genera un document nou, es manifesta sobre un document existent prèviament o sobre un registre (d'expedient o de llibres)?	- Genera un document nou. - Es plasma en un document existent. - Es registra, sense generar manifestació documental.
7. Requereix la comprovació prèvia de la identitat de qui realitza l'acte?	- Sí/No. - Determinació del mètode d'identificació i autenticació de la persona que actua. - En concret, necessitat d'emprar codis, números o targetes d'identificació per poder actuar. - Valoració del nivell d'evidència del mètode emprat d'acord amb l'esquema de CATCert.
8. Requereix la comprovació prèvia de la qualitat de qui realitza l'acte?	- Sí/No. - Comprovació de la facultat d'actuació, orgànica o legal. - Comprovació d'un apoderament o d'una autorització, en representació voluntària. - Comprovació de la condició de professional de col·lectiu autoritzat.

9. Requereix una comunicació confidencial prèvia o posterior?	- Sí/No. - Determinació del mètode de protecció emprat.
10. És d'execució automàtica o mecànica, totalment o parcialment?	- Sí/No. - Determinació dels tractaments automàtics o mecànics.

5.4.3. *L'anàlisi dels documents i els registres (D)*

Pel que fa als actes a documentar, cal identificar les sortides documentals que generen, així com els requisits formals corresponents, tant en documents independents com en col·leccions de documents (llibres electrònics) o registres administratius electrònics.

Alguns exemples habituals són:

- Les sol·licituds de serveis públics o en relació amb procediments administratius.
- Les resolucions administratives i les seves notificacions.
- Els recursos de tot tipus.
- Els llibres o els registres electrònics administratius.
- Les certificacions i les còpies.

Els aspectes a considerar són els següents:

1. Quin és el contingut del document?	- Descripció del document. - Tipus de document (privat, administratiu, públic).
2. Quina és la normativa aplicable al document?	- Identificació de les normes aplicables.
3. Quins requisits formals són exigibles?	- Necessitat de ser original, còpia simple o còpia autèntica. - Necessitat d'incorporar una signatura. - Necessitat d'incorporar una marca, un registre o un segell. - Necessitat d'incorporar la data i/o l'hora. - Necessitat d'incorporar un rol, un càrrec o una altra condició subjectiva o personal.
4. Quins requisits d'acreditació del contingut són exigibles?	- Necessitat d'acreditar la personalitat jurídica. - Necessitat d'acreditar la capacitat per actuar en nom de tercer.

	- Necessitat d'aportar acreditació objectiva del contingut.
5. Quins són els destinataris del document?	- Persones o entitats destinatàries directes del document. - Persones o entitats a les quals pot arribar el document, indirectament (per exemple, mitjançant el lliurament per part del destinatari inicial).
6. Quin és el termini de vida previst del document?	- Nombre d'anys que el document roman en circulació. - Nombre d'anys que el document roman arxivat.

5.4.4. *L'anàlisi de les signatures o els segells (S)*

En el cas dels actes documentats, finalment resulta necessari identificar els requisits d'autenticitat, d'integritat i, habitualment, d'imputació de la qualitat d'autor o altres qualitats, fet que ens condueix a l'anàlisi dels requisits de signatura.

En aquest punt, i d'acord amb els requisits de l'acte i del document corresponent, cal determinar els aspectes concrets de la signatura o el segellament automàtic:

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). - Actua en nom propi o en representació.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. - Ordre de les signatures.

5.4.5. *Emprar certificats digitals per al servei*

Durant l'execució de l'anàlisi PADS duta a terme anteriorment haurem trobat necessitats relatives a l'autenticació robusta dels actors o la necessitat de protegir informació

confidencial, i especialment la necessitat de signar documents electrònics, funcionalitats que es basen en certificats.

L'objectiu d'aquesta fase és identificar el catàleg de requisits de certificació, que detalla els relatius als certificats que cal emprar com a suport de les operacions criptogràfiques d'autenticació, de signatura i de xifratge.

Els aspectes a considerar són els següents:

1. Quin tipus de certificats es necessiten?
   - Persona física.
     - Individuals/ciutadà.
     - Professionals.
     - Vinculació a entitat.
     - Representació.
   - Persona jurídica.
   - Entitat sense personalitat jurídica.
   - Dispositiu.
2. Quins usos cal donar als certificats?
   - Autenticació.
   - Signatura digital.
   - Xifratge.
3. Quines aplicacions específiques han de suportar els certificats?
   - S/MIME.
   - SSL/TLS.
   - Seguretat de serveis web.
   - Signatura de codi.
   - Signatura d'aplicació.
   - TSA, OCSP, altres.
4. Quines estratègies de certificació digital cal establir?
   - Emissió de certificats amb entitat de certificació pròpia.
   - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats).
     - Per a ús propi.
     - Per dotar terceres persones o entitats.
   - Admissió de certificats d'altres entitats de certificació.

5.4.6. *Preparació dels casos d'ús de seguretat de l'aplicació*

El casos d'ús del servei són un conjunt d'escenaris que descriuen les interaccions entre un usuari i un sistema d'informació a l'efecte d'establir els requisits corresponents. Els casos d'ús tenen un cicle de vida complex i, de fet, es transformen durant la seva evolució, des de la fase de descobriment, implementació i acceptació per part dels usuaris. Així doncs, hi ha diverses formes de representar els casos d'ús en funció del moment evolutiu del cas d'ús durant les fases d'anàlisi, desenvolupament, implementació i prova del programari.

És força habitual agrupar-los en diagrames de casos d'ús, que mostren les relacions entre els actors —usuaris o sistemes— i els diferents casos d'ús, cosa que permet visualitzar ràpidament la funcionalitat global del servei. Una altra representació emprada habitualment en relació amb els casos d'ús són els diagrames de seqüències d'interacció i els diagrames d'activitats, especificats d'acord amb el llenguatge universal de modelització (UML, *universal modeling language*).

En aquesta fase inicial convé preparar els casos d'ús relatius a les funcions de seguretat criptogràfica del servei, entre els quals caldria considerar els següents:

- Casos d'ús d'autenticació dels actors i de la documentació gestionada pels sistemes.
- Casos d'ús de signatura electrònica de documentació pels actors.
- Casos d'ús de signatura electrònica de transport segur de missatges entre actors i sistemes, com ara en el cas de la missatgeria de serveis web entre sistemes remots.
- Casos d'ús d'arxiu de signatura electrònica.
- Casos d'ús associats a les evidències electròniques, incloent-hi els procediments judicials i administratius en paper.

D'altra banda, no és estrany que la definició i la descripció dels casos d'ús evolucionin a mesura que s'hi treballa, de manera que podem trobar els estats següents:

- Casos d'ús identificats recentment, amb poca descripció a més del nom del cas d'ús.
- Casos d'ús descrits succintament, en general de manera poc rigorosa.
- Descripció inicial de les seqüències d'accions que conformen el cas d'ús.
- Identificació de la seqüència d'accions essencials que conformen el cas d'ús.
- Casos d'ús descrits detalladament, en forma narrativa o conversativa.
- Casos d'ús descrits completament, sense ambigüitats, que permeten la comprensió total, exacta i verificable del sistema.

Es recomana redactar els casos d'ús de seguretat de la manera més detallada possible o de manera que continguin, com a mínim, la identificació de la seqüència de les accions que resulten essencials en relació amb el cas d'ús, perquè molts incidents de seguretat deriven d'una definició incompleta de l'escenari.

Com a resultat d'aquesta anàlisi, s'ha d'obtenir el catàleg de casos d'ús de seguretat del servei d'acord amb les categories següents:

- Diagrama de casos d'ús.
- Diagrama de seqüències d'interacció dels casos d'ús.
- Diagrama d'activitats relatives als casos d'ús.

5.5. Anàlisi dels requisits de signatura o segellament i certificació dels casos d'ús d'automatització

A continuació exposem, com a cas pràctic, l'anàlisi dels requisits de signatura o segellament i certificació dels casos d'ús següents, presentats al capítol 4 anterior.

5.5.1. *L'expedició automàtica de rebut de registre electrònic*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu de registre i garanteix la validesa del rebut acreditatiu de la presentació. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. El registre actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs, especialment en relació amb els terminis administratius, es considera necessari acreditar la data de la signatura independentment de la data del document presentat.
4. La signatura s'ha de produir després d'una altra	- Sí/No.

	signatura?	No aplicable.
		- Ordre de les signatures.
		No aplicable.
5.	Quin tipus de certificats es necessiten?	- Dispositiu.
		No aplicable.
		- Servidor segur.
		No aplicable.
		- Seu electrònica.
		No aplicable.
		- Segell electrònic.
		Aplicable, en cas d'emissió automàtica del rebut de registre.
		- Personal al servei de l'Administració.
		Aplicable, en cas d'emissió manual del rebut de registre, cosa que ja s'anticipa poc convenient.
6.	Quins usos cal donar als certificats?	- Autenticació.
		No aplicable.
		- Signatura electrònica.
		Aplicable.
		- Xifratge.
		No aplicable.
7.	Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents.
		Aplicable, ja que el rebut serà, típicament, un document de presentació, com ara un PDF.
		- Correu electrònic S/MIME.
		No aplicable.
		- Canal segur SSL/TLS.
		No aplicable.
		- Seguretat de serveis web.
		Aplicable al lliurament de rebuts en comunicacions interadministratives.
		- Signatura de codi.
		No aplicable.
		- Signatura d'aplicació.
		No aplicable.
		- TSA, OCSP, altres.
		Aplicable, en la mesura que cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.
8.	Quines estratègies de certificació digital cal	- Emissió de certificats amb entitat de certificació pròpia.
		Aplicable.

establir?	- Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. No aplicable, perquè no hi ha recepció de rebuts d'altres administracions, sinó únicament emissió de rebuts propis.

5.5.2. *La comprovació automàtica de dades de sol·licitud*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu que actua i garanteix la validesa del procés de comprovació de la sol·licitud. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia o per delegació.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. No es considera necessari acreditar la data de la signatura independentment de la data del document de comprovacions.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No aplicable. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. Aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable.

- Personal al servei de l'Administració.

  No aplicable.

6. Quins usos cal donar als certificats?
   - Autenticació.

     No aplicable.
   - Signatura digital.

     Aplicable.
   - Xifratge.

     No aplicable.

7. Quines aplicacions específiques han de suportar els certificats?
   - Signatura de documents.

     Aplicable, ja que el document específic serà, típicament, un document estructurat.
   - Correu electrònic S/MIME.

     No aplicable.
   - Canal segur SSL/TLS.

     No aplicable.
   - Seguretat de serveis web.

     Aplicable per a la realització de comunicacions interadministratives necessàries per obtenir dades que permetin dur a terme les comprovacions automàtiques.
   - Signatura de codi.

     No aplicable.
   - Signatura d'aplicació.

     No aplicable.
   - TSA, OCSP, altres.

     No aplicable.

8. Quines estratègies de certificació digital cal establir?
   - Emissió de certificats amb entitat de certificació pròpia.

     Aplicable.
   - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats).
     - Per a ús propi.

       Aplicable.
     - Per dotar terceres persones o entitats.

       No aplicable.
   - Admissió de certificats d'altres entitats de certificació.

     Aplicable, per a la verificació de les signatures de comunicacions interadministratives necessàries per obtenir dades que permetin dur a terme les comprovacions automàtiques.

5.5.3. *La digitalització automàtica de documents*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu que actua i garanteix la validesa del procés de digitalització. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia o per delegació.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Es considera necessari acreditar la data de la signatura independentment de la data del document digitalitzat, ja que cal garantir en quin moment s'ha creat la còpia digital.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No aplicable. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable. - Personal al servei de l'Administració. No aplicable.
6. Quins usos cal donar als certificats?	- Autenticació. No aplicable. - Signatura digital. Aplicable. - Xifratge. No aplicable.
7. Quines aplicacions específiques han de suportar	- Signatura de documents. Aplicable.

	els certificats?	- Correu electrònic S/MIME. No aplicable. - Canal segur SSL/TLS. No aplicable. - Seguretat de serveis web. No aplicable. - Signatura de codi. No aplicable. - Signatura d'aplicació. No aplicable. - TSA, OCSP, altres. No aplicable.
8.	Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. Aplicable a la dotació de certificats propis a entitats contractades per al procés de digitalització. - Admissió de certificats d'altres entitats de certificació. Aplicable a les còpies digitalitzades per altres administracions públiques.

5.5.4. *L'impuls automàtic del procediment*

1.	Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu que actua i garanteix la validesa de l'acte d'impuls. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2.	Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia o per delegació.
3.	Cal acreditar la data de la	- Sí/No.

signatura independentment de la data del document?	No es considera necessari acreditar la data de la signatura independentment de la data del document corresponent.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No aplicable. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable. - Personal al servei de l'Administració. No aplicable.
6. Quins usos cal donar als certificats?	- Autenticació. No aplicable. - Signatura digital. Aplicable. - Xifratge. No aplicable.
7. Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents. Aplicable, ja que el document específic serà, típicament, un document estructurat. - Correu electrònic S/MIME. Aplicable quan l'acte d'impuls implica una comunicació per correu electrònic segur. - Canal segur SSL/TLS. No aplicable. - Seguretat de serveis web. Aplicable quan l'acte d'impuls implica la realització de comunicacions interadministratives necessàries per obtenir dades. - Signatura de codi. No aplicable. - Signatura d'aplicació. No aplicable. - TSA, OCSP, altres. No aplicable.

8. Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. Aplicable, per a la verificació de les signatures de comunicacions interadministratives necessàries per obtenir dades en alguns actes d'impuls.

5.5.5. *L'acte automàtic de constància electrònica*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs del document, especialment en el cas dels certificats.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. Depèn. - Ordre de les signatures. La normativa sectorial determina, en alguns casos d'expedició de certificats, la necessitat que signin diverses persones (com en el cas dels certificats dels acords dels òrgan col·legiats, en què signa el secretari de l'òrgan amb el vistiplau del president). Cal considerar les implicacions d'aquest flux de signatura en cas d'automatització del tràmit, ja que en principi es farà servir el segell de l'òrgan.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur.

No aplicable.

- Seu electrònica.

  No aplicable.

- Segell electrònic.

  Aplicable.

- Personal al servei de l'Administració.

  No aplicable.

6. Quins usos cal donar als certificats?
   - Autenticació.

     No aplicable.

   - Signatura electrònica.

     Aplicable.

   - Xifratge.

     No aplicable.

7. Quines aplicacions específiques han de suportar els certificats?
   - Signatura de documents.

     Aplicable, ja que el document corresponent a l'acte de constància serà, típicament, un document ofimàtic, com ara un PDF.

   - Correu electrònic S/MIME.

     No aplicable.

   - Canal segur SSL/TLS.

     No aplicable.

   - Seguretat de serveis web.

     Podria ser aplicable als actes automàtics de constància integrats en comunicacions interadministratives.

   - Signatura de codi.

     No aplicable.

   - Signatura d'aplicació.

     No aplicable.

   - TSA, OCSP, altres.

     Aplicable, en la mesura que cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.

8. Quines estratègies de certificació digital cal establir?
   - Emissió de certificats amb entitat de certificació pròpia.

     Aplicable.

   - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats).
     - Per a ús propi.

       Aplicable.

     - Per dotar terceres persones o entitats.

       No aplicable.

	- Admissió de certificats d'altres entitats de certificació. Aplicable en cas de recepció de documents de constància emesos per altres administracions.

5.5.6. *L'expedició automàtica de còpia autèntica electrònica*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs del document.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. Depèn. - Ordre de les signatures. La normativa sectorial determina, en alguns casos d'expedició de còpia autèntica, la necessitat que signin diverses persones, especialment quan la còpia gaudeix de fe pública. Cal considerar les implicacions d'aquest flux de signatura en cas d'automatització del tràmit, ja que en principi es farà servir el segell de l'òrgan.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable. - Personal al servei de l'Administració. No aplicable.
6. Quins usos cal donar als certificats?	- Autenticació. No aplicable.

	- Signatura electrònica. Aplicable. - Xifratge. No aplicable.
7. Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents. Aplicable, ja que el document corresponent a la còpia autèntica serà, típicament, un document de presentació, com ara un PDF. - Correu electrònic S/MIME. No aplicable. - Canal segur SSL/TLS. No aplicable. - Seguretat de serveis web. Podria ser aplicable als actes automàtics d'expedició de còpia autèntica integrats en comunicacions interadministratives. - Signatura de codi. No aplicable. - Signatura d'aplicació. No aplicable. - TSA, OCSP, altres. Aplicable, en la mesura que cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.
8. Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. Aplicable en cas de recepció de còpies autèntiques emeses per altres administracions.

5.5.7. *L'obertura i el tancament automàtic de llibres electrònics*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del llibre.

	- Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor de l'acte d'obertura i tancament del llibre. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. No.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable. - Personal al servei de l'Administració. No aplicable.
6. Quins usos cal donar als certificats?	- Autenticació. No aplicable. - Signatura electrònica. Aplicable. - Xifratge. No aplicable.
7. Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents. No aplicable. - Correu electrònic S/MIME. No aplicable. - Canal segur SSL/TLS. No aplicable. - Seguretat de serveis web. No aplicable.

	- Signatura de codi. No aplicable. - Signatura d'aplicació. Aplicable. - TSA, OCSP, altres. No aplicable.
8. Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. Aplicable en cas de recepció de llibres diligenciats o legalitzats per altres administracions públiques.

5.5.8. *La foliació automàtica d'expedients*

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. No.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable.

- Servidor segur.

  No aplicable.

- Seu electrònica.

  No aplicable.

- Segell electrònic.

  Aplicable.

- Personal al servei de l'Administració.

  No aplicable.

6. Quins usos cal donar als certificats?
   - Autenticació.

     No aplicable.

   - Signatura electrònica.

     Aplicable.

   - Xifratge.

     No aplicable.

7. Quines aplicacions específiques han de suportar els certificats?
   - Signatura de documents.

     Aplicable, ja que el document corresponent a l'índex serà, típicament, un document estructurat, com ara un XML.

   - Correu electrònic S/MIME.

     No aplicable.

   - Canal segur SSL/TLS.

     No aplicable.

   - Seguretat de serveis web.

     No aplicable.

   - Signatura de codi.

     No aplicable.

   - Signatura d'aplicació.

     No aplicable.

   - TSA, OCSP, altres.

     No aplicable.

8. Quines estratègies de certificació digital cal establir?
   - Emissió de certificats amb entitat de certificació pròpia.

     Aplicable.

   - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats).
     - Per a ús propi.

       Aplicable.

     - Per dotar terceres persones o entitats.

       No aplicable.

   - Admissió de certificats d'altres entitats de certificació.

     Aplicable en cas de recepció d'expedients indexats per altres

administracions públiques.

5.5.9. *La migració automàtica de document electrònic*

1.	Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2.	Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3.	Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs del document.
4.	La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No. - Ordre de les signatures. No aplicable.
5.	Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable. - Personal al servei de l'Administració. No aplicable.
6.	Quins usos cal donar als certificats?	- Autenticació. No aplicable. - Signatura electrònica. Aplicable. - Xifratge. No aplicable.
7.	Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents. Aplicable, ja que el document corresponent a la còpia autèntica serà, típicament, un document ofimàtic o de presentació, com ara un PDF. - Correu electrònic S/MIME.

	No aplicable. - Canal segur SSL/TLS. No aplicable. - Seguretat de serveis web. No aplicable. - Signatura de codi. No aplicable. - Signatura d'aplicació. No aplicable. - TSA, OCSP, altres. Aplicable, en la mesura que cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.
8. Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. Aplicable en cas de recepció de còpies autèntiques emeses per altres administracions.

5.5.10. Els intercanvis automàtics de dades entre administracions públiques

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs del document.
4. La signatura s'ha de produir després d'una altra	- Sí/No.

signatura?	No.
	- Ordre de les signatures.
	No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu.
	Aplicable en sistemes tancats de comunicació, si ho preveu així el conveni previst a l'article 20 de la Llei 11/2007.
	- Servidor segur.
	Aplicable en sistemes tancats de comunicació, si ho preveu així el conveni previst a l'article 20 de la Llei 11/2007.
	- Seu electrònica.
	No aplicable.
	- Segell electrònic.
	Aplicable.
	- Personal al servei de l'Administració.
	No aplicable.
6. Quins usos cal donar als certificats?	- Autenticació.
	No aplicable.
	- Signatura electrònica.
	Aplicable.
	- Xifratge.
	No aplicable.
7. Quines aplicacions específiques han de suportar els certificats?	- Signatura de documents.
	Aplicable, ja que el document corresponent a la transmissió de dades podrà ser un document de presentació, com ara un PDF.
	- Correu electrònic S/MIME.
	No aplicable.
	- Canal segur SSL/TLS.
	No aplicable.
	- Seguretat de serveis web.
	Aplicable, ja que la transmissió de dades es realitzarà típicament mitjançant serveis web automàtics.
	- Signatura de codi.
	No aplicable.
	- Signatura d'aplicació.
	No aplicable.
	- TSA, OCSP, altres.
	Aplicable, en la mesura que cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.

8. Quines estratègies de certificació digital cal establir?	- Emissió de certificats amb entitat de certificació pròpia. Aplicable. - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats). o Per a ús propi. Aplicable. o Per dotar terceres persones o entitats. No aplicable. - Admissió de certificats d'altres entitats de certificació. Aplicable a la recepció de transmissions de dades originades per altres administracions públiques.

5.5.11. La remissió automàtica de comunicació electrònica al ciutadà

1. Quin és el significat jurídic de la signatura?	- Descripció del tipus de significat. La signatura acredita la condició d'òrgan administratiu i garanteix la validesa del document. - Indicació de si la signatura és mancomunada, solidària, següent dins una seqüència o d'una altra mena. No aplicable.
2. Quina condició personal acredita la signatura?	- Autor o una altra condició (en substitució, per delegació o per un altre mecanisme). La signatura acredita la condició d'autor del document. - Actua en nom propi o en representació. L'òrgan actua en nom propi, exercint la competència pròpia.
3. Cal acreditar la data de la signatura independentment de la data del document?	- Sí/No. Sí, a causa de la rellevància i dels efectes externs del document.
4. La signatura s'ha de produir després d'una altra signatura?	- Sí/No. No. - Ordre de les signatures. No aplicable.
5. Quin tipus de certificats es necessiten?	- Dispositiu. No aplicable. - Servidor segur. No aplicable. - Seu electrònica. No aplicable. - Segell electrònic. Aplicable.

- Personal al servei de l'Administració.

  No aplicable.

6. Quins usos cal donar als certificats?
   - Autenticació.

     No aplicable.
   - Signatura electrònica.

     Aplicable.
   - Xifratge.

     No aplicable.
7. Quines aplicacions específiques han de suportar els certificats?
   - Signatura de documents.

     Aplicable, ja que el document corresponent a la comunicació serà, típicament, un document de presentació, com ara un PDF.
   - Correu electrònic S/MIME.

     Aplicable a comunicacions sense valor legal realitzades per correu electrònic.
   - Canal segur SSL/TLS.

     No aplicable.
   - Seguretat de serveis web.

     No aplicable.
   - Signatura de codi.

     No aplicable.
   - Signatura d'aplicació.

     No aplicable.
   - TSA, OCSP, altres.

     Aplicable, en la mesura que en alguns casos cal disposar de segell de data i hora, la qual cosa pot implicar la instal·lació d'una entitat de segellament de data i hora.
8. Quines estratègies de certificació digital cal establir?
   - Emissió de certificats amb entitat de certificació pròpia.

     Aplicable.
   - Emissió de certificats en col·laboració amb CATCert (adquisició de certificats).
     - Per a ús propi.

       Aplicable.
     - Per dotar terceres persones o entitats.

       No aplicable.
   - Admissió de certificats d'altres entitats de certificació.

     Aplicable en cas de rebre justificants de recepció produïts pels sistemes de lliurament de comunicacions electròniques.

6. ELS REQUISITS DE SEGURETAT DE L'APLICACIÓ D'ACTUACIÓ ADMINISTRATIVA AUTOMATITZADA

En aquesta secció es tracten els requisits de seguretat de l'aplicació d'actuació administrativa automatitzada, sobretot tenint en compte les necessitats de protecció d'una clau privada de segell d'acte automatitzat.

6.1. Les aplicacions informàtiques de signatura electrònica i els actius a protegir

En aquest primer apartat presentem els actius emprats per les aplicacions informàtiques de signatura electrònica. També hi tractem la problemàtica de seguretat, que motiva la necessitat d'emprar dispositius segurs de signatura electrònica dins el marc de la Directiva i la Llei de signatura electrònica, i d'acord amb els estàndards tècnics internacionals.

Presentarem, doncs:

- Els dispositius, en sentit ampli, d'ús de la signatura electrònica.
- Els algorismes criptogràfics relacionats amb la signatura electrònica.
- Les dades informàtiques relacionades amb la signatura electrònica.

6.1.1. *Els dispositius per a l'ús de la signatura electrònica*

6.1.1.1. El dispositiu de creació de signatura electrònica

Un dispositiu de creació de signatura electrònica és un programa o un sistema informàtic (un producte) que serveix per aplicar les dades de creació de signatura (de conformitat amb l'article 24.2 de la Llei 59/2003, de 19 de desembre, de signatura electrònica).

Aquesta definició connecta la creació de la signatura electrònica amb l'aplicació (l'ús) de les dades de creació de signatura, de manera que el posseïdor del dispositiu és la persona que pot crear la signatura, sigui o no el subscriptor del certificat.

Per aquest motiu, la signatura serà imputable al subscriptor en la mesura que una persona no autoritzada no pugui aplicar les dades de creació de signatura. Això justifica

la necessitat de disposar de les dades d'activació de la signatura electrònica per poder fer aquesta imputació.

D'altra banda, no forma part d'aquest dispositiu l'aplicació de creació de signatura, que, de fet, empra aquest dispositiu de creació en condicions de seguretat. Així, aquesta aplicació pot ser independent i única o bé un conjunt d'aplicacions, fins i tot distribuïdes, les quals, a més, poden fer servir protocols i interfícies de programació de serveis de seguretat de tercers, sempre sota la seva responsabilitat.

6.1.1.2. El dispositiu de verificació de signatura

Un dispositiu de verificació de signatura electrònica és, d'acord amb l'article 25.2 de la Llei 59/2003, un programa o un sistema informàtic que serveix per aplicar les dades de verificació de signatura.

Segons aquesta concepció, qualsevol posseïdor de la clau pública d'una persona la pot "aplicar" per comprovar la validesa de la signatura electrònica. Per tant, el legislador s'oblida d'altres elements que haurà d'aplicar aquesta persona per poder completar el procés de verificació, com ara la construcció d'una ruta de certificació fins a una arrel fiable, per comprovar la validesa del certificat que conté la clau pública, o la verificació de tots els certificats de la ruta.

Els dispositius de verificació de signatura han de garantir que el procediment de verificació compleix una sèrie de requisits generals sempre que això sigui *possible tècnicament*, un concepte jurídic indeterminat que cal resoldre amb les normes tècniques nacionals i internacionals aplicables, o, mancant aquestes, amb les especificacions tècniques voluntàries, com ara CEN CWA 14171, sobre procediments de verificació de signatura electrònica.

Des de la perspectiva de la comprovació dels requisits exposats anteriorment, els fabricants o els importadors poden utilitzar el mecanisme de la certificació de productes de signatura electrònica de l'article 27 de la Llei 59/2003.

6.1.2. *Els algorismes criptogràfics*

Els algorismes que tenen com a finalitat el tractament del secret de la informació s'anomenen *criptogràfics* i són essencials per a la signatura electrònica avançada, atès que suporten l'ús de xifres segures per a la producció i la comprovació de la signatura electrònica.

Un algorisme és una funció matemàtica executada per un producte informàtic, format habitualment per un maquinari i un programari.

En conseqüència, els algorismes criptogràfics rauen al cor de la signatura electrònica (avançada i reconeguda, però no necessàriament en el cas de la signatura ordinària).

6.1.2.1. Els algorismes de resum

L'algorisme de resum permet obtenir una versió reduïda d'un document que cal signar. Aquesta versió resumida es pot enviar juntament amb el document per tal de garantir que el document no ha estat manipulat (propietat que s'anomena *integritat documental electrònica*).

Aquest sistema s'aplica, en relació amb la signatura electrònica avançada, perquè les operacions executades amb algorismes de signatura són molt lentes i, addicionalment, incrementen de manera considerable el volum del document signat. Per evitar aquests inconvenients, el que realment se signa és aquest resum, i no el document sencer.

Hi ha també un gran nombre d'aplicacions que requereixen la integritat documental, però no la signatura electrònica, i, per tant, també utilitzen aquests algorismes de resum.

L'algorisme de resum ha de garantir una sèrie de condicions:

- Ha de ser irreversible, és a dir, no s'ha de poder obtenir el document original a partir del resum.

- Ha de ser únic per a cada document i infalsificable, és a dir, no han d'existir dos o més resums iguals per a documents diferents ni dos resums diferents per al mateix document.

Els dos algorismes de resum que es fan servir habitualment són MD5 i SHA-1, encara que ja s'han proposat substituts com RIPEMD-160 i SHA-224. En concret, MD5 ja ha estat declarat obsolet per a força aplicacions, incloent-hi la generació de resums per a signatures electròniques.

6.1.2.2. Els algorismes de signatura electrònica

L'algorisme de signatura electrònica es basa en una xifra asimètrica —és a dir, formada per una clau privada i una clau pública— que permet "signar" documents amb la clau privada i verificar la signatura amb la clau pública.

Criptogràficament, *signar* és generar una dada matemàtica associada al document electrònic, de la mateixa manera que, en el món físic, *signar* és produir un grafisme fixat al suport material que conté el document.

Aquesta signatura ofereix també la propietat anomenada *integritat documental electrònica*, que permet determinar que un document no ha estat manipulat, així com la propietat anomenada *autenticació*, que permet comprovar quina entitat ha originat el document.

La xifra utilitzada per l'algorisme de signatura s'anomena legalment *dada de signatura electrònica*. Concretament, la clau privada de signatura s'anomena *dada de creació de signatura electrònica*, mentre que la clau pública de signatura rep el nom de *dada de verificació de signatura electrònica*.

L'algorisme de signatura ha de garantir una sèrie de condicions:

- Ha de ser irreversible en un sentit doble: en primer lloc, no s'ha de poder obtenir la clau privada a partir de la clau pública; en segon lloc, no s'ha de poder obtenir la clau privada a partir de la signatura.

- Ha de ser única per a cada document i infalsificable, és a dir, no s'ha de poder obtenir una signatura idèntica a la del document original a partir d'una manipulació del document original.

Els dos algorismes de signatura electrònica que es fan servir habitualment són RSA i DSA.

A més, per obtenir la clau pública cal que aquesta clau hagi estat certificada per un prestador de serveis de certificació en qui es confiï.

Quan el certificat ha estat emès d'acord amb els requisits de la Llei 59/2003, de signatura electrònica, i la signatura ha estat produïda emprant un dispositiu segur de creació de signatura electrònica, aleshores la signatura permet fer la imputació legal del document electrònic al signatari identificat al certificat. Aquesta propietat s'anomena,

amb certa incorrecció, *no repudi d'origen* o *no rebuig d'origen*, termes que cal substituir per *irrefutabilitat d'origen*.

La suma de tots aquests factors es resumeix amb el concepte d'*autenticitat documental electrònica*, un element essencial dels serveis d'evidència electrònica.

6.1.3. *Les dades informàtiques relacionades amb la signatura electrònica*

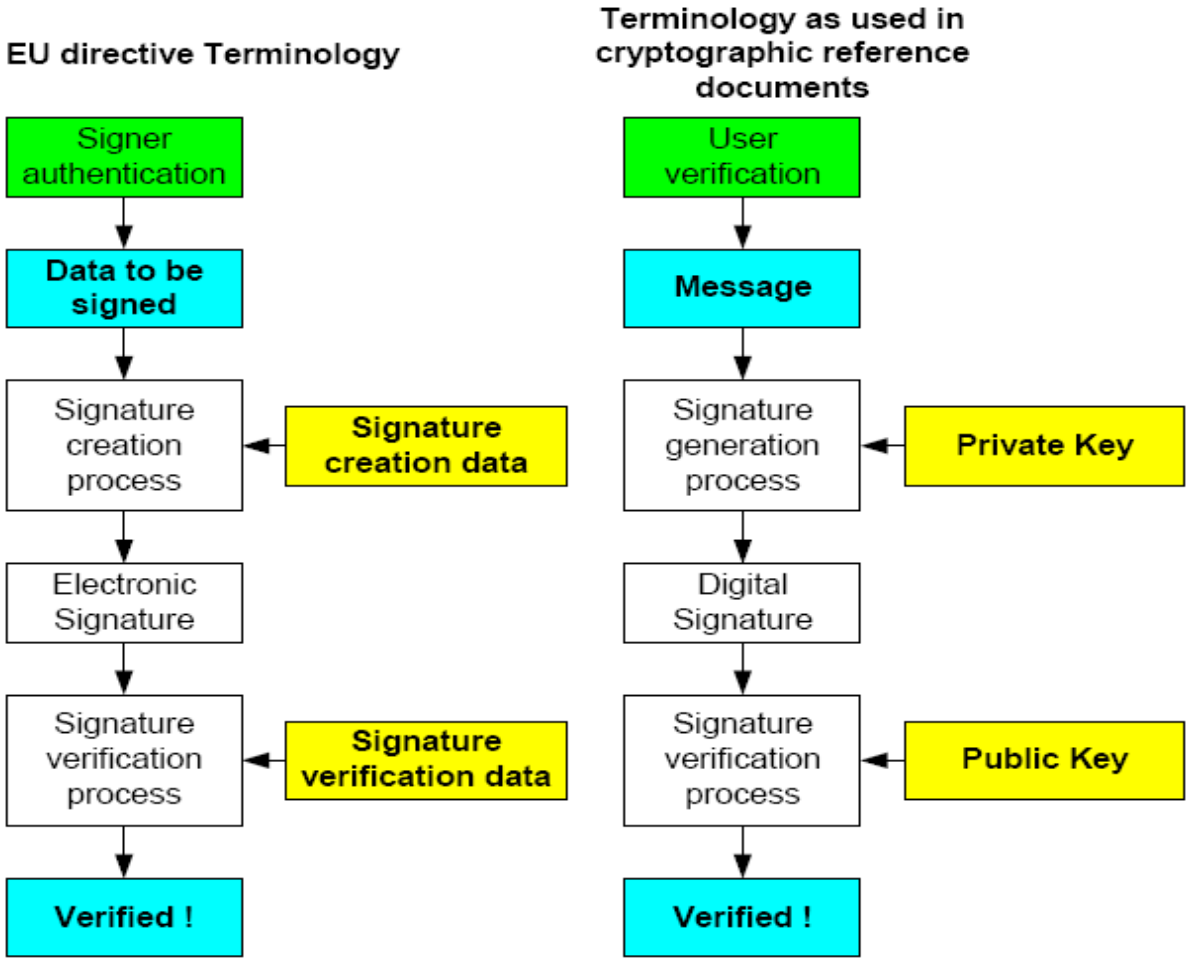
En aquest apartat presentem els conceptes legals relatius a les dades que cal emprar en els processos de generació i verificació de signatura.

Cal advertir que una de les dificultats amb què topem a l'hora de treballar amb els documents legals és la terminologia que utilitzen, molt diferent de la dels documents de caire més tècnic. Per exemple, mentre que legalment es parla de l'*autenticació del signatari*, des d'una perspectiva més tècnica es parla de la *verificació de l'usuari*. De manera semblant, mentre que legalment es parla del *document* o *missatge a signar*, tècnicament cal parlar de *dades a signar*, que és un conjunt de dades que inclou el document, però també altres informacions necessàries per a la signatura electrònica.

El mateix succeeix amb el concepte legal de *signatura electrònica avançada* (o *reconeguda*), que es correspon amb el concepte tècnic de *signatura digital*, de tal manera que una signatura digital és una signatura electrònica avançada, però també hi ha signatures electròniques que no són signatures digitals.

L'esquema següent[64] mostra les diferències terminològiques principals:

[64] CEN CWA 14890-1.



6.1.3.1. Les dades de creació i verificació de la signatura electrònica

Les dades de creació de signatura electrònica són, d'acord amb l'article 24.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, les dades úniques, com ara codis o claus criptogràfiques privades, que el signatari utilitza per crear la signatura electrònica.

Les dades de creació de signatura s'han de poder protegir contra la utilització indeguda per part de tercers, i sovint es generen dins un dispositiu segur de creació de signatura del qual no es poden extreure mai. Tampoc no poden ser copiades en cap altre lloc.

Per la seva banda, les dades de verificació de signatura electrònica són, de conformitat amb l'article 25.1, les dades —no es diu que hagin de ser úniques, però hem d'entendre la norma en aquest sentit— com ara codis o claus criptogràfiques públiques, que utilitzen

els tercers destinataris de comunicacions i documents signats per verificar la signatura electrònica.

La referència a codis o claus criptogràfiques —privades i públiques— es fa per preservar la suposada neutralitat tecnològica de la llei, tot i que podem dir que, en aquest punt, la normativa preveu clarament el cas de les xifres criptogràfiques asimètriques i els algorismes de signatura corresponents.

Aquestes claus criptogràfiques són els elements numèrics que formen una xifra criptogràfica. Funcionen conjuntament amb els algorismes criptogràfics per generar signatures electròniques i formes d'autenticació o bé per fer confidencial un document.

Per aquest motiu, les claus són els elements més importants i crítics dels sistemes de seguretat en general i dels sistemes de signatura en particular: conèixer la clau d'una persona implica adquirir la capacitat d'identificar-se o signar en nom seu, com també poder accedir a dades secretes.

Com hem vist, les claus criptogràfiques tenen la consideració legal de dades de creació i de verificació de signatura electrònica, d'acord amb els articles 24.1 i 25.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Consegüentment, el conjunt més important de mesures de seguretat en matèria de signatura electrònica té a veure amb la generació, la protecció i la gestió correctes de les claus privades, tant quan corresponen a xifres simètriques com quan corresponen a xifres asimètriques.

De manera coherent amb aquesta necessitat, la regulació més important en matèria dels dispositius que es consideren segurs per produir signatures electròniques gira al voltant de la gestió de les claus dels usuaris.

Una clau criptogràfica d'usuari és una dada numèrica que forma part d'una xifra i que ha de ser absolutament secreta, perquè serveix per autenticar-se, signar o accedir a dades confidencials.

En les xifres simètriques, com les que es fan servir per generar la signatura electrònica ordinària, només existeix una clau, que coneixen tant el signatari com el tercer que rep el document signat. En aquest cas, totes dues parts han de protegir el secret de la clau.

En les xifres asimètriques, com les que s'utilitzen per generar la signatura electrònica avançada o reconeguda, existeixen dues claus, de les quals una és privada i l'altra

pública. Les persones que signen ho fan amb la clau privada, mentre que els tercers que reben documents signats els verifiquen amb la clau pública, que no cal que sigui secreta.

De fet, la idea és que la clau sigui el màxim de pública possible, motiu pel qual es certifica la clau, en associació amb el seu titular, que posseeix la clau privada, perquè es pugui lliurar aquesta clau pública certificada a través de la xarxa Internet i que arribi a qualsevol potencial destinatari de documents signats.

Naturalment, aquestes claus estan correlacionades mitjançant un lligam matemàtic que permet utilitzar una clau per fer una acció (signar, per exemple) i l'altra clau per desfer-la (per tant, verificant la signatura). Com també és evident, sense aquest lligam, propi de les xifres asimètriques, el sistema no funcionaria.

El lligam, però, ha de permetre garantir la seguretat del sistema, de manera que el coneixement de la clau pública no representi una amenaça per a la clau privada (propietat sovint anomenada *irreversibilitat*).

Concretament, l'article 24.3 de la Llei 59/2003 determina que les claus criptogràfiques produïdes o emprades pels dispositius segurs de creació de signatura electrònica han de garantir, de forma raonablement segura, que no es podrà obtenir la clau privada a partir de la clau pública.

Així mateix, les claus criptogràfiques han de tenir una certa longitud per tal que siguin segures. Aquesta longitud, que és una propietat de la clau, consisteix en el límit superior de l'espai numèric de la xifra, i, per tant, determina el nombre de combinacions que hauria de provar un atacant que volgués endevinar la clau privada.

La longitud de la clau criptogràfica s'expressa en bits. Actualment es considera que una clau privada de signatura electrònica d'usuari de 1.024 bits ja és absolutament segura, mentre que la clau privada d'un prestador de serveis de certificació normalment té una longitud de 2.048 bits.

Atesa la seva importància, el titular de la clau criptogràfica privada ha de protegir aquesta clau convenientment mitjançant un producte de signatura electrònica que es consideri *segur*.

La mateixa definició de la signatura electrònica avançada fa referència a la protecció de la clau quan indica que aquesta ha estat creada per mitjans que el signatari pot mantenir sota el seu control exclusiu (article 3.2 de la Llei 59/2003), un dels aspectes més controvertits i complexos del sistema de signatura electrònica.

També s'hi refereix explícitament l'article 24.3 de la mateixa Llei, que estableix que el dispositiu segur de creació de signatura ha de permetre al signatari protegir les dades de creació de signatura electrònica d'una manera fiable per evitar que siguin utilitzades per tercers no autoritzats degudament.

6.1.3.2. Les dades d'activació de la signatura electrònica

Les dades d'activació de la creació de la signatura electrònica són les dades que s'empren per iniciar un procés de creació de signatura electrònica.

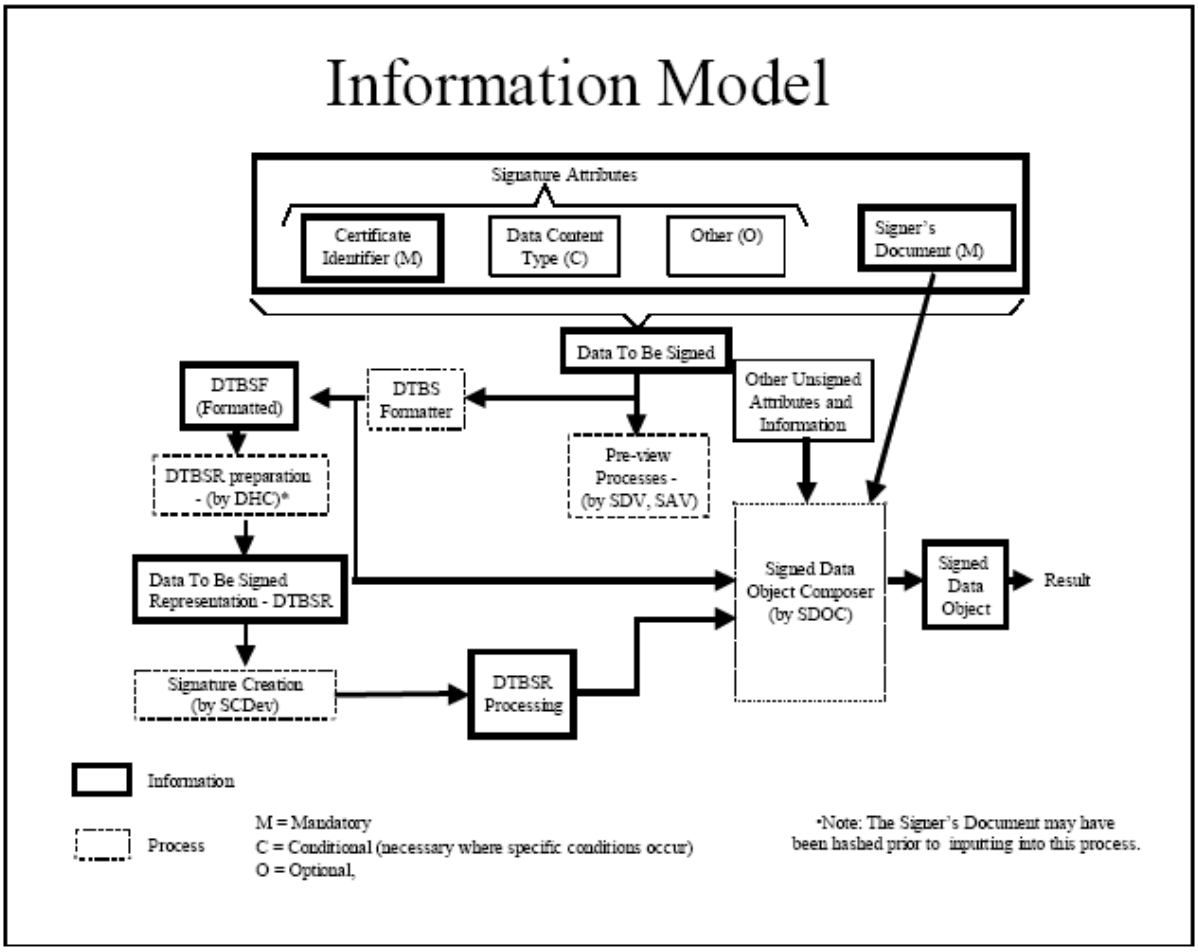
Encara que no apareixen definides a la Llei 59/2003, la seva existència i la seva necessitat connecten amb la protecció de les dades de creació de signatura electrònica, ja que amb les dades d'activació —conegudes únicament pel signatari o per les persones en qui aquest "delegui" la creació de la signatura— es pot accedir a les dades de creació de signatura i "activar" el procediment de generació de la signatura.

Precisament aquesta dada d'activació de la creació de la signatura electrònica és el mecanisme de protecció més habitual de les dades de creació de signatura electrònica que s'esmenta a l'article 24.3.c) de la Llei 59/2003.

Les dades d'activació són una dada alfabètica i numèrica que pot tenir una longitud variable i que hauria d'estar formada com a mínim per vuit caràcters, encara que moltes vegades coincideix amb un número d'identificació personal de quatre dígits.

6.1.4. *El model d'informació dels productes de signatura electrònica*

El gràfic següent il·lustra el model d'informació associat a la creació d'una signatura electrònica:



En aquest gràfic, els acrònims tenen els significats següents:

- DTBS (*Data To Be Signed*) significa les dades a signar, que resulten de formar un conjunt amb els elements següents:

    - El document a signar (*signer's document*), que és una dada que s'ha de fer constar obligatòriament.[65]

      Es pot tractar d'un document en format per a revisió, com ara un document d'un processador de textos, un missatge de correu electrònic o un fitxer, del qual es mostra una representació particular, depenent de les capacitats del dispositiu que el mostra, i, per tant, pot ser diferent de la representació que en veurà el verificador de la signatura.

[65] Lògicament, si no tenim document a signar difícilment podrem produir una signatura útil, ja que signarem la resta d'elements que realment són accessoris de la mateixa signatura.

També es pot trobar en format no modificable, com ara en un fitxer protegit (PDF, Postscript), i ser exposat en un sistema amb regles que mostren igual el document al signatari i al verificador.

En alguns casos, el document pot contenir informacions i dades que no resulten visibles al signatari, o fins i tot *codi maliciós*, informacions que poden generar dubtes sobre la signatura electrònica i que, en conseqüència, es tracten com amenaces a la seguretat.[66]

També es pot trobar en un format que visualitzen necessàriament de manera diferent el signatari i el verificador tot i representar la mateixa semàntica, com passa amb els fitxers EDI, HTML, XML, SGML i d'altres.

Finalment, el document pot contenir altres objectes de signatura electrònica creades per altres persones.

- El tipus de contingut de dades a signar (*data content type*), atribut que defineix el format del document a signar, i, per derivació, les normes per visualitzar-lo al signatari i al verificador de la signatura electrònica.

- La identificació del certificat de signatura electrònica (*certificate identifier*) amb què es podrà verificar aquesta signatura, que també és una dada que s'ha de fer constar de manera obligatòria.[67]

  Amb aquesta dada es pot determinar exactament el certificat que caldrà emprar per verificar la signatura electrònica, ja que un mateix signatari pot disposar de molts certificats diferents al mateix temps. També permet evitar els atacs de substitució de certificats de signatura electrònica per altres amb semàntica diferent.[68]

- Altres dades, opcionalment, com ara atribucions del signatari, o altres documents o informacions.

  Una d'aquestes dades addicionals opcionals és l'identificador de la política de signatura electrònica (*signature policy identifier*), que indica el conjunt de normes de seguretat aplicable a la creació i la verificació d'aquesta

[66] Això no vol dir que no sigui possible o legal signar aquests documents, sinó que caldrà provar que el signatari va conèixer efectivament el contingut perquè aquest el vinculi. Aquesta prova forma part de la pericial que caldrà practicar, hipotèticament, sobre el programari de creació de signatura i, en especial, sobre la seva interfície amb el signatari.

[67] Vegeu ETSI TS 101733, secció 8.8.1.

[68] En aquest cas, es tracta de la modificació de dades del certificat, respectant-ne la clau pública.

signatura, així com del seu significat jurídic, de manera independent del context de la signatura.

Una altra d'aquestes dades és l'identificador del tipus de compromís de signatura (*commitment type*), que indica, de forma expressa, el significat jurídic —o d'un altre tipus— de la signatura electrònica. Quan una política de signatura electrònica conté diversos tipus de compromisos, aquesta dada possibilita conèixer el tipus concret de compromís d'acord amb el qual ha estat emesa aquesta signatura.

Finalment, les dades a signar es poden referir a rols, permisos, poders, segells de temps i altres informacions.

- DTBSF (*Data To Be Signed Formatted*) significa les dades a signar que ja han rebut el format necessari previ a la generació del resum criptogràfic mitjançant el procés de format corresponent.

  Aquest procés resulta necessari per garantir que les dades es troben en l'ordre correcte, d'acord amb una estructura concreta de signatura electrònica, com ara el format SignedData definit per PKCS#7, CMS, XMLDSig o XAdES.

- DTBSR (*Data To Be Signed Representation*) significa la representació matemàtica de les dades a signar formatades, és a dir, el resum criptogràfic de les dades a signar que s'emprarà per a la creació de la signatura electrònica.

- SDO (*Signed Data Object*) significa l'objecte de dades signades, que és el resultat, ja tractat, del procés de signatura.

  L'objecte de dades signades es troba en el mateix format que el DTBSF. Incorpora al seu interior la signatura digital produïda a partir de la DTBSR, com també altres dades i informacions que no han estat objecte de signatura.

6.1.5. *El dispositiu segur de creació de signatura electrònica*

6.1.5.1. La definició del dispositiu segur de creació de signatura electrònica

Un dispositiu segur de creació de signatura electrònica és un dispositiu que, d'acord amb l'article 24.3 de la Llei 59/2003, compleix els requisits següents:

- Les dades utilitzades per a la generació de la signatura electrònica (és a dir, la clau privada) es poden produir només una vegada. El dispositiu n'assegura raonablement el secret.

- Existeix una seguretat raonable del fet que les dades utilitzades per generar la signatura electrònica no poden derivar de les dades de verificació de signatura (propietat d'irreversibles) o de la mateixa signatura i del fet que la signatura està protegida contra la falsificació amb la tecnologia existent en cada moment (longitud de claus).

- Les dades de creació de la signatura electrònica poden ser protegides de forma fiable pel signatari contra la seva utilització per tercers (dades d'activació de la creació de signatura).

- El dispositiu no altera les dades o el document que s'ha de signar ni impedeix que aquest es mostri al signatari abans del procés de signatura.

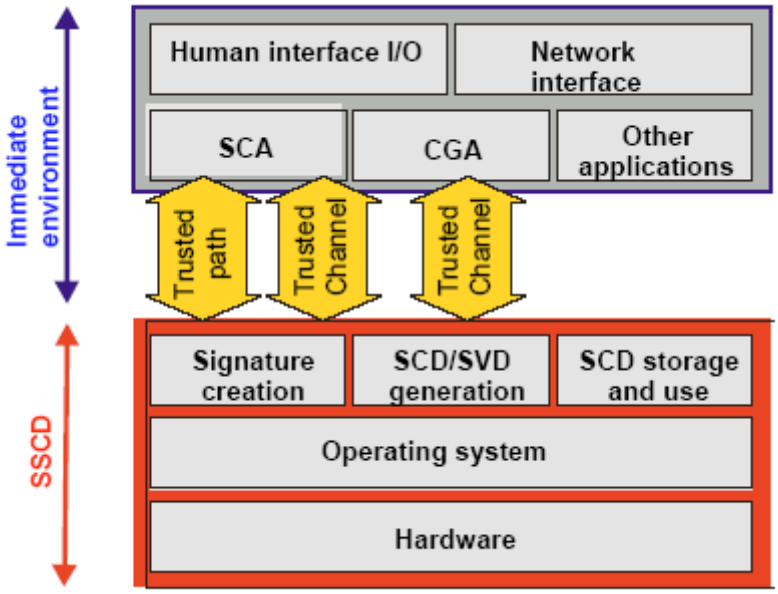
El dispositiu segur és un dels elements requerits per obtenir una signatura electrònica reconeguda, directament equivalent a la signatura escrita, malgrat que les signatures electròniques produïdes amb dispositius que no gaudeixen d'aquesta consideració també poden tenir efectes, especialment mitjançant un pacte entre les parts o una norma administrativa.

La major part de les normes administratives actuals fan una interpretació molt flexible del concepte, de tal manera que el programari de signatura electrònica d'ús ampli, com el que inclouen els sistemes operatius més utilitzats, es considera dispositiu segur de creació de signatura electrònica.

Davant aquesta postura, les normes europees contenen una interpretació més estricta del concepte, que habitualment connecta amb l'ús d'un element de maquinari o *hardware* —com ara una targeta criptogràfica o un element similar— per poder considerar que el sistema de creació de signatura electrònica és un dispositiu segur.

Concretament, CEN CWA 14169[69] ofereix un perfil de protecció, escrit d'acord amb la norma ISO 15408: Common Criteria, que determina criteris comuns per avaluar la seguretat de la informació per a dispositius segurs de creació de signatura electrònica (representats pel TOE, *target of evaluation*), amb l'estructura següent:

[69] Es tracta d'un perfil de protecció molt adient per a targetes, tot i que, amb algunes adaptacions, també es pot fer servir per a altres tipus de maquinari.



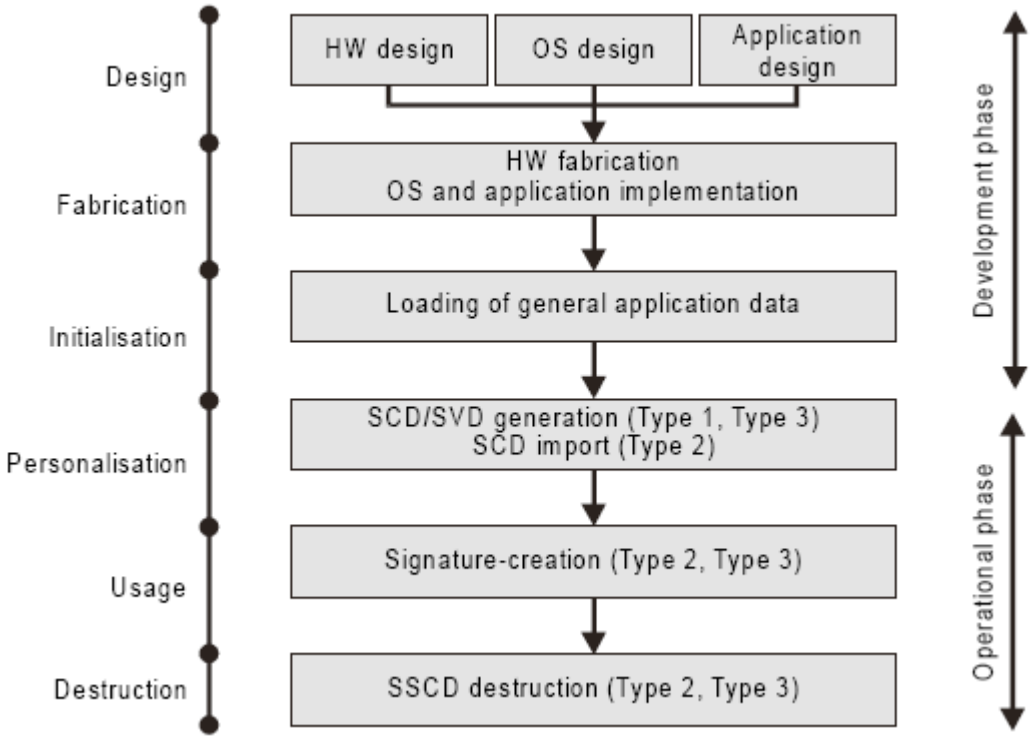
En aquest gràfic, cal remarcar la diferència entre l'SSCD, que és el dispositiu segur —i l'objecte de les mesures de seguretat a implantar— i el seu entorn immediat (*immediate environment*), que pot ser l'ordinador personal de l'usuari, i amb el qual és necessari que el dispositiu es relacioni de manera fiable.

Així doncs, podem veure que entre el procés de creació de signatura i l'aplicació de creació de signatura (SCA, acrònim de *signature creation application*) existeix una ruta fiable (*trusted path*) per obtenir les dades d'autenticació de l'usuari i confirmar la seva voluntat,[70] així com un canal fiable (*trusted channel*) per transmetre les dades per a la generació de la signatura a l'SSCD, com ara la representació de les dades a signar (DTBSR, per exemple, el *hash* del document).

Quan l'SSCD té la capacitat de generar claus de signatura (amb el procés *SCD/SVD generation*), aleshores també és necessari disposar d'un canal fiable amb l'entitat de certificació (CGA, acrònim de *certificate generation application*) per garantir que els processos per sol·licitar i obtenir certificats són fiables.

Tot i aquesta visió estructural de l'SSCD, cal considerar les mesures de seguretat des d'una perspectiva de cicle de vida del dispositiu que ha de preveure els processos següents:

[70] Excepte quan l'SSCD aporta ell mateix la interfície amb l'usuari; en aquest cas, ja es defineixen mesures de seguretat específiques per a aquesta funció dins el TOE.



Les amenaces contra el dispositiu identificades per l'especificació tècnica CEN CWA 14169, per a les quals es determinen mesures de seguretat, són les següents:

- Atacs físics a l'SSCD mitjançant les seves interfícies.
- Divulgació de les dades de creació de signatura mitjançant l'emmagatzematge o la còpia d'aquestes dades fora del dispositiu.
- Derivació de les dades de creació de signatura a partir de dades públiques, com les dades de verificació de signatura o signatures electròniques generades amb aquestes dades de creació.
- Falsificació de la signatura electrònica.
- Refutació de la signatura electrònica.
- Falsificació de les dades de verificació de signatura electrònica.
- Falsificació de la representació de les dades a signar.
- Mal ús de la funció de creació de signatura amb vista a crear signatures sense el coneixement del signatari.

A més, com veurem posteriorment, respecte a les mesures de seguretat de l'entorn immediat de l'SSCD, l'especificació tècnica CEN CWA 14170 ofereix un conjunt de mesures de seguretat funcional aplicables al programari que funciona conjuntament amb dispositius segurs de creació de signatura electrònica (aplicacions de signatura

electrònica) per tal de garantir un nivell apropiat de seguretat, en desplegament de la Directiva 99/93/CE.

La qüestió de la fiabilitat de l'aplicació de signatura electrònica és essencial, ja que l'SSCD confia absolutament en les dades que provenen dels canals de comunicació autèntics de l'aplicació.

6.1.5.2. L'acreditació de la qualitat de dispositiu segur

Des de la perspectiva de la comprovació dels requisits exposats anteriorment, els fabricants o els importadors poden fer servir el mecanisme de la certificació de productes de signatura electrònica de l'article 27 de la Llei 59/2003.

En relació amb aquest mecanisme de certificació dels dispositius segurs de creació de signatura electrònica, cal considerar les opcions següents:

- Qualsevol producte de signatura electrònica certificat a qualsevol estat amb un esquema nacional d'avaluació i certificació de la seguretat de les tecnologies de la informació, sempre que el certificat de seguretat s'hagi fet emprant CC (*common criteria*) i un objectiu de seguretat que declari adherència al perfil de protecció CEN CWA 14169 (EAL4+) per a dispositius de creació de signatura de tipus 3.

  La llista de productes avaluats es pot consultar a l'adreça web següent: http://www.commoncriteriaportal.org/public/expert/index.php?menu=9

- Com a segona opció, es pot acceptar un producte certificat d'acord amb CC (*common criteria*) amb adherència a un altre perfil de protecció, o sense adherència a cap perfil concret, sempre que de l'anàlisi del seu objectiu de seguretat es desprengui un nivell de seguretat equivalent.

- Com a tercera opció, es pot acceptar un producte certificat amb adherència a un perfil de protecció (o document equivalent) d'un esquema d'avaluació i certificació de la seguretat de les tecnologies de la informació diferent de CC (*common criteria*), sempre que de l'anàlisi corresponent del perfil de protecció o document equivalent es desprengui un nivell de seguretat equivalent i que la metodologia d'avaluació ofereixi un nivell de rigor avaluador equivalent.

Molts experts consideren que solament un programari no pot ser de cap manera un dispositiu segur de creació de signatura electrònica, i, per tant, que és imprescindible una targeta o equivalent per obtenir la signatura electrònica reconeguda d'acord amb la Llei 59/2003, de 19 de desembre.

En aquest sentit, l'ús de mòduls criptogràfics basats en programari, encara que siguin programats de forma força segura, tenen la problemàtica d'haver de funcionar en sistemes que no resulten fiables en si, com passa amb els sistemes operatius, que funcionen en plataformes a les quals accedeixen moltes persones, sovint amb capacitat d'instal·lar moltes aplicacions, de fonts no controlades, i que poden rebre molts atacs de seguretat, directament o a través de les connexions a Internet.[71]

Això implica la possibilitat que una aplicació fraudulenta pugui actuar fins i tot en contra del mòdul criptogràfic basat en programari,[72] o bé modificar o substituir aquest mòdul criptogràfic.[73]

Potser és per aquest motiu que, fins avui, els únics dispositius segurs de creació de signatura electrònica que han obtingut la certificació de seguretat a l'efecte de la Llei de signatura electrònica es basen en maquinari. En particular, els més emprats són targetes (tradicionals o USB) amb xip criptogràfic, tot i que ja s'han començat a avaluar altres productes de maquinari, sobretot maquinari de signatura centralitzada.

Des de la perspectiva del programador d'aplicacions de creació de signatura electrònica, aquesta problemàtica queda suposadament resolta pel dispositiu —i el programari— corresponent que subministra el fabricant o l'importador o, quan s'escaigui, el prestador de serveis de certificació, com en el cas de CATCert quan subministra la targeta, atès que amb la seva garantia jurídica en té prou per confiar-hi.

Tot i això, és important entendre l'arquitectura de forma global, ja que quedarà sota la responsabilitat del programador d'aplicacions de creació de signatura emprar correctament els mecanismes de comunicació segura entre el signatari i el dispositiu segur, així com altres parts importants del procés de creació de signatura.

De fet, tot el que no és el dispositiu segur de creació de signatura i la seva interfície immediata es considera *aplicació de creació de signatura electrònica* i queda sota la responsabilitat del seu programador, que haurà d'assegurar l'aplicació esmentada davant potencials atacs de tercers.

---

[71] Per exemple, per virus o programari espia (*spyware*).

[72] Mitjançant un *bypass*.

[73] Mitjançant una aplicació que imiti el comportament del mòdul criptogràfic, per exemple, o un virus troià que modifiqui el codi del mòdul.

6.1.6. *L'arquitectura de programació de criptografia dels sistemes operatius*

La complexitat dels sistemes criptogràfics exigeix aprofundir una mica en el model d'implantació de l'arquitectura de programació de criptografia als sistemes operatius, en què cal distingir els nivells o les capes següents:

- La capa d'interfície de serveis criptogràfics amb el dispositiu.
- La capa d'interfície de programació de serveis criptogràfics.
- La capa de serveis criptogràfics en entorns d'execució virtual.
- La capa d'interfície de programació de serveis de seguretat.

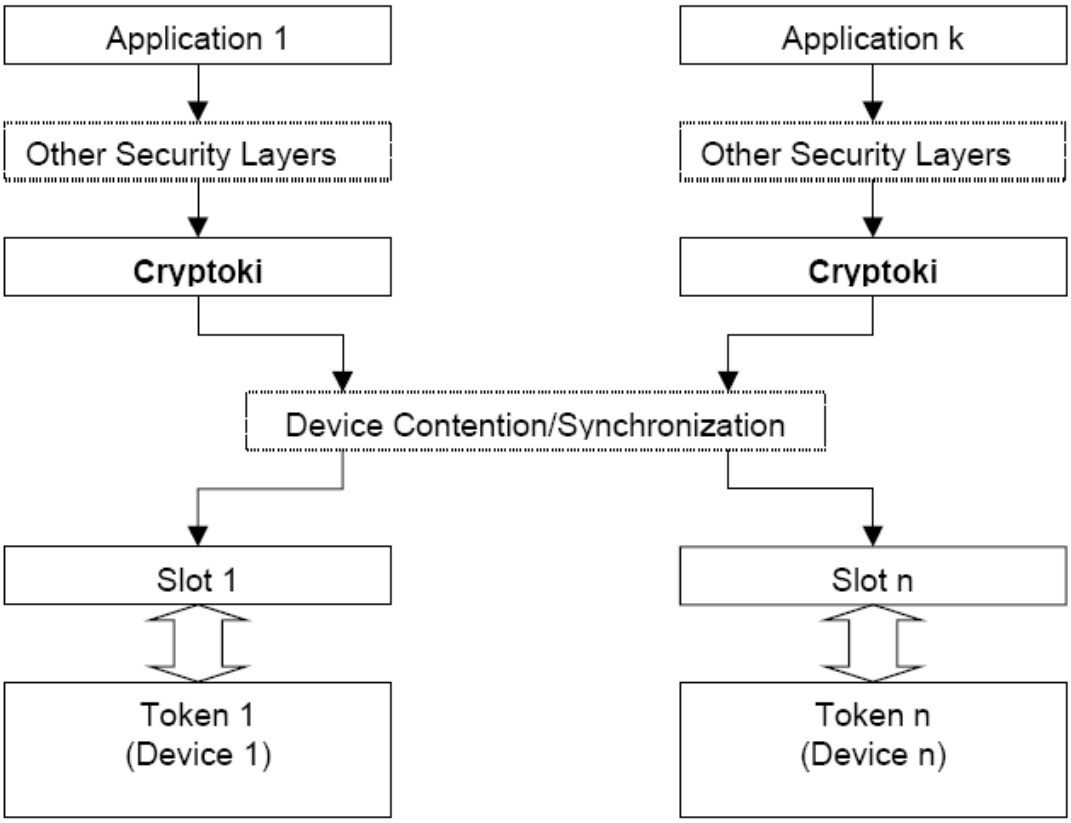
La capa d'interfície de serveis criptogràfics amb el dispositiu

A la complexitat de la separació entre el sistema del dispositiu —eventualment segur— de creació de signatura i l'aplicació, s'hi afegeix el fet que aquest dispositiu de creació de signatura es relaciona amb el sistema operatiu sobre el qual treballen les aplicacions de signatura electrònica mitjançant una o diverses interfícies de servei, més o menys estàndards, amb la finalitat que el programador de l'aplicació de creació de signatura pugui interactuar amb el dispositiu.

Moltes vegades aquestes interfícies de servei s'anomenen *mòduls* o *proveïdors de serveis criptogràfics*. Les subministra el proveïdor del dispositiu en circuit integrat i representen la capa inferior del sistema de programació de funcions criptogràfiques.

Aquests mòduls són els responsables inicials de les operacions criptogràfiques i de gestió de claus, i s'utilitzen mitjançant interfícies de programació de serveis criptogràfics, que veurem tot seguit.

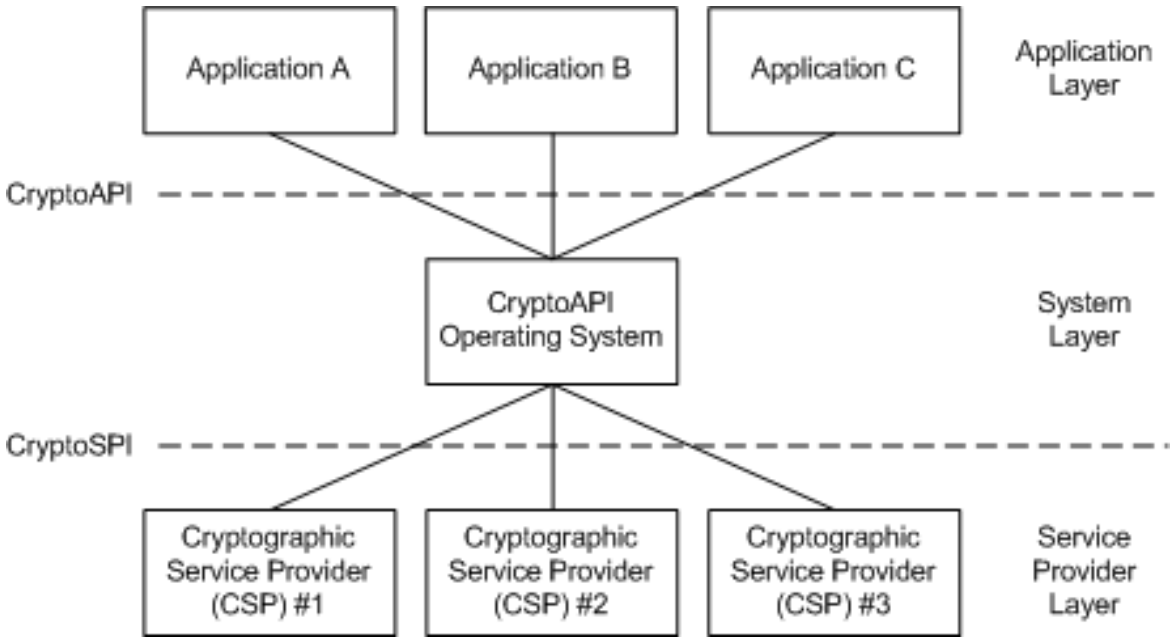
En general, per a qualsevol sistema operatiu es pot emprar Criptoki (PKCS#11) per definir una interfície de serveis criptogràfics abstracta, vàlida per a qualsevol tipus d'element (anomenat *token* en anglès) de seguretat, incloent-hi targetes i altres dispositius segurs de creació de signatura. La il·lustració següent mostra l'arquitectura de Criptoki:



En el cas del sistema operatiu Microsoft Windows, el proveïdor de serveis criptogràfics adopta obligatòriament la forma d'una biblioteca d'enllaços dinàmics (DLL, *dynamic link library*) que implanta les funcions criptogràfiques de CryptoSPI, la interfície de serveis criptogràfics de l'arquitectura de seguretat de Microsoft, a les quals s'accedeix amb la interfície de programació CryptoAPI.

Com a mesura de seguretat, cada CSP s'ha de signar abans per poder ser emprat amb la versió de distribució del sistema operatiu Windows.

La il·lustració següent mostra l'arquitectura de la família de sistemes operatius Microsoft Windows:



Cal dir que habitualment tots els proveïdors de dispositius de signatura electrònica (per exemple, targetes) subministren biblioteques d'enllaços dinàmics DLL per accedir amb totes dues interfícies de servei, cosa que permet emprar diferents interfícies de programació criptogràfica.[74]

La capa d'interfície de programació de serveis criptogràfics

Per sobre dels mòduls criptogràfics, trobem la interfície de programació de serveis criptogràfics. Té com a objectiu facilitar la programació de les aplicacions segures de signatura electrònica, tot embolcallant les crides a les funcions de serveis criptogràfics ofertes pels mòduls criptogràfics que hem vist anteriorment.

Aquestes API permeten separar les aplicacions (com el correu electrònic segur, incloent-hi els paquets de seguretat i les interfícies de programació de serveis de seguretat que empren) de la criptografia. Les interfícies de programació de serveis criptogràfics més utilitzades són les següents:

[74] Tot i que no és gaire freqüent fer-ho, res no impedeix programar una aplicació amb CryptoAPI que accedeixi a un mòdul que exposa una interfície PKCS#11 mitjançant una traducció (manual) de les funcions de programació de CryptoAPI a les funcions de servei de criptografia d'un mòdul PKCS#11, feina que no caldrà dur a terme si l'accés al mòdul es fa mitjançant el CSP corresponent subministrat pel mateix fabricant del dispositiu.

- API d'accés a proveïdors de serveis o mòduls criptogràfics RSA Criptoki (PKCS#11, l'estàndard més independent de sistemes operatius).

  Els projectes basats en programari lliure Mozilla, com el client web Firefox o el client de correu electrònic Thunderbird, per exemple, han adoptat PKCS#11 com a tecnologia de seguretat criptogràfica de base. Els usuaris poden accedir a la seva targeta mitjançant el mòdul criptogràfic corresponent. En cas que no disposin de targeta, poden emprar diferents *tokens* basats en programari, com ara el *softoken* subministrat amb la llicència de Mozilla o com un objecte PSS de Safelayer amb emmagatzematge a l'ordinador personal o en un altre dispositiu només d'emmagatzematge, com una clau USB no criptogràfica o un disc flexible,[75] per exemple.

- API d'accés a proveïdors de serveis o mòduls criptogràfics de Microsoft (CSP) mitjançant CryptoAPI, que és la interfície de programació d'aplicacions que se subministra[76] amb el sistema operatiu Microsoft Windows, i, en un nivell més baix, mitjançant les funcions genèriques de CryptoSPI.[77]

  Microsoft ofereix també el component client CAPICOM per facilitar el desenvolupament ràpid d'aplicacions de signatura electrònica, amagant les complexitats de CryptoAPI en un objecte dinàmic al qual fer les crides de serveis pertinents.

Com que CryptoAPI només funciona en plataformes Windows, una aplicació que hagi de funcionar en diferents plataformes (incloent-hi Linux, per exemple) probablement serà programada emprant Criptoki (PKCS#11), sense emprar CryptoAPI, per aprofitar la màxima part de codi possible, amb el corresponent estalvi de cost i de temps. Una altra opció consisteix a emprar una interfície més abstracta que després pugui traduir els comandaments d'aquesta interfície (signar, xifrar...) als corresponents de PKCS#11 o CryptoAPI, com veurem a continuació.

[75] Cal advertir del risc de seguretat que suposa la confusió entre els dispositius (siguin targetes tradicionals o en suport USB) que només emmagatzemen i els que realment fan les operacions criptogràfiques al dispositiu: mentre que en el primer cas les claus privades surten del dispositiu cada vegada que s'han d'utilitzar —ja que les operacions es fan a la memòria de l'ordinador—, en el segon cas les claus mai no abandonen el dispositiu, característica essencial per poder qualificar de segur el dispositiu de creació de signatura.

[76] Mitjançant les biblioteques del sistema Advapi32.dll and Crypt32.dll.

[77] *Cryptographic service provider interface*.

La capa de serveis criptogràfics en entorns d'execució virtual

Els darrers anys han empès la indústria a la creació d'entorns d'execució virtual, com Java o .NET, per donar resposta a una sèrie de necessitats cada vegada més importants. Entre aquestes necessitats podem esmentar la portabilitat del codi, la programació a múltiples entorns i plataformes i amb múltiples llenguatges, la seguretat de l'execució de codi i la necessitat d'operar en entorns web altament distribuïts.

Un entorn d'execució virtual és un sistema que controla l'execució de codi intermedi[78] que s'avalua i s'executa (quan s'escau, amb compilació sota demanda), amb independència del seu lloc de "residència", amb polítiques estrictes de contenció i accés a codi i a dades.

En aquests entorns l'accés directe al sistema està absolutament restringit als processos ordinaris,[79] per motius inherents a la definició arquitectònica d'aquests processos, i resulta necessari disposar de classes, mètodes i interfícies abstractes i independents per accedir a les interfícies del sistema —que hem presentat anteriorment.

Sovint aquestes classes s'anomenen *codi gestionat* per l'entorn d'execució virtual o, més explícitament, per la màquina virtual.

A més, habitualment aquests entorns ofereixen propietats de seguretat importants, entre les quals en podem esmentar una de molt important, com és la impossibilitat d'accedir una aplicació a l'espai de memòria d'una altra aplicació de manera directa. Aquest fet facilita la protecció de les informacions sensibles emmagatzemades en memòria, com ara una contrasenya d'usuari.

Algunes d'aquestes classes, mètodes i interfícies actuen com "embolcalls" de proveïdors de serveis de criptografia (*wrappers*), tot i que normalment reben també la denominació, més freqüent, de *proveïdors criptogràfics*, que no hem de confondre amb els esmentats anteriorment, que realment ho són en sentit estricte.

La diferència entre ambdós rau en el fet que l'existència d'una classe Java o .NET que embolcalla les funcions d'un proveïdor criptogràfic no garanteix que realment existeixi, a la plataforma en què finalment s'executa el codi, el CSP o mòdul PKCS#11 necessari: es tracta d'una representació més aviat abstracta d'aquesta possibilitat per poder tenir accés des de la màquina virtual.

[78] Un tipus de *bytecode*, com ara Microsoft Intermediate Language (MSIL).

[79] Tot i això, explícitament es pot executar codi "insegur", que accedeix al sistema, com ara amb JNI a Java o amb *unsafe* o *P/Invoque* a .NET; aleshores és responsabilitat del programador assegurar-se d'aplicar controls molt estrictes al resultat d'aquestes crides "insegures".

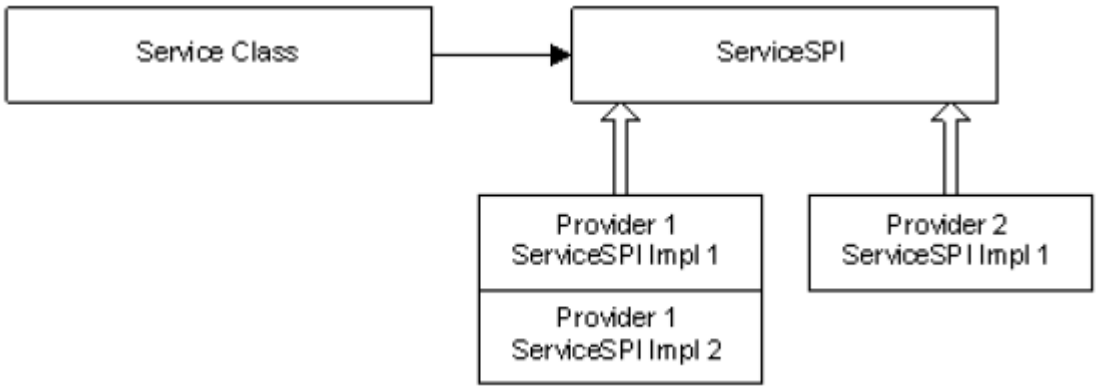
Els entorns basats en màquina virtual que podem comentar són dos:

- Java Cryptography Architecture (JCA) / Java Cryptography Extension (JCE). Inicialment estaven separats a causa de restriccions legals d'exportació, però a partir de la versió 1.4 del Java Development Kit han esdevingut un únic sistema, ja que JCE ha estat integrat com a component intern de la plataforma Java, en lloc de mantenir-se com a paquet opcional.

  JCA i JCE disposen d'una arquitectura basada en proveïdors, molt emprada en les solucions basades en la plataforma Java. Aquests paquets consisteixen en els anomenats *marcs de treball* (*frameworks*), que implanten la infraestructura requerida, i un nombre de proveïdors addicionals, que subministren els algorismes criptogràfics. Normalment aquests proveïdors són embolcalls criptogràfics (*wrappers*) d'objectes PKCS#11, la qual cosa permet la comunicació amb les capes inferiors del sistema fins a arribar, quan s'escaigui, al dispositiu de signatura electrònica.

  Els marcs de treball JCA i JCE són paquets interns de Java i, per tant, no es poden reemplaçar ni esquivar. Com a exemple, el marc de treball JCE autentica els proveïdors JCE mitjançant la seva signatura[80] per una entitat de certificació fiable (SUN o IBM).

  La figura següent il·lustra, de forma simple, el model de classes del marc de treball del proveïdor JCA:



- Microsoft .NET, que es basa, sobretot, en Microsoft CryptoAPI, el qual ja hem comentat anteriorment. Molts algorismes criptogràfics s'implanten en forma

[80] Una possibilitat per als venedors independents d'interfícies criptogràfiques és no emprar el marc de treball JCE i instal·lar-ne un de propi.

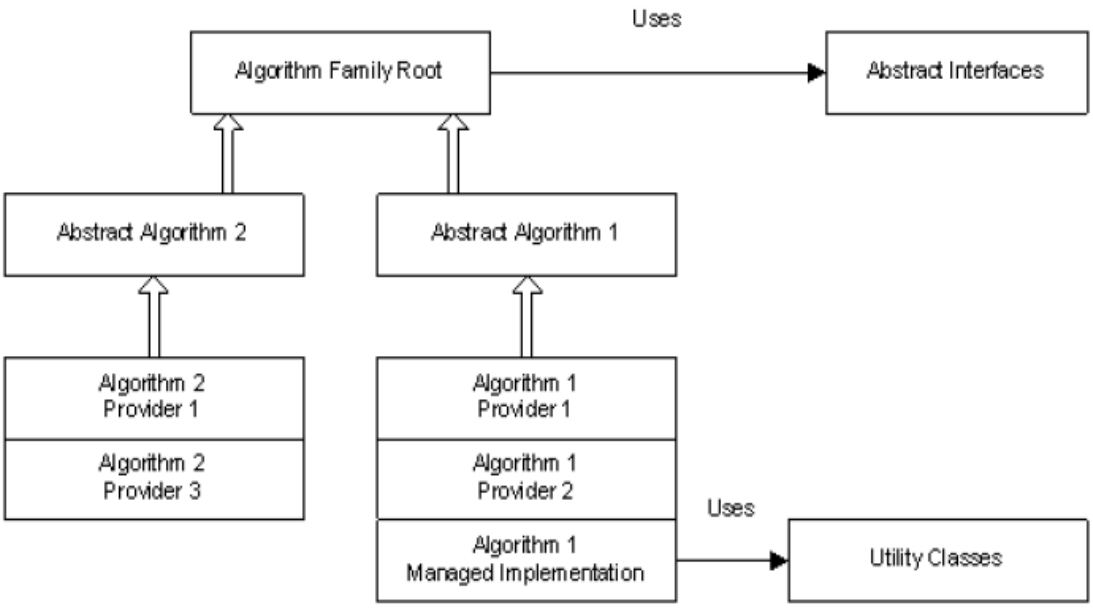
d'embolcalls gestionats per sobre de CryptoAPI, i el sistema de gestió de claus es basa també en els contenidors de claus dels CSP.

El model criptogràfic de .NET, que es conté a l'espai de nom System.Security.Cryptography, s'organitza horitzontalment en forma de capes, i verticalment en forma d'agrupacions de tipus. Cada família d'algorismes (simètrics, asimètrics...) integra una agrupació vertical, jeràrquica, que deriva d'una classe única arrel de la família, amb dues capes per sota: una representació abstracta de l'algorisme i la seva implantació concreta.

Una característica important de les classes arrel familiars és que estan protegides, de manera que les aplicacions no en poden produir extensions. Això vol dir que la classe arrel de la família d'algorismes asimètrics no permet fer extensions més enllà de les abstraccions de RSA i DSA que subministra el sistema.

Per convenció de .NET, la classe d'implantació s'anomena *proveïdora* (*provider*) quan és un embolcall d'un objecte CryptoAPI, i *gestionada* (*managed*) quan és una implantació totalment nova.

La figura següent il·lustra, de forma simple, la jerarquia de classes criptogràfiques de .NET:



La capa d'interfície de programació de serveis de seguretat

Per sobre de les interfícies de programació de serveis criptogràfics encara podem trobar, opcionalment, una capa addicional formada per les categories d'elements següents:

- Paquets de seguretat que implanten protocols orientats a aplicacions, els quals fan més simple la programació criptogràfica per a aquelles aplicacions. Alguns exemples dels nombrosos paquets de seguretat que hi ha són:

    - S/MIME i PGP/MIME, orientat al correu electrònic segur i a la signatura de fitxers.

    - Netscape SSL —i les seves evolucions TLS i WTLS—, orientat als intercanvis segurs, íntegres i confidencials, d'informacions per Internet mitjançant HTTP.

- Interfícies de programació de serveis de seguretat, que embolcallen i fan ús de funcionalitats de criptografia de forma estàndard i abstracta. Podem citar, entre d'altres, els següents:

    - IETF GSS-API és una interfície genèrica d'alt nivell de serveis de seguretat promoguda des del grup Common Authentication Technology (CAT) de l'IETF, l'organisme que impulsa els estàndards d'Internet. Disposa d'un conjunt d'extensions per a la protecció d'unitats de dades independents (IDUP-GSS-API).

      GSS-API es va dissenyar per protegir comunicacions amb control de sessió, com ara File Transfer Protocol (FTP) entre entitats. IDUP-GSS-API, per la seva banda, no assumeix comunicacions en temps real entre l'emissor i el receptor de la comunicació, sinó que protegeix cada unitat de dades, sigui un fitxer o un missatge, de manera independent de la resta. Per tant, resulta adequat per protegir dades en aplicacions de missatgeria i és capaç de gestionar objectes de signatura electrònica amb valor evidencial.

    - Microsoft SSPI és una interfície genèrica de serveis de seguretat promoguda per Microsoft, de forma paral·lela a GSS-API, que ofereix autenticació mútua entre entitats, així com autenticació i confidencialitat de missatges. Atesa la seva orientació a connexions, és la base dels protocols de "canal segur" de Microsoft.

- Open Group CSSM-API és una interfície de gestió de serveis de seguretat que forma part de la iniciativa d'arquitectura comuna de seguretat de dades (CDSA).

  CSSM-API ofereix un conjunt força important de serveis de seguretat, com ara criptografia, gestió de certificats, polítiques de confiança, emmagatzematge de dades o recuperació de claus.

6.2. La seguretat en l'aplicació de creació de la signatura electrònica

A l'apartat anterior hem vist que és responsabilitat del programador d'aplicacions la problemàtica de la seguretat en el procés de creació de signatura extern al dispositiu segur (que té no poca complexitat), i, en especial, la delicada situació de relacionar-se amb el signatari d'una manera fiable i fer d'intermediari entre aquest signatari i el seu dispositiu de signatura.

Els principals reptes de seguretat que han de resoldre les aplicacions de signatura electrònica són els següents:[81]

- Comunicació segura entre l'aplicació de creació de signatura electrònica i el dispositiu segur corresponent, incloent-hi:

  - Identificació de l'aplicació de creació de signatura i dispositiu —segur— de creació de signatura, necessària per a l'establiment del canal fiable.[82]

  - Creació i manteniment d'una ruta fiable que permeti a l'aplicació mostrar les dades a signar i obtenir el consentiment de l'usuari quan aquesta funcionalitat no l'ofereixi directament la interfície del dispositiu segur de creació de signatura.[83]

  - Creació i manteniment d'un canal fiable per comunicar els comandaments al dispositiu, com també la representació de les dades a signar entre l'aplicació de creació de signatura i el dispositiu —segur— de creació de

[81] CEN CWA 14355.

[82] Així com per evitar que falses aplicacions puguin aconseguir signatures mitjançant usos fraudulents.

[83] Per exemple, mitjançant la funcionalitat *card holder verification* (CHV).

signatura, incloent-hi la selecció de les dades de creació de signatura i la comunicació del consentiment al dispositiu.[84]

- Gestió de la seguretat de les dades relatives a la signatura, especialment en relació amb la ratificació del consentiment del signatari pel dispositiu mitjançant un procés d'acceptació de l'acció de signar que garanteixi que la persona ha entès les conseqüències de l'acte de signatura, que resulta coherent amb la política de seguretat del dispositiu.

- Tractament segur del procés d'usuari previ i posterior a la creació de la signatura electrònica, així com de la interfície amb el signatari.

L'acord del grup de treball de signatura electrònica del Comitè Europeu de Normalització (CEN CWA 14170) ofereix un conjunt de mesures de seguretat funcional aplicables al programari que funciona conjuntament amb dispositius segurs de creació de signatura electrònica (aplicacions de signatura electrònica) per garantir un nivell apropiat de seguretat, en desenvolupament de la Directiva 99/93/CE.

Tot i no gaudir de la consideració legal de norma tècnica, CEN CWA 14170 és, ara per ara, l'únic document aplicable a l'Estat espanyol, ja que no existeix desplegament reglamentari de la Llei 59/2003, de 19 de desembre, de signatura electrònica, per interpretar els requisits de l'article 24 de la Llei esmentada, en relació amb les aplicacions de creació de signatura electrònica, d'una manera objectiva, transparent i no discriminatòria.

6.2.1. *El model funcional de creació de la signatura electrònica*

L'objectiu d'aquest model és explicar quins són els participants principals en un sistema de creació de signatura electrònica, d'acord amb els diferents entorns o escenaris en què treballen, i les funcions que executen, amb un grau elevat de detall, per arribar a entendre les seves necessitats de seguretat.

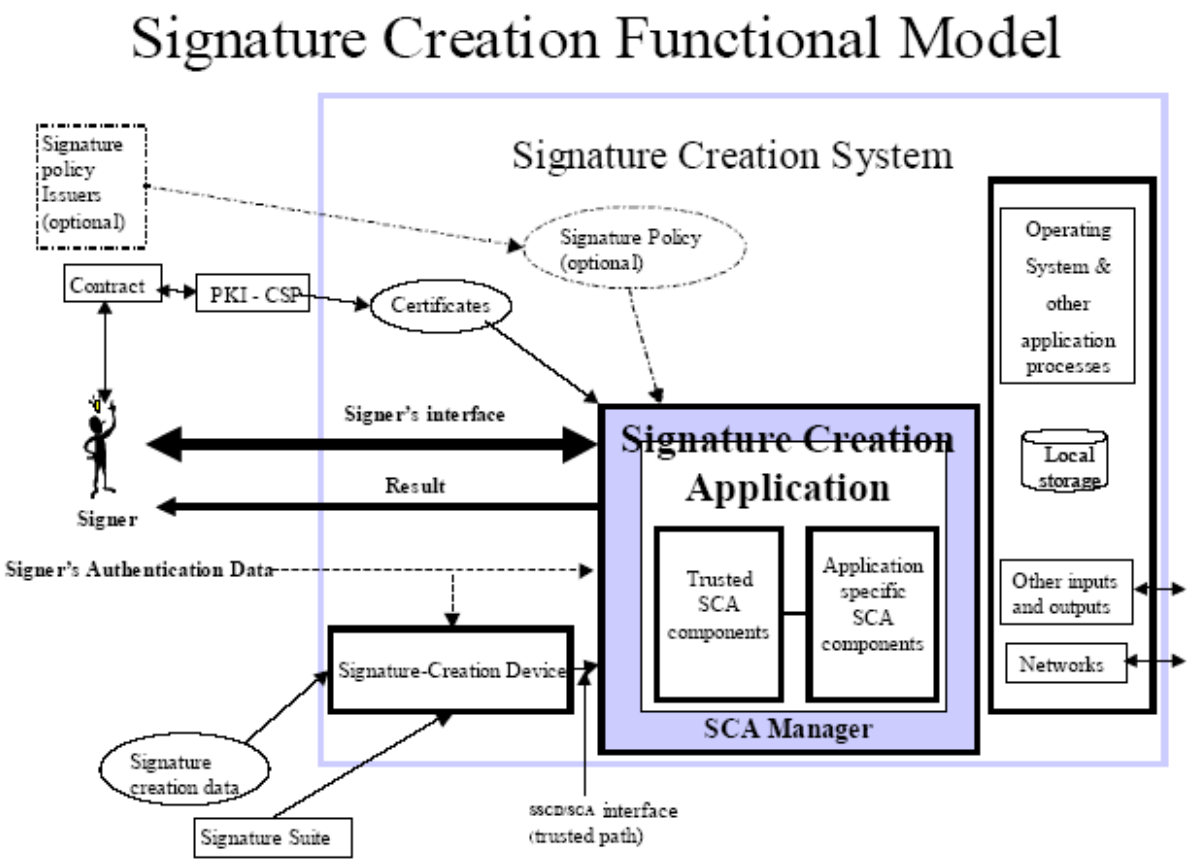
L'entorn de creació de signatura és l'element més genèric del model, i inclou un signatari que interactua amb un sistema de creació de signatura.

[84] Funcionalitat que haurà d'aportar la biblioteca de programació de serveis criptogràfics (PKCS#11, CSP o una altra de diferent), però que cal emprar correctament, excepte quan el sistema creï i utilitzi el canal fiable de manera transparent per a l'usuari.

El sistema de creació de signatura conté fonamentalment els elements següents:

- Una aplicació de creació de signatura.
- Un dispositiu —segur— de creació de signatura.
- Un certificat electrònic —reconegut— de signatura associat al dispositiu de creació de signatura.
- Opcionalment, una política de signatura electrònica, que indica els requisits de seguretat tècnica per a la creació de la signatura que hauran de complir l'aplicació de signatura electrònica i el dispositiu.

El gràfic següent[85] il·lustra el model funcional de creació de la signatura electrònica:



El propòsit de l'aplicació de signatura electrònica i del dispositiu de creació de signatura és generar, a partir d'un document del signatari i dels atributs associats a la signatura —com ara la data i l'hora de la signatura o el rol d'acord amb el qual el signatari crea la signatura (càrrec de l'Administració pública, apoderat, delegat, etc.)—, el conjunt de les dades a signar.

[85] CEN CWA 14170.

Posteriorment, es genera una signatura electrònica avançada —o reconeguda, quan el dispositiu és segur i el certificat és reconegut— sobre les dades a signar i, finalment, un document en suport informàtic anomenat *dades signades*.

Lògicament, és molt important que les funcions de l'aplicació de creació signatura electrònica i les comunicacions entre l'aplicació de creació de signatura electrònica i el dispositiu —segur— de creació de signatura siguin realment fiables, perquè altrament aquesta aplicació podria enganyar l'usuari i obtenir una signatura electrònica per a un document diferent, per exemple, del que es mostra a la pantalla de l'ordinador.

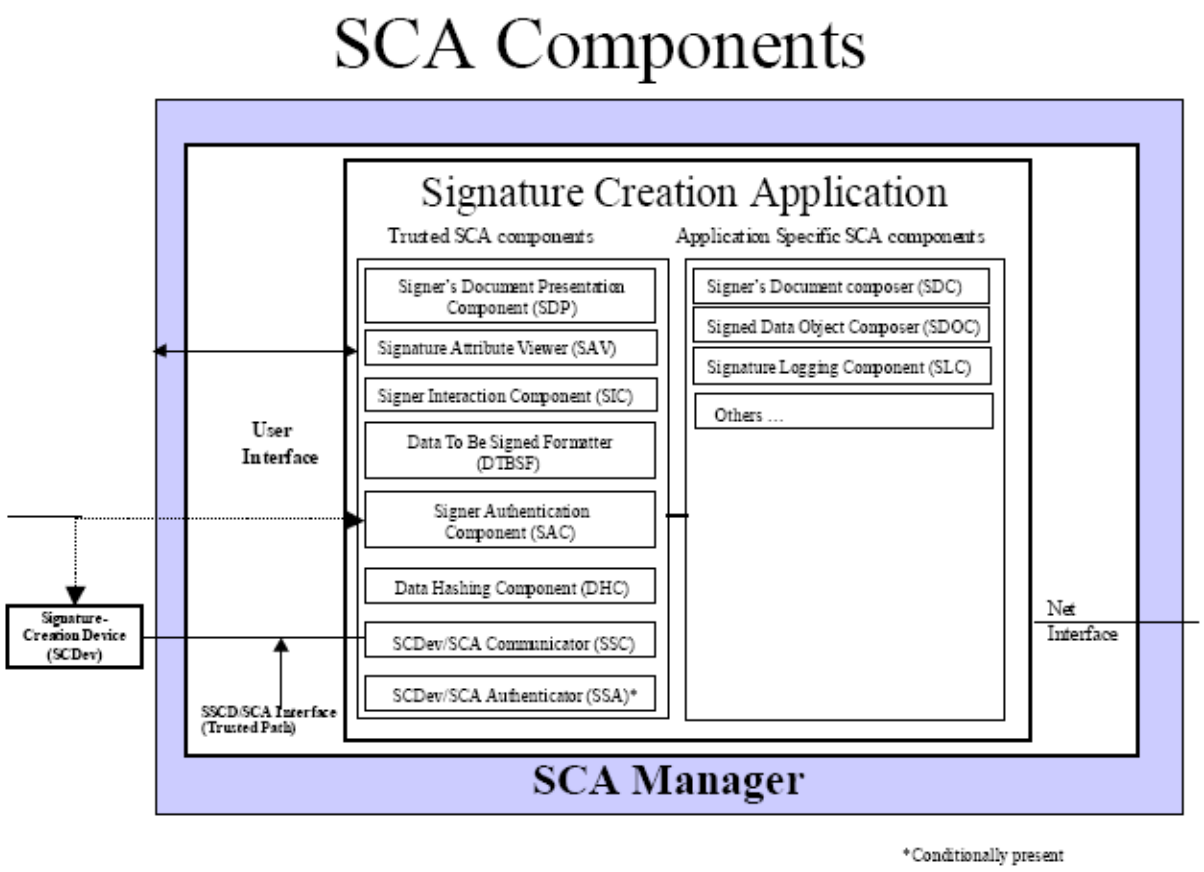
6.2.2. *Els components fiables de l'aplicació de signatura electrònica*

Per garantir la fiabilitat de les funcions i les comunicacions de l'aplicació de signatura electrònica, CEN CWA 14170 estableix requisits de seguretat a diferents components que formen part de l'aplicació i distingeix els components fiables dels components específics de l'aplicació.

Evidentment, aquests components no imposen cap restricció d'arquitectura als proveïdors d'aplicacions de creació de signatura, sinó que suposen agrupacions de funcionalitats útils per determinar-ne els requisits de seguretat corresponents.

Mentre que els components fiables són, en general, obligatoris, els components específics d'aplicació són opcionals i depenen de cada proveïdor d'aplicacions de creació de signatura.

La figura següent mostra els components d'una aplicació de creació de signatura:



Els components fiables de l'aplicació de creació de signatura són els següents:

- Component de presentació del document del signatari, que s'empra per presentar el document que el signatari escull per signar, mitjançant el component d'interacció amb el signatari.

- Component visor d'atributs de signatura, que es fa servir per visualitzar els atributs de la signatura que el signatari escull per incorporar a la signatura, mitjançant el component d'interacció amb el signatari. Ha d'incloure la possibilitat de visualitzar els continguts principals del certificat —reconegut— del signatari.

- Component d'interacció amb el signatari, que el signatari utilitza per interactuar amb l'aplicació de signatura electrònica i controlar el procés de creació de signatura, així com per notificar informacions d'estat i d'errors de l'aplicació. Aquest component inclou totes les interaccions amb el signatari tret de l'autenticació.

- Component de formatació de dades a signar, que s'empra per donar format previ a un document o a un resum criptogràfic d'un document, juntament amb els

atributs de la signatura, per passar-ho al component de creació de resums criptogràfics.

- Component d'autenticació de signatari, que s'utilitza per obtenir credencials conegudes pel signatari, o alguna mostra biomètrica d'aquest, i preparar aquestes dades d'autenticació per comparar-les amb les dades d'autenticació del signatari emmagatzemades al dispositiu —segur— de creació de signatura electrònica.

- Component de creació de resums criptogràfics, que es fa servir per produir la representació de les dades a signar a partir de les dades a signar formatades (que poden estar resumides totalment o parcialment de forma criptogràfica o en text en clar). Només s'utilitza en cas que el dispositiu —segur— de creació de signatura no generi els seus propis resums criptogràfics.

- Component de comunicació entre l'aplicació de creació de signatura electrònica i el dispositiu —segur— de creació de signatura, que s'empra per gestionar la interacció entre tots dos.

- Component d'autenticació entre l'aplicació de creació de signatura electrònica i el dispositiu —segur— de creació de signatura, que s'utilitza per establir una ruta fiable entre tots dos quan aquesta no es pot establir per mecanismes organitzatius.

Així mateix, els components específics de l'aplicació de creació de signatura poden ser, entre d'altres, els següents:

- Component de composició de documents, que s'empra per crear i editar documents, mitjançant el component d'interacció amb el signatari. Aquest component no s'utilitza en el cas de l'actuació administrativa automatitzada.

- Component de composició d'objectes de dades signades, que es fa servir per donar format al resultat del procés de creació de signatura, per exemple associant la signatura i les dades signades, en un format preferit per l'aplicació —com ara el definit per ETSI TS 101733 o TS 101903.

- Component de registre de signatures, que enregistra detalls importants sobre les signatures produïdes.

- Component d'indicació del posseïdor del dispositiu —segur— de creació de signatura electrònica.

- Altres, d'acord amb les necessitats de cada aplicació concreta.

6.3. La seguretat de les comunicacions de l'aplicació

En aquest apartat presentem els requisits de seguretat de les comunicacions entre els diferents components del sistema de signatura, com ara entre l'aplicació i el dispositiu de creació de signatura electrònica, així com entre els diferents components de l'aplicació distribuïda de signatura electrònica, i l'ús de les interfícies externes a l'aplicació.

Podem agrupar els requisits en dues categories:

- Requisits de comunicació fiable entre components del sistema.
- Requisits de les interfícies externes a l'aplicació.

6.3.1. *Els requisits de comunicació fiable entre components del sistema*

En primer lloc, cal establir una comunicació fiable entre tots dos elements del sistema de signatura amb la finalitat de protegir les dades relatives a la signatura (dades d'autenticació, dades a signar, dades a signar formatades i representació de les dades a signar). Aquesta comunicació fiable serà més exigent quan l'aplicació de signatura es trobi en un entorn públic.

Com hem vist, aquesta comunicació dóna compliment al requisit de ruta fiable (*trusted path*) amb l'SSCD en relació amb les dades d'autenticació del signatari, i amb el requisit de canal fiable (*trusted channel*) amb l'SSCD en relació amb la resta de dades de la signatura electrònica.

En segon lloc, quan l'aplicació de creació de signatura funcioni de forma distribuïda, amb components en diferents plataformes, és necessari protegir les comunicacions entre aquests components, ja que és possible que la informació relativa a la signatura circuli per enllaços de comunicacions potencialment no fiables o per interfícies d'aplicacions internes també potencialment no fiables, com també per mòduls de programari i maquinari que podrien sotmetre les dades relatives a la signatura a vulnerabilitats quant a integritat, autenticitat i confidencialitat.

Un cas d'aplicació distribuïda és l'ús de servidors centrals d'aplicació de signatura electrònica (de vegades anomenats *servidors de signatures*) connectats a sistemes de

gestió documental o de gestió d'expedients, davant els quals l'usuari sol·licita la signatura, per exemple emprant l'estàndard DSS.[86]

En aquest cas, l'usuari normalment no posseeix físicament el document. Totes les operacions es duen a terme de manera remota, entre dos sistemes que rauen en plataformes diferents, fet que implica haver d'establir requisits addicionals de seguretat per garantir la fiabilitat global del sistema.

En tercer lloc, habitualment el sistema en què resideix l'aplicació de signatura electrònica executa altres processos informàtics i, a més, disposa de perifèrics i ports de comunicacions amb altres sistemes. Tots aquests elements s'han de considerar potencialment no fiables.

Les amenaces identificades són les següents:

- En relació amb la comunicació fiable entre l'aplicació i el dispositiu:

    - Alteració accidental o maliciosa dels component de les dades a signar. Consisteix en el fet que els processos de la infraestructura emprada per l'aplicació de signatura electrònica alteren, per accident o malintencionadament, les dades a signar, abans o després de rebre format, o la representació resumida criptogràficament d'aquestes dades seleccionades pel signatari, o qualsevol altra dada dels protocols de comunicació entre l'aplicació i el dispositiu.

    - Ruptura accidental o maliciosa de la confidencialitat de les dades d'autenticació del signatari, dels components de les dades a signar o de les dades a signar formatades. Consisteix en el fet que la infraestructura de l'aplicació de signatura revela o copia a persones no autoritzades les dades d'autenticació del signatari (per exemple, la seva contrasenya), els components de les dades a signar o les dades a signar formatades.

    - Divulgació o ús erroni de les dades d'autenticació del signatari, dels components de les dades a signar o de les dades a signar formatades per un sistema públic de creació de signatura operat per un proveïdor de servei. Consisteix en el fet que el sistema públic de signatura infringeix la confidencialitat de les dades d'autenticació del signatari, dels components de les dades a signar o de les dades a signar formatades.

[86] DSS és un estàndard produït per OASIS que permet la sol·licitud remota de generació i de verificació de signatures mitjançant serveis web.

- Substitució d'un o diversos components de les dades a signar o de les dades a signar formatades. Consisteix en el fet que la infraestructura de l'aplicació de signatura substitueix components de les dades a signar, abans o després de rebre format, de manera accidental o malintencionada, abans que es completi el procés de generació de signatura.

- En relació amb les aplicacions distribuïdes de creació de signatura:

  - Ruptura de la integritat o la confidencialitat de les dades d'autenticació del signatari en trànsit entre components de l'aplicació distribuïda de signatura electrònica. Consisteix en el fet que les dades d'autenticació del signatari (per exemple, la seva contrasenya) es corrompen, s'alteren o es divulguen, accidentalment o maliciosament, mentre són transferides entre els components de l'aplicació distribuïda de signatura electrònica.

  - Ruptura de la integritat o la confidencialitat de les dades a signar, abans o després de la formatació, en trànsit entre components de l'aplicació distribuïda de signatura electrònica. Consisteix en el fet que les dades a signar o les dades a signar formatades es corrompen, s'alteren o es divulguen, accidentalment o maliciosament, mentre són transferides entre els components de l'aplicació distribuïda de signatura electrònica.

- En relació amb els processos i els ports de comunicacions no fiables:

  - Interferència produïda per processos i ports de comunicacions no fiables. Consisteix en el fet que els processos i els ports d'entrada i sortida del sistema de l'aplicació de creació de signatura electrònica que no estan sota el control de l'aplicació poden corrompre o trencar la confidencialitat de les dades d'autenticació del signatari, de les dades a signar —amb format o sense— o corrompre els processos de la mateixa aplicació de creació de signatura electrònica.

Els requisits de seguretat corresponents són els següents:

- L'aplicació ha de mantenir la integritat de:

  - Les dades a signar, les dades a signar formatades, la representació de les dades a signar i la resta d'informacions subministrades pel signatari.

- Els intercanvis de dades durant el flux del protocol de comunicació entre l'aplicació i el dispositiu, mitjançant l'ús d'un canal segur.

- L'aplicació ha de mantenir la confidencialitat dels components de les dades a signar, de les dades a signar formatades i de les dades d'autenticació del signatari.

- L'aplicació que operi en un entorn públic esborrarà de forma segura totes les dades relatives a una signatura després d'haver completat el procés corresponent.

- Quan s'utilitzi un sistema públic de creació de signatura, aquest no haurà de retenir les dades d'autenticació del signatari, dels components de les dades a signar i de les dades a signar formatades. Tampoc no haurà de copiar les dades esmentades a cap persona no autoritzada pel signatari.

- L'aplicació ha de garantir que les dades a signar presentades al signatari són les mateixes que les que aquest va seleccionar.

- L'aplicació ha de garantir que els components de les dades a signar emprades per crear les dades a signar formatades i la representació de les dades a signar són els mateixos que es van presentar al signatari, com també que les dades són idèntiques a les que aquest va seleccionar.

- Qualsevol dada d'autenticació del signatari que sigui transferida entre diferents components distribuïts de l'aplicació de creació de signatura electrònica s'ha de transferir emprant una ruta fiable que ofereixi integritat i confidencialitat.

- Les dades a signar —amb format o sense— que siguin transferides entre diferents components distribuïts de l'aplicació de creació de signatura electrònica s'han de transferir emprant un canal fiable que ofereixi integritat i confidencialitat

- Tots els processos i els ports d'entrada i sortida del sistema de l'aplicació de creació de signatura electrònica que no estiguin sota el control de l'aplicació es tancaran o es monitoraran per evitar interferències.

6.3.2. *Els requisits de les interfícies externes a l'aplicació*[87]

Les interfícies externes a l'aplicació de signatura electrònica impliquen diversos riscos per a l'aplicació. Podem esmentar, entre d'altres, la possibilitat d'atac de substitució o de modificació de l'aplicació de signatura electrònica o dels seus components, així com vulnerabilitats degudes a virus i altres formes de programari maliciós.

Les amenaces identificades són les següents:

- Compromís de components de l'aplicació per programari maliciós. Consisteix en el fet que el programari maliciós importat corromp components de l'aplicació de signatura electrònica.

- Compromís de components de l'aplicació per intrusos. Consisteix en el fet que l'intrús corromp components de l'aplicació de signatura electrònica.

- Compromís de components de l'aplicació per programari fals instal·lat. Consisteix en el fet que el programari fals instal·lat genera signatures electròniques invàlides.

Els requisits de seguretat corresponents són els següents:

- L'aplicació de signatura electrònica ha d'evitar ser corrompuda per codi maliciós i, en cas que això passi, ha d'existir un procés per sanejar els components corruptes.

- L'aplicació de signatura electrònica ha de mantenir la integritat dels seus components funcionals i evitar la possibilitat que els corrompin intrusos.

- En relació amb els components de l'aplicació que es poden descarregar de la xarxa, la descàrrega s'ha de fer des d'una font fiable, circumstància que s'indicarà a la documentació del producte.

[87] CEN CWA 14170, secció 18.

6.4. La seguretat de les dades de signatura gestionades per l'aplicació

En aquest apartat presentem els requisits de seguretat dels documents, les dades i altres informacions relatius a la signatura electrònica que queden dins l'àmbit de responsabilitat de l'aplicació de signatura electrònica.

Els atacs contra aquestes dades són especialment importants, ja que la manipulació, la corrupció o la substitució del document —o de les dades— a signar, en qualsevol moment del procés, condueixen a la generació de signatures falses.

Tot i els objectius de seguretat que exposarem a continuació, convé remarcar que és important verificar l'objecte signat en finalitzar el procés, fet que ens permetrà detectar i corregir possibles errors.

Podem agrupar els requisits en les categories següents:

- Requisits generals de seguretat de les dades a signar.
- Requisits de seguretat propis del document a signar.
- Requisits de seguretat dels atributs de signatura electrònica.
- Requisits de seguretat del procés de resum i formatació de les dades a signar.

6.4.1. *Els requisits generals de seguretat de les dades a signar*[88]

Existeixen situacions que afecten la seguretat global del sistema, resultants de la manipulació de les dades a signar per part de l'aplicació de signatura electrònica, així com la producció de l'estructura de dades que conté l'objecte signat.

Per aquest motiu, cal garantir que les dades a signar tenen una seguretat mínima, abans de continuar el procés, i verificar la signatura produïda abans de lliurar-la a terceres persones.

Les amenaces identificades són les següents:

- Generació d'una signatura inapropiada. Consisteix en el fet que es genera una signatura per a un document nul, sense cap contingut, de tal manera que la signatura es genera només sobre els atributs de signatura del document.

[88] CEN CWA 14170, seccions 7.5 i 7.6.

- Ambigüitat del certificat del signatari que consta a la signatura electrònica. Consisteix en el fet que es pot associar la signatura a un certificat del signatari, amb una semàntica diferent de la prevista pel signatari.

- Generació d'una signatura incorrecta. Consisteix en el fet que es produeix una signatura incorrecta matemàticament a causa de la corrupció d'alguna de les dades a signar o, especialment, de la representació resumida d'aquestes dades, per error de l'aplicació o del dispositiu de creació de signatura.

Els requisits de seguretat corresponents són els següents:

- Les dades a signar han d'incloure necessàriament un document del signatari.

- La signatura ha de contenir necessàriament el certificat del signatari seleccionat, quan s'escaigui, relatiu a les dades de creació de signatura emprades per produir la signatura electrònica, d'acord amb la intenció del signatari.

- Les dades a signar han de contenir el tipus de contingut de dades del document del signatari sempre que aquesta informació no consti al mateix fitxer.

- Cal verificar la signatura electrònica produïda, encara que aquesta verificació no sigui completa.[89]

6.4.2. *Els requisits de seguretat propis del document a signar*[90]

L'aplicació de creació de signatura electrònica ha de garantir que el document que veu[91] el signatari a la seva pantalla és el mateix que signarà. Aquest document no ha estat ni serà manipulat, corromput ni substituït des del moment que el signatari l'haurà seleccionat i fins a la producció de la signatura.

Per oferir aquestes garanties, cal implantar les funcions d'un component de presentació del document al signatari. Aquest component ha de conèixer els tipus de contingut de

[89] La verificació es pot referir a la correcció criptogràfica de la signatura digital, per exemple, abans d'incrustar-la a l'estructura de dades de l'objecte signat. Si ja hem verificar el certificat anteriorment o si tenim garantia de la seva vigència, no cal tornar-lo a verificar.

[90] CEN CWA 14170, secció 8.

[91] El document a mostrar té un tipus de contingut de dades concret, que és el que s'utilitza per cridar el mòdul que interpreta i visualitza el document. Així, per exemple, per al tipus de contingut PDF, cridem el visor d'Adobe Acrobat.

dades associats als documents que es poden signar, ja que aleshores es poden senyalitzar les situacions pròpies de cada format.[92]

En el cas de l'actuació administrativa automatitzada, no es dóna la circumstància que el document sigui presentat al signatari. Així doncs, no serà necessari implementar mesures de seguretat específiques, però sí que caldrà, en tot cas, controlar quin és el format documental sobre el qual s'ha de generar la signatura electrònica, sobretot si es tracta d'una signatura electrònica embolcallada dins el document.

6.4.3. *Els requisits de seguretat dels atributs de signatura electrònica*[93]

L'aplicació de signatura electrònica ha de garantir la seguretat dels atributs de la signatura electrònica mitjançant la funcionalitat d'un component de visualització dels atributs de signatura electrònica que permeti presentar-los al signatari, amb la finalitat que aquest els pugui inspeccionar de manera fiable.

El signatari hauria de poder accedir a tots els atributs de la signatura, però especialment als següents:

- El certificat del signatari.
- El tipus de contingut de dades corresponent al document del signatari, quan es troba present.
- La política de signatura electrònica, quan es troba present.
- El tipus de compromís de la signatura electrònica, quan es troba present.

Es considera que l'ús d'un certificat que hagi estat revocat o hagi expirat constitueix una amenaça de seguretat perquè pot conduir a la producció de signatures invàlides. L'aplicació de signatura electrònica hauria de comprovar-ne la validesa i l'estat de revocació abans de finalitzar el procés general de signatura electrònica.[94]

D'altra banda, és imprescindible que el signatari pugui conèixer el contingut del certificat de signatura i triï expressament el certificat amb què vol signar —quan en disposa de més d'un— per evitar errors que indubtablement afectaran la validesa de la signatura electrònica corresponent.

---

[92] Per exemple, que el tipus de contingut té informació invisible per al signatari, de la qual cosa deriva que no quedarà vinculat per aquesta informació, sinó únicament per la informació que va poder veure quan signava.

[93] CEN CWA 14170, secció 9.

[94] Per exemple, mitjançant la consulta a la llista de revocació de certificats (CRL) o al servidor OCSP (protocol en línia d'estat de certificats).

Les amenaces identificades són les següents:

- Signatura d'un atribut incorrecte. Consisteix en el fet que la signatura s'aplica sobre atributs que no són apropiats per a la signatura que es desitja generar.

- Alteració accidental o maliciosa dels atributs per part de l'aplicació. Consisteix en el fet que la signatura canvia de significat i intenció a causa de la modificació, accidental o maliciosa, dels atributs per part de l'aplicació de signatura electrònica.

- Referència a un certificat de signatura invàlid. Consisteix en el fet que el certificat de signatura ha expirat o ha estat revocat i, per tant, la signatura ha estat produïda invàlidament.

- Referència a un certificat de signatura incorrecte. Consisteix en el fet que la signatura s'associa a un certificat diferent del que pretenia l'usuari, cosa que pot implicar un canvi en el significat de la signatura i produir errors de verificació.

Els requisits de seguretat corresponents són els següents:

- L'aplicació de signatura electrònica ha de controlar els atributs a signar.

- L'aplicació de signatura electrònica ha de garantir la integritat i l'autenticitat dels atributs de la signatura.

- L'aplicació de signatura electrònica ha d'informar el signatari de la presència de text ocult, macros o codi actiu als atributs,[95] sempre que no es tracti d'un comportament programat prèviament, cosa que implica parar el procés automatitzat i permetre la inspecció d'aquests atributs mitjançant un visor dels atributs signats, amb la capacitat de detectar les modificacions de la presentació dels atributs signats.

- L'aplicació de signatura electrònica ha de comprovar el període de validesa del certificat i el seu estat de revocació abans de finalitzar el procés de signatura, i també impedir-ne l'ús en cas d'invalidesa.

[95] Normalment els atributs no contenen aquests tipus de dades, però, si ho fan, aleshores cal fer-ne conscient el signatari.

- L'aplicació de signatura electrònica ha de permetre al signatari la inspecció dels principals elements del certificat de signatura amb què signarà[96] en el moment de configurar l'acte administratiu automatitzat.

6.4.4. *Els requisits de seguretat del procés de resum[97] i formatació[98] de les dades a signar*

L'aplicació de signatura electrònica ha de garantir la seguretat del procés de formatació de les dades a signar, que es produeix a partir del document de signatari i dels atributs de signatura.

En cas que les dades a signar hagin d'incloure el resum criptogràfic de les dades, aleshores abans de finalitzar el procés de formatació es produeix aquest resum en les condicions de seguretat necessàries.[99] Aquest resum criptogràfic també s'anomena, com hem vist, *representació de les dades a signar*.

Quant al procés de resum criptogràfic, hi ha tres possibilitats:

- Produir-lo íntegrament a l'aplicació de signatura electrònica.
- Produir-lo parcialment a l'aplicació de signatura electrònica i acabar-lo al dispositiu —segur— de creació de signatura electrònica.
- Produir-lo íntegrament al dispositiu —segur— de creació de signatura electrònica.[100]

Les amenaces identificades són les següents:

- En relació amb la formatació de la signatura:
    - Producció de dades a signar incorrectes o incompletes. Consisteix en el fet que, com a resultat d'un atac, l'aplicació no aplica totes les dades necessàries per a la signatura electrònica d'acord amb un format concret (com ara el format de signatura de llarga durada), o bé en el fet que

[96] Aquesta obligació no implica que el signatari sempre hagi d'escollir el seu certificat per signar, ja que, si només en té un, és evident que no es pot equivocar a l'hora de triar-lo per a la signatura.
[97] CEN CWA 14170, secció 13.
[98] CEN CWA 14170, secció 12.
[99] Incloent-hi, en funció de l'algorisme emprat, el *padding* del resum.
[100] Això requereix disposar d'un canal de comunicació amb el dispositiu d'un ample de banda considerable, com succeeix amb els dispositius de maquinari connectats físicament al servidor de signatura, mitjançant el bus de comunicacions físiques (PCI, per exemple) o per xarxa, quan es vol fer sobre documents de gran longitud.

l'aplicació de signatura rep components de la signatura que han estat falsificats.

- En relació amb la formatació de la signatura:

    - Algorisme dèbil de resum. Consisteix en el fet que es poden produir col·lisions, és a dir, que dos documents diferents poden donar lloc al mateix resum.

    - Format d'entrada dèbil de signatura electrònica. Consisteix en el fet que es poden produir problemes per computar la signatura electrònica.

    - Producció de la representació de les dades a signar incorrecta o incompleta. Consisteix en el fet que la representació de les dades a signar no conté els components requerits per la política de seguretat i pel signatari, la qual cosa pot produir un document signat incomplet i ambigu.

Els requisits de seguretat corresponents són els següents:

- L'aplicació de signatura electrònica imposarà controls per verificar la validesa, l'autenticitat i la totalitat dels els components obtinguts per produir el format correcte de signatura escollit pel signatari.

- L'aplicació de signatura electrònica emprarà els algorismes de resum adequats per a la producció de la representació de les dades a signar.

- L'aplicació de signatura electrònica emprarà els formats d'entrada de signatura electrònica adequats per a la producció de la signatura de les dades a signar.

- L'aplicació de signatura electrònica ha de garantir la producció correcta de la representació de les dades a signar.

6.5. La seguretat dels processos amb el signatari

En aquest apartat presentem la seguretat dels processos amb el signatari —concretament, de la interfície entre l'usuari i l'aplicació— i l'autenticació de l'usuari per part de l'aplicació.

La secció no inclou cap aspecte relatiu a la interacció segura entre l'aplicació i el dispositiu (autenticació entre tots dos elements i comunicació segura posterior), qüestions que ja s'han explicat anteriorment.

Podem agrupar els requisits en les categories següents:

- Requisits d'interacció segura entre el signatari i l'aplicació.
- Requisits d'identificació i autenticació del signatari.

6.5.1. *Els requisits d'interacció segura entre el signatari i l'aplicació*[101]

La interacció que s'estableix entre l'aplicació de signatura electrònica i el signatari és de vital importància, per tal com el component d'interacció amb el signatari es responsabilitza de captar la voluntat del signatari i traduir-la correctament als processos de creació de signatura que s'imputaran a la persona.

Evidentment, aquesta problemàtica només existeix quan el dispositiu —segur— de creació de signatura electrònica delega a l'aplicació l'autenticació del signatari, perquè, en cas contrari, senzillament s'aplica la política de seguretat del dispositiu —que és el que passa en el cas de l'actuació administrativa automàtica.

6.5.2. *Els requisits d'identificació i autenticació del signatari*[102]

L'aplicació de signatura electrònica pot gestionar els mecanismes d'identificació i autenticació del signatari en col·laboració amb el dispositiu —segur— de creació de signatura electrònica.

Aquesta possibilitat depèn, en realitat, del proveïdor del dispositiu segur, ja que si la seva política és autenticar directament, mitjançant la seva pròpia interfície d'usuari, com hem vist, aleshores l'aplicació no s'haurà d'interposar en aquella interacció directa.

Tanmateix, si el dispositiu de creació de signatura no disposa d'interfície amb el signatari, o quan aquesta opció es pugui configurar a voluntat del signatari (mitjançant la corresponent interfície de gestió administrativa del dispositiu), l'aplicació de signatura

[101] CEN CWA 14170, secció 10.
[102] CEN CWA 14170, secció 11.

electrònica es podrà fer càrrec dels aspectes d'autenticació del signatari, sempre implantant una sèrie de mesures de seguretat.

En el cas de l'actuació administrativa automatitzada, els requisits d'identificació i d'autenticació resulten aplicables en el moment de posada en marxa de l'aplicació, ja que aquesta ha de tenir accés a la clau privada del segell d'òrgan, administració pública o entitat de dret públic.

Les amenaces identificades són les següents:

- Ús no autoritzat del dispositiu —segur— de signatura electrònica. Consisteix en el fet que una persona no autoritzada obté accés al dispositiu de creació de signatura i, en conseqüència, pot falsificar signatures.

- Divulgació, per l'aplicació de signatura, de les dades d'autenticació del signatari. Consisteix en el fet que les dades d'autenticació del signatari, que l'aplicació de signatura coneix, són divulgades a terceres persones.

- Introducció accidental de dades incorrectes d'autenticació del signatari.

- Endevinament de les dades d'autenticació del signatari. Consisteix en el fet que un atacant endevina les dades d'autenticació del signatari, per sort o per un atac de força bruta.

- Intercepció i mal ús posterior de les dades d'autenticació del signatari. Consisteix en el fet que una tercera persona intercepta les dades d'autenticació del signatari introduïdes mitjançant el teclat de l'ordinador personal, o el teclat del dispositiu, i les utilitza posteriorment per suplantar la identitat del signatari.

- Compromís del secret de les dades d'autenticació del signatari. Consisteix en el fet que una tercera persona obté les dades d'autenticació del signatari sense trencar la seguretat de l'aplicació de signatura electrònica, o del dispositiu segur de signatura electrònica, i les utilitza posteriorment per suplantar la identitat del signatari.

- Visualització, per l'aplicació de signatura, de les dades d'autenticació del signatari. Consisteix en el fet que l'aplicació mostra les dades d'autenticació del signatari que aquest introdueix, cosa que fa que puguin ser observades i conegudes per terceres persones.

- Error de tecleig d'unes noves dades d'autenticació del signatari durant el procés de canvi d'aquestes dades. Consisteix en el fet que el signatari no podrà canviar les seves dades d'autenticació, de manera que haurà de conservar unes dades d'autenticació que, amb el temps, perdran força.

Els requisits de seguretat corresponents són els següents:

- L'aplicació de signatura electrònica, quan sigui responsable de l'autenticació del signatari, haurà de proveir una funció per dur a terme aquest procés de manera segura.

- Quan les dades d'autenticació del signatari estiguin emmagatzemades a l'aplicació de signatura electrònica, aquestes dades s'hauran de preservar de manera confidencial i s'hauran d'esborrar quan ja no siguin necessàries.

- L'aplicació de signatura electrònica, de manera coordinada amb el dispositiu segur de signatura electrònica, haurà de permetre diversos intents d'autenticació mitjançant un comptador i una funció de bloqueig, en cas de superació dels intents permesos. L'aplicació no haurà de donar informació sobre el tipus d'error comès per la persona que s'autentica.

- L'aplicació de signatura electrònica ha de funcionar de manera coordinada amb el dispositiu de signatura electrònica en tot allò referit a la política de seguretat de les dades d'autenticació (especialment longituds de claus i semàntica de la contrasenya), i no ha d'impedir aplicar la política de canvi de contrasenya del dispositiu de signatura electrònica.

- L'aplicació de signatura que gestioni l'autenticació del signatari ha d'implantar una ruta fiable des del teclat de l'ordinador, o des del lector de targeta, fins al dispositiu de signatura electrònica.

- L'aplicació de signatura ha d'implantar una funció de canvi de les dades d'autenticació de signatura, excepte quan la seva política de seguretat ho prohibeixi i aquesta prohibició no suposi una interferència amb la política de canvi de contrasenya del dispositiu de signatura electrònica.

- L'aplicació de signatura electrònica no mostrarà les dades d'autenticació de signatura, sinó un o més símbols per indicar el tecleig de les dades. Aquests símbols no revelaran les dades d'autenticació ni permetran endevinar-les.

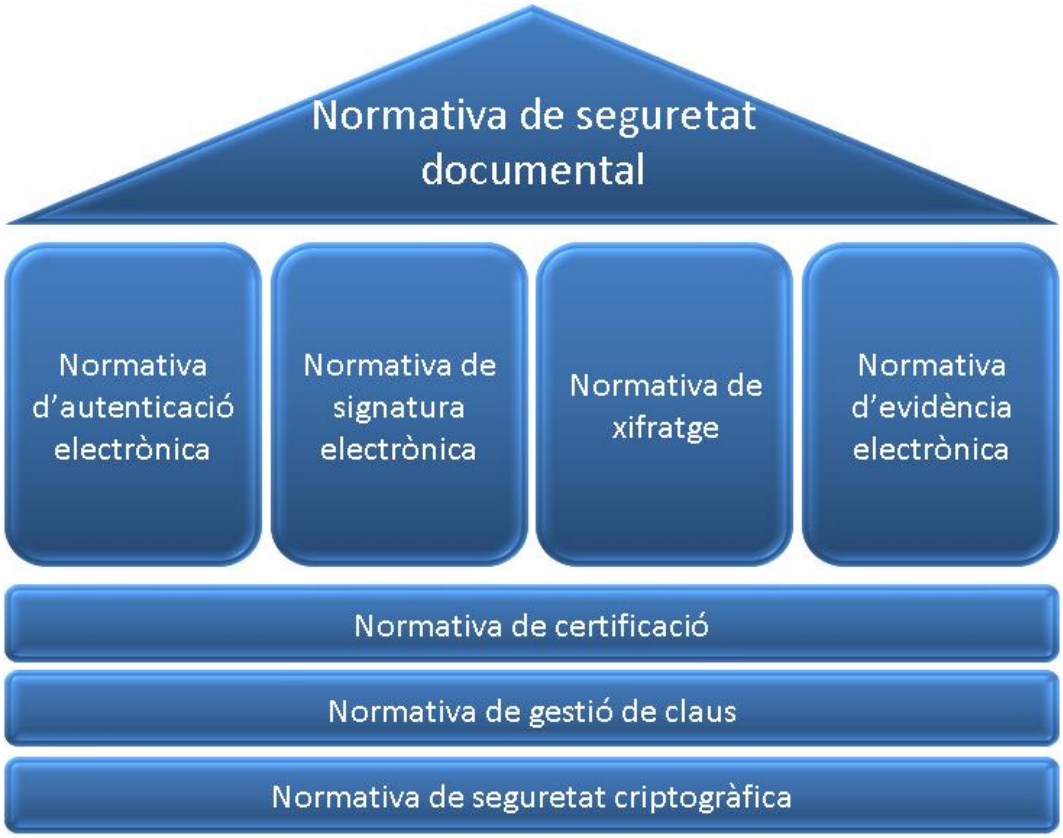
- L'aplicació de signatura electrònica requerirà la introducció dos cops d'unes noves dades d'autenticació i comprovarà que totes dues són idèntiques abans de lliurar-les al dispositiu de signatura per al canvi.

7. LES NORMATIVES DE SEGURETAT CRIPTOGRÀFICA DE L'APLICACIÓ D'ACTUACIÓ ADMINISTRATIVA AUTOMATITZADA

En aquest apartat es tracten les normatives de seguretat criptogràfica de l'aplicació d'actuació administrativa automatitzada. Hi analitzem el cos normatiu que es requereix per a l'assegurament de la seguretat de l'aplicació, i, en especial, les normatives de signatura electrònica, que desenvolupem d'una manera particularment intensa per la seva rellevància en termes de validesa formal dels actes automàtics.

Les normatives de seguretat s'estructuren en forma de documents específics de seguretat que cal inserir dins l'estructura documental del procés general de seguretat de l'organització. Cada document de normativa implementa controls definits per la norma ISO/IEC 27002:2005 i per altres normes rellevants.

A continuació es presenta de forma esquemàtica el conjunt de normes de seguretat criptogràfica:



7.1. La normativa de seguretat documental

La normativa de seguretat documental s'aplica als diferents tipus de documents a formalitzar i concreta de manera detallada l'aplicació de les normatives i els estàndards d'autenticació, signatura electrònica, xifratge i evidència electrònica, segons s'escaigui.

Aquesta normativa s'alinea amb els requisits de seguretat de gestió documental, d'acord amb les normes ISO 15489 i MoReq 2, i es desplega en forma d'estàndards tècnics obligatoris per a documents tipus i expedients concrets en guies o recomanacions i en procediments operatius.

Així mateix, és necessari concretar un catàleg de formats documentals electrònics a emprar (PDF, ODF, Word, WS, S/MIME…) a l'efecte d'establir les normes de seguretat oportunes per a cada format.

Els continguts principals són els següents:

- Establiment de principis generals de seguretat documental d'acord amb la legislació (p. ex., Llei 11/2007).
    - Protecció de dades personals.
    - Seguretat mínima.
    - Proporcionalitat.
    - Accessibilitat a la informació i multicanalitat.
- Requisits legals de seguretat documental.
    - Entrades de documents.
    - Producció de documents i còpies.
    - Sortida de documents.
    - Formació d'expedients, conservació i arxivament.
- Requisits de gestió documental segura.
    - Producció de documents originals electrònics.
        - Originals interns (resolució).
        - Originals adreçats als ciutadans (notificació).
        - Originals per publicar (edicte).

- Producció de còpies electròniques.

    - Còpia autèntica de document original intern, per lliurar al ciutadà, si s'escau amb canvi de format (còpia autèntica d'una resolució).
    - Còpia autèntica de document extern, amb canvi de suport (digitalització) o de format (d'un format ofimàtic a un format de preservació).

Algunes aplicacions de la norma són les següents:

- Estàndard tècnic de seguretat documental de resolució administrativa.
- Estàndard tècnic de seguretat documental de publicació.
- Estàndard tècnic de seguretat documental de factura electrònica.
- Estàndard tècnic de seguretat documental d'expedient indexat.
- Estàndard tècnic de gestió d'objectes de signatura electrònica.

7.2. La normativa d'autenticació

La normativa d'autenticació concreta el conjunt de normes per a l'autenticació d'una persona per mitjans electrònics emprant certificats de clau pública i altres mecanismes criptogràfics i no criptogràfics.

Aquesta normativa permet el compliment de les seccions 9.1.2, 10.6.2, 10.8.2, 10.9.1, 11.2.3, 11.3.3, 11.4.2, 11.4.3, 11.5.2, 11.5.4, 11.5.6, 11.7.1 i 12.3.1 de la norma ISO/IEC 27002:2005. Es desplega en forma d'estàndards obligatoris referits a nivells d'autenticació (alt, mitjà, baix) i estàndards de mecanismes d'autenticació, en guies per a l'aplicació de mecanismes d'autenticació i en procediments operatius.

Els actes electrònics, així com els accessos a sistemes d'informació, s'han de dur a terme dins un marc de treball que imposi l'autenticació dels usuaris.

Han d'existir una o diverses normatives d'autenticació per escrit (o en suport informàtic), signades degudament (quan s'escaigui, electrònicament), que determinin les condicions de seguretat que cal aplicar als procediments d'autenticació.

En alguns casos, el mecanisme d'autenticació pot fer ús de mecanismes criptogràfics basats en certificats digitals X.509v3.

Els continguts principals són els següents:

- Informació general.

    - Identificació de la normativa, consistent en identificació numèrica i títol textual corresponent a la normativa.
    - Data d'emissió.
    - Identificació de l'emissor de la normativa.
    - Període de validesa de la normativa, amb indicació de l'entrada en vigor i la durada (si s'escau, indefinida).
    - Àmbit d'aplicació de la normativa, amb indicació de l'objectiu (a què s'aplica la normativa) i el subjectiu (a qui s'aplica la normativa).

- Identificació.

    - Quines dades del certificat seran emprades per a la identificació de la persona o l'entitat que s'autentica.
    - Per exemple, es podria indicar que la identificació es farà mitjançant la dada NIF continguda al SubjectName del certificat. També es podrien establir normes relatives a la identificació practicada pel prestador que va emetre el certificat.

- Autenticació.

    - Normes relatives a protocols i algorismes. Per exemple, es podria indicar que l'autenticació es realitzarà emprant TLS 1.0, amb determinats algorismes d'intercanvi de claus i de xifratge.
    - Normes relatives a l'ús de prestadors de serveis de certificació, en què s'indiquin els certificats admesos que es consideren vàlids per a aquesta acció d'autenticació, així com els prestadors autoritzats corresponents.
    - Quan s'escaigui, cal indicar el nivell de classificació de CATCert sobre els certificats admesos.
    - Normes sobre els punts fiables per a la construcció de rutes de certificats vàlids, com ara les identificacions de les entitats de certificació arran dels prestadors admesos, com també normes sobre la gestió d'aquests certificats.
    - Normes sobre les rutes de certificació, amb la indicació de si es podran establir altres models de confiança diferents del jeràrquic.
    - Normes relatives a l'ús de la informació d'estat dels certificats, indicant l'obligatorietat de verificar la signatura electrònica i la forma de fer-ho entre les opcions següents:

- Ús de l'entitat de validació de CATCert (administracions públiques catalanes) o altres (sector privat).
- Ús de llistes de revocació de certificats emeses pel prestador de serveis de certificació.
- Ús del servei de consulta en línia de certificats (OCSP) del prestador de serveis de certificació, quan estigui disponible.
- Ús d'altres mecanismes de consulta d'estat de certificats, quan aquests estiguin disponibles (consulta web al Registre de certificats).

Algunes aplicacions de la norma són les següents:

- Estàndard tècnic d'autenticació web (SSL/TLS).
- Estàndard tècnic d'autenticació de serveis web (WSS).

7.3. La normativa de signatura electrònica

La normativa de signatura electrònica defineix com s'ha de generar la signatura, amb quins certificats, quins controls s'aplicaran per verificar els permisos i els privilegis, si la signatura se segellarà amb la data i l'hora, de quina manera es verificaran els certificats, quins algorismes es podran emprar per signar i, molt especialment, què vol dir legalment l'acte de signar i quins controls de programari s'aplicaran per garantir l'autenticitat de la voluntat del signatari.

La normativa es desplega en forma d'estàndards tècnics de nivells de signatura (alt, mitjà, baix) i estàndards de signatura per als diferents tipus d'actes, en guies de signatura (PDF, ODF, Word, WS, S/MIME…) i procediments de signatura.

Els actes i les manifestacions de voluntat efectuats amb mitjans electrònics, quan generen documents amb rellevància per al procediment administratiu, s'han de signar electrònicament.

Han d'existir una o diverses normatives de signatura electrònica per escrit (o en suport informàtic), signades degudament (quan s'escaigui, electrònicament), que determinin les condicions de seguretat que cal aplicar als procediments de signatura electrònica.

La normativa de signatura electrònica ha de fer ús de mecanismes criptogràfics basats en certificats digitals X.509v3 (normativa de signatura electrònica avançada) i, quan

s'escaigui, emprar dispositius segurs de creació de signatura electrònica (normativa de signatura electrònica reconeguda).

Els continguts principals són els següents:

- Informació general:

    - Identificació de la normativa, consistent en identificació numèrica i títol textual corresponent a la normativa.
    - Data d'emissió.
    - Identificació de l'emissor de la normativa.
    - Període de validesa de la normativa, amb indicació de l'entrada en vigor i la durada (si s'escau, indefinida).
    - Àmbit d'aplicació de la normativa, amb indicació de l'objectiu (a què s'aplica la normativa) i el subjectiu (a qui s'aplica la normativa).

- Significat i manifestacions vinculants:

    - Descriu què vol dir, fàcticament i legalment, el fet de produir una signatura electrònica, així com altres manifestacions col·laterals, en especial referides al suport normatiu a la signatura electrònica o a l'acte i al reconeixement corresponent.
    - És la manifestació semàntica explícita de l'acte i el compromís (resoldre favorablement), i permet identificar de manera automàtica els documents en consideració als tipus d'acte (molt important a l'efecte del manteniment de la validesa de la signatura).

- Normes sobre aportació de dades de verificació de signatura, pel signatari o, quan s'escaigui, per terceres persones, incloent-hi:

    - El document o el registre de transacció a signar.
    - La identificació del signatari, en forma de certificat digital.
    - La data i l'hora de l'acte.
    - La identificació de la política de signatura electrònica aplicable.
    - La verificació de la signatura, en forma documentada.
    - Les evidències que sustenten la verificació practicada (com llistes de revocació de certificats, consultes OCSP o informes de l'entitat de validació de CATCert).
    - La data i l'hora de la verificació de la signatura.

- Validació de signatura:

- Normes relatives a protocols i algorismes. És molt important alinear-les amb les recomanacions del CNI-CCN-CERT en matèria de signatura electrònica (Guia CCN-STIC-405).
- Normes relatives a l'ús de prestadors de serveis de certificació, en què s'indiquin els certificats admesos que es consideren vàlids per a aquesta acció d'autenticació, així com els prestadors autoritzats corresponents.
- Quan s'escaigui, cal indicar el nivell de classificació de CATCert sobre els certificats admesos.
- Normes sobre els punts fiables per a la construcció de rutes de certificats vàlids, com ara les identificacions de les entitats de certificació arran dels prestadors admesos, com també normes sobre la gestió d'aquests certificats.
- Normes sobre les rutes de certificació, amb la indicació de si es podran establir altres models de confiança diferents del jeràrquic.
- Normes relatives a l'ús de la informació d'estat dels certificats, indicant l'obligatorietat de verificar la signatura electrònica i la forma de fer-ho entre les opcions següents:

    - Ús de l'entitat de validació de CATCert (administracions públiques catalanes) o altres (sector privat).
    - Ús de llistes de revocació de certificats emeses pel prestador de serveis de certificació.
    - Ús del servei de consulta en línia de certificats (OCSP) del prestador de serveis de certificació, quan estigui disponible.
    - Ús d'altres mecanismes de consulta d'estat de certificats, quan aquests estiguin disponibles (consulta web al Registre de certificats).

- Normes sobre l'ús de rols, indicant si s'utilitzen i s'indiquen dins la signatura electrònica i, en cas afirmatiu, si són rols al·legats que caldrà comprovar o si són rols certificats:

    - En aquest segon cas, caldrà implantar una entitat de certificació d'atributs que emeti els certificats corresponents.
    - Normalment aquesta possibilitat no s'empra, tot i que complementa l'ús de certificats generalistes.

- Ús del segellament de data i hora, i d'altres informacions relatives al temps:

- La necessitat o no d'emprar segells de data i hora criptogràfics, i, en cas afirmatiu, el format i la normativa tècnica i jurídica aplicables al segell de data i hora.
- La necessitat que la manifestació de la data i l'hora referida anteriorment s'incorpori com un atribut a la signatura electrònica, i si aquest atribut se signarà o no.
- La necessitat que altres accions sobre una signatura —com ara la verificació d'aquesta— incorporin segells de data i hora o altres manifestacions sobre la data i l'hora de l'acció corresponent.
- La precisió i la qualitat de la manifestació de la data i de l'hora, com també la sincronització de les fonts de temps fiables amb l'hora UTC.

- Altres normes:

  - Normes sobre formats de signatura electrònica (PKCS#7/CMS o XMLDSig/XAdES).
  - Impressió del document signat electrònicament (codi de verificació electrònica).
  - Visualització gràfica de la signatura electrònica abans i després de la verificació.

Algunes aplicacions de la norma són les següents:

- Estàndard tècnic de signatura electrònica d'actes de voluntat (definitius/tràmit).
- Estàndard tècnic de signatura electrònica d'actes de judici.
- Estàndard tècnic de signatura electrònica d'actes de coneixement.
- Estàndard tècnic de signatura electrònica d'actes de desig.
- Estàndard tècnic de signatura electrònica de format documental PDF.

7.4. La normativa de xifratge

La normativa de xifratge concreta el conjunt de normes per al xifratge de comunicacions i documents per mitjans electrònics emprant certificats de clau pública i altres mecanismes criptogràfics, de conformitat amb la secció 12.3.1 de la norma ISO/IEC 27002:2005.

La normativa es desplega en forma d'estàndards de nivell de confidencialitat (alt, mitjà, baix), estàndards de mecanismes de xifratge o guies de xifratge (recomanacions en relació amb el xifratge).

Les informacions sensibles, així com les que continguin dades personals de nivell alt, s'han de xifrar per tal de protegir-ne la confidencialitat.

Han d'existir una o diverses normatives de xifratge per escrit (o en suport informàtic), signades degudament (quan s'escaigui, electrònicament), que determinin les condicions de seguretat que cal aplicar als mecanismes de xifratge.

En alguns casos, el mecanisme de xifratge pot fer ús de mecanismes criptogràfics basats en certificats digitals X.509v3.

Els continguts principals són els següents:

- Informació general.
    - Identificació de la normativa, consistent en identificació numèrica i títol textual corresponent a la normativa.
    - Data d'emissió.
    - Identificació de l'emissor de la normativa.
    - Període de validesa de la normativa, amb indicació de l'entrada en vigor i la durada (si s'escau, indefinida).
    - Àmbit d'aplicació de la normativa, amb indicació de l'objectiu (a què s'aplica la normativa) i el subjectiu (a qui s'aplica la normativa).
- Xifratge.
    - Normes relatives a protocols i algorismes. Per exemple, es podria indicar que el mecanisme a emprar és XML Encryption, amb determinats algorismes de xifratge.
    - Normes relatives a l'ús de prestadors de serveis de certificació, en què s'indiquin els certificats admesos que es consideren vàlids per a aquesta acció d'autenticació, així com els prestadors autoritzats corresponents
    - Quan s'escaigui, cal indicar el nivell de classificació de CATCert sobre els certificats admesos.
    - Normes sobre els punts fiables per a la construcció de rutes de certificats vàlids, com ara les identificacions de les entitats de certificació arran dels prestadors admesos, com també normes sobre la gestió d'aquests certificats.
    - Normes sobre les rutes de certificació, amb la indicació de si es podran establir altres models de confiança diferents del jeràrquic.

- Normes relatives a l'ús de la informació d'estat dels certificats, indicant l'obligatorietat de verificar la signatura electrònica i la forma de fer-ho entre les opcions següents:

    - Ús de l'entitat de validació de CATCert (administracions públiques catalanes) o altres (sector privat).
    - Ús de llistes de revocació de certificats emeses pel prestador de serveis de certificació.
    - Ús del servei de consulta en línia de certificats (OCSP) del prestador de serveis de certificació, quan estigui disponible.
    - Ús d'altres mecanismes de consulta d'estat de certificats, quan aquests estiguin disponibles (consulta web al Registre de certificats).

Algunes aplicacions de la norma són les següents:

- Estàndard tècnic de xifratge SSL/TLS/WTLS.
- Estàndard tècnic de xifratge de serveis web (WSS).
- Estàndard tècnic de xifratge CMS.
- Estàndard tècnic de xifratge XML.

7.5. La normativa d'evidència electrònica

La normativa d'evidència electrònica concreta el conjunt de normes per a la producció i la gestió de tot el cicle de vida dels registres d'activitat a l'efecte de disposar de registres amb valor probatori suficient (BS 10008:2008), sobretot en el cas de les actuacions no formalitzades documentalment (NIST SP 800-92).

La normativa es desplega en forma d'estàndards de gestió de registres d'activitat (*logs*) per a la publicació d'informacions o els registres interns, en procediments d'evidència electrònica i en guies d'aplicació de la normativa d'evidència electrònica, amb recomanacions.

Els continguts principals són els següents:

- Generació i captura d'evidències.

    - Interpretació i extracció de dades.
    - Filtratge d'esdeveniments.

  - Agregació d'esdeveniments.

- Emmagatzematge d'evidències.

  - Rotació de registres.
  - Arxivament, incloent-hi la retenció i la preservació.
  - Compressió de registres.
  - Reducció de registres.
  - Conversió de registres.
  - Normalització de registres.
  - Comprovació d'integritat de registres.

- Anàlisi d'evidències.

  - Correlació d'esdeveniments.
  - Revisió de registres de seguretat.
  - Informes sobre registres de seguretat.
  - Informes d'evidència.

- Disposició (eliminació) dels registres de seguretat.

7.6. La normativa de certificació

La normativa de certificació defineix com cal prestar el servei de certificació. N'han de disposar els prestadors de serveis de certificació per als seus propis serveis, o els usuaris, per definir els requisits i les condicions que exigiran als prestadors que els subministrin certificats (adquisició o admissió de certificats).

La normativa es desplega en forma d'estàndards de certificació, tipus de certificats a adquirir o admetre —incloent-hi certificats de persona física, certificats de persona jurídica, certificats d'entitat sense personalitat, certificats de segell d'òrgan...—, de procediment d'admissió de certificats, procediments d'adquisició de certificats, i en una base dades de certificats admesos.

Els continguts principals són els següents:

- Informació general

  - Presentació

        - Tipus i classes de certificats
        - Relació entre la normativa de certificació i altres documents

    - Nom del document i identificació
    - Comunitat d'usuaris de certificats, d'acord amb la llei aplicable (p. ex., Llei 11/2007)

        - Prestadors de serveis de certificació
        - Entitats de registre
        - Subscriptors i entitat usuària dels certificats

    - Ús dels certificats
        - Tal vegada l'aspecte més important és definir adequadament per a quina finalitat ha de servir —s'admet— l'ús de cada tipus de certificat descrit anteriorment.
        - Per exemple, ús general en el procediment administratiu, ús tributari o autoritzacions d'ús específiques per a certificats d'entitat sense personalitat jurídica.

    - Administració de la normativa

        - Organització que administra l'especificació
        - Dades de contacte de l'organització
        - Procediment d'aprovació

- Requisits d'operació del cicle de vida dels certificats

    - Sol·licitud d'emissió de certificat

        - Legitimació per sol·licitar l'emissió
        - Procediment d'alta; responsabilitats

    - Acceptació del certificat
    - Ús del parell de claus i del certificat
    - Renovació de certificats sense renovació de claus
    - Renovació de certificats amb renovació de claus
    - Modificació de certificats
    - Revocació i suspensió de certificats

        - Causes de revocació de certificats
        - Legitimació per sol·licitar la revocació

        - Obligació de consulta d'informació de revocació de certificats
        - Causes de suspensió de certificats
        - Qui pot sol·licitar la suspensió

    - Serveis de comprovació d'estat de certificats

        - Característiques dels serveis
        - Disponibilitat dels serveis

    - Finalització de la subscripció

- Perfils de certificats i llistes de revocació de certificats

    - Perfils de certificats admesos

        - Formats de noms
        - Restriccions de noms

    - Perfil de la llista de revocació de certificats

- Requisits legals

    - Obligacions i responsabilitat civil

        - Subscriptors dels certificats
        - Entitat usuària dels certificats, en la seva actuació com a tercer

    - Protecció de dades personals
    - Conformitat amb la llei aplicable

7.7. La normativa de gestió de claus

La normativa de gestió de claus detalla les normes d'ús en relació amb les claus criptogràfiques, d'acord amb la normativa de seguretat criptogràfica, per complir els controls que preveu la norma ISO/IEC 27002:2006, seccions 12.3.1 i 15.1.6, i sobre la base de les recomanacions de millors pràctiques contingudes a la publicació especial 800-57, parts 1 i 2, del NIST (EUA).

La normativa es desplega en forma d'estàndards d'infraestructura tècnica de gestió de claus, procediments previs a les operacions de gestió de claus, procediments operatius de gestió de claus i procediments posteriors de gestió de claus.

Totes les claus criptogràfiques s'han de protegir de la modificació, la pèrdua o la destrucció. Les claus criptogràfiques privades i les claus secretes s'han de protegir contra la divulgació no autoritzada.

El maquinari emprat per generar, emmagatzemar i arxivar les claus criptogràfiques s'hauria de protegir físicament.

Els continguts principals són els següents:

- Estàndards, procediments i mètodes segurs en relació amb aquests aspectes:

    - Generació de claus per diferents sistemes criptogràfics i aplicacions.
    - Generació i obtenció de certificats de clau pública.
    - Distribució de claus als usuaris, incloent-hi l'activació un cop hagin estat rebudes.
    - Emmagatzematge de claus, incloent-hi la manera com obtenen accés a les claus els usuaris autoritzats.
    - Canvi o actualització de claus, incloent-hi normes sobre el moment en què cal canviar o actualitzar les claus i el procediment aplicable.
    - Gestió de claus compromeses.
    - Revocació de claus, incloent-hi la retirada o la desactivació.
    - Arxivament de claus, especialment en cas d'informació xifrada que hagi estat arxivada.
    - Destrucció de claus.
    - Registre i auditoria d'operacions relatives a gestió de claus.

- Períodes d'activació i desactivació de claus, per reduir el risc de compromís, de manera que les claus es puguin emprar només durant un termini concret, d'acord amb les circumstàncies i l'anàlisi de risc.

- Procediments per garantir l'autenticitat de les claus públiques mitjançant entitats de certificació.

- En cas que hi hagi tercers prestadors de serveis relacionats amb la criptografia, cal establir acords de nivell de servei que tractin específicament qüestions de responsabilitat, fiabilitat dels serveis i temps de resposta garantits.

7.8. La normativa de seguretat criptogràfica

La normativa de seguretat criptogràfica especifica normes d'ús en relació amb la criptografia, incloent-hi estàndards per a la seva implementació a l'organització, amb l'objectiu de complir els controls que preveu la norma ISO/IEC 27002:2006, seccions 12.3.1 i 15.1.6, i sobre la base de les recomanacions de millors pràctiques contingudes a la publicació especial 800-57, parts 1 i 2, del NIST (EUA), com també de les guies STIC del CNI.

La normativa es desplega en forma d'estàndards d'implementació d'infraestructura criptogràfica, estàndards i procediments en relació amb els algorismes segurs, estàndard de codi segur de verificació i guies d'ús de la criptografia en les aplicacions, amb recomanacions conformes a la legislació aplicable.

Els continguts principals són els següents:

- L'aproximació de la direcció respecte a l'ús de controls criptogràfics dins l'organització, incloent-hi els principis generals de protecció de la informació.

- El nivell requerit de protecció, d'acord amb l'anàlisi de risc corresponent, tenint en compte el tipus, la fortalesa i la qualitat dels algorismes criptogràfics corresponents.

- Ús del xifratge per a la protecció d'informacions sensibles transportades mitjançant dispositius mòbils, amb mitjans o dispositius que es poden remoure o per línies de comunicació.

- Aproximació a la gestió de claus, incloent-hi els mètodes per tractar la protecció de les claus criptogràfiques i la recuperació d'informació xifrada en cas de pèrdua, compromís o dany de les claus.

- Determinació dels rols i les responsabilitats relacionats amb els aspectes següents:

    - Implementació de la normativa.
    - Gestió de claus, incloent-hi la generació de claus.

- Els estàndards per aconseguir la implementació efectiva de la normativa en tota l'organització, mitjançant controls tècnics i de procediment.

- La valoració d'impacte de l'ús d'informació xifrada sobre controls basats en inspecció de continguts, com ara antivirus.

- Aspectes legals:

    - Restriccions sobre la importació i/o l'exportació de maquinari i programari que executen operacions criptogràfiques.
    - Restriccions sobre la importació i/o l'exportació de maquinari i programari dissenyats perquè s'hi incorporin funcions criptogràfiques.
    - Restriccions sobre l'ús del xifratge.
    - Mètodes obligatoris o voluntaris que permeten a les autoritats públiques l'accés a informacions xifrades emprant maquinari o programari per garantir-ne la confidencialitat.