Treballs de recerca | 2011-2012

# ASPECTES JURÍDICS DE LA PRESTACIÓ DE SERVEIS PÚBLICS EMPRANT COMPUTACIÓ AL CLOUD

Nacho Alamillo Domingo i Xavier Urios Aparisi

Barcelona 2012

Generalitat de Catalunya
**Escola d'Administració Pública de Catalunya**



# Aspectes jurídics de la prestació de serveis públics emprant computació al Cloud

Autors del treball:

Nacho Alamillo Domingo
Investigador del Grup de Recerca de Governança del Risc (GRISC) de la Universitat Autònoma de Barcelona

Xavier Urios Aparisi
Cap de l'assessoria jurídica, departament de Governació i Relacions Institucionals de la Generalitat de Catalunya

2012

## Resum

L'administració electrònica s'ha convertit en una de les àrees de recerca i aplicació més importants en l'àmbit del Dret Administratiu, tant des de la perspectiva de la millor organització dels recursos de les administracions públiques com des de la perspectiva de l'increment de l'eficiència i de l'eficàcia en l'acció pública; espai de recerca que s'ha ampliat progressivament amb l'aparició de les actuacions de reutilització de la informació del sector públic, especialment en l'àmbit de l'anomenat "govern obert" i dels nous models de virtualització de la computació, sota el paradigma del Cloud (núvol).

No obstant això, aquesta ampliació és paral·lela al naixement de nous reptes, davant la incorporació d'àmbits d'actuació fins ara desconeguts. En aquest sentit, el trànsit de la tramitació presencial a la tramitació electrònica ja ha suposat un important canvi en les relaciones jurídiques. En particular, en l'àmbit d'actuació de les administracions públiques s'ha produït un rellevant canvi de model, que actualment es troba en desenvolupament, i que ha justificat el canvi de models organitzatius i de models normatius; amb la necessària adaptació de l'actuació administrativa i de la normativa que li dona cobertura. Igualment, l'avenç de la tecnologia suposa igualment l'aparició de noves possibilitats tècniques que, sota el paràmetre de reducció de costos i agilitat, permeten donar un pas endavant en relació amb determinades necessitats que tenen les administracions públiques, com és el tractament, desenvolupament i conservació tant de la informació que generen, com de les aplicacions o programes que utilitzen per actuar.

Així el Cloud és una d'aquestes eines, que permet el tractament a distància d'aquests elements, amb els avantatges que en suposa però, al mateix temps, amb els riscos que se'n deriven, un dels quals és la pèrdua de la capacitat de control que la majoria de les solucions que s'adoptin pot suposar. Aquesta absència de control de les informacions genera importants problemes jurídics, tant des de la perspectiva de la privacitat o protecció de dades personals, com des de la perspectiva de les dades gestionades per l'Administració pública.

En ambdós casos, resulta imprescindible establir pràctiques de negoci, suportades en solucions tecnològiques solvents, per garantir el control sobre la ubicació de les dades i informacions en el Cloud, a efectes del compliment de les normes jurídiques aplicables en cada cas, així com per limitar l'exposició de les dades a entorns hostils.

En aquest projecte s'ha realitzat una revisió detallada de la problemàtica apuntada, de les propostes tecnològiques i el seu estat de maduresa, i, a partir d'aquestes, s'han explotat les oportunitats que ofereixen les tecnologies per establir millors pràctiques que permetin el establiment de controls efectius per a la gestió i protecció de les dades en el Cloud i, en conseqüència, facilitin el compliment de la regulació aplicable en cada cas.

Com a resultats principals de la recerca, s'han identificat els principals riscos legals, s'han recollit recomanacions per al correcte tractament dels mateixos i s'han desenvolupat instruments contractuals i normatius per facilitar a les Administracions Públiques l'adopció dels diferents tipus i modalitats de serveis de *Cloud computing*.

A títol d'exemple de la rellevància del Cloud Computing, un estudi realitzat per Avanade[1] al juny del 2011 indica que s'està produint un important creixement dels serveis públics al Cloud. Aquest estudi, d'ara ja fa un any, constata que actualment un 74% de les empreses està utilitzant alguna forma de servei al Cloud (el que suposa un increment del 23% respecte a un estudi de l'any 2009). A més, de les empreses que encara no disposen d'aquest servei, tres quartes parts manifesten que està en els seus plans implementar serveis al Cloud.

A més, l'estudi indica que el 35 per cent de les empreses nord-americanes enquestades han experimentat nivells perceptiblement més alts de seguretat des que es van mudar al Cloud. Igualment, el 32 per cent manifesta que ha de dedicar menys temps a preocupar-se per l'amenaça d'atacs cibernètics, el que suposa un estalvi de temps en l'administració de la seguretat en comparació amb les empreses que no utilitzen el Cloud, així com de mitjans de seguretat, pel que fa a aquells que ja són gestionats o integrats al propi Cloud. Les empreses també posen de manifest que un dels elements més rellevants del Cloud és la seva flexibilitat, el que permet a les empreses estructurar-se per satisfer amb precisió les seves necessitats presents i futures.

En qualsevol cas, tal com s'exposarà al present treball de recerca, a l'hora d'implementar serveis al Cloud cal tenir present que s'han de definir prèviament els objectius a aconseguir, ja sigui en la prestació del propi servei o en la gestió d'aquest, determinants quines són les aplicacions o informació que es vol traslladar al Cloud, i avaluar els requeriments tecnològics que s'han de complir. A més, quan es tracta de les Administracions Públiques, aquestes qüestions que es relacionen amb el que seria estrictament el model de negoci s'han de conjuminar igualment amb els requeriments legalment exigibles, com a conseqüència de que ens trobem en l'àmbit del Dret públic, en què els requeriments legals a complir són més exigents comparativament amb els que es produeixen en l'àmbit del dret privat.

Així, a diferència del que passa en l'àmbit del dret privat, les Administracions Públiques estan sotmeses a uns límits que condicionen l'actuació administrativa. Aquests límits són de naturalesa essencialment interna, però també tenen o poden tenir una transcendència externa.

Pel que fa als primers, és necessària l'adaptació de les estructures organitzatives per una adequada incorporació del Cloud, el que es trasllada no tan sols al que és estrictament mitjans materials, sinó que també s'han de preparar o formar a les persones en les particularitats que se'n deriven de la prestació de serveis al Cloud. Igualment cal tenir present que la contractació de serveis al Cloud es troba sotmesa a la normativa de contractes del sector públic, el que requereix

[1] Avanade és una joint venture entre Accenture i Microsoft que es va fundar al 2000 per a prestar serveis de consultoria al voltant de Microsoft.

una tasca prèvia de qualificació del contracte, abans d'aplicar les singularitats del règim jurídic que es pugui derivar d'aquesta determinació prèvia, així com tota la tramitació administrativa que és exigible.

Finalment, caldrà tenir present la vessant externa, el que exigirà el seguiment de les condicions externes de prestació del servei i, si s'escau, l'adaptació de la normativa que li dona empara. Això també suposarà la necessària adaptació de la normativa, o adopció de les decisions singulars, que permetin garantir que la prestació de serveis es produeix amb plenes garanties jurídiques, amb estricte compliment del principi de legalitat, i sense que es produeixi cap reducció de les garanties de que el ciutadà disposa quan es relaciona amb una Administració Pública.

Índex del treball

# 1 Caracterització del *Cloud computing*

L'enorme creixement de la web en l'última dècada ha donat lloc a una nova classe de problemes "a escala Web" en l'àmbit de les relaciones juridicoadministratives. En aquest sentit, no tan sols en l'àmbit privat sinó també en l'àmbit públic, els mitjans electrònics comencen a ser una eina habitual per relacionar-se i, en línia amb aquesta situació, cada vegada són més els continguts que es troben a la web. Igualment, sorgeixen reptes com el suport a milers de e-transaccions comercials concurrents o milions de recerques al dia.

En resposta, les empreses de tecnologia han creat centres de dades cada vegada més grans, que han propiciat la consolidació d'un gran nombre de servidors (centenars, si no milers) amb la corresponent infraestructura associada d'emmagatzematge, xarxes i refrigeració, amb la finalitat de gestionar aquesta demanda creixent. Amb els anys, les empreses de tecnologia, especialment les empreses d'Internet, com Google, Amazon, eBay o Yahoo, han assolit una enorme quantitat d'experiència en l'operació d'aquests centres de dades enormes, en termes de desenvolupament de la tecnologia, la infraestructura física necessària, la gestió de processos, i altres intangibles.

El *Cloud computing* suposa un pas endavant, amb la comercialització d'aquests desenvolupaments. Abans de la seva aparició, l'adquisició d'aquests recursos – la inversió de capital inicial en la compra dels equips propis i els importants recursos dedicats a l'establiment i manteniment de la infraestructura – era una qüestió costosa i difícil per a les organitzacions i simplement inassolible per als individus. Avui en dia, una vegada es pot considerar que el *Cloud computing* s'ha estès, s'ha posat de manifest que la computació en núvol té un gran potencial a l'hora de beneficiar tant als proveïdors i usuaris. D'una banda, els proveïdors de *Cloud* poden obtenir fonts addicionals d'ingressos i són capaços de comercialitzar els seus enormes centres de dades i l'experiència de la gestió de dades a gran escala. El cost total es redueix a través de la consolidació, mentre que la inversió de capital en infraestructura física s'amortitza amb serveis prestats a molts clients (JAEGER *et al*., 2009); d'altra banda, els usuaris poden accedir a uns serveis amb un alt grau d'eficiència amb un cost assumible.

El *Cloud computing* és, per tant, una nova manera de facilitar recursos de computació, no una nova tecnologia. Ara els serveis de computació, des de l'emmagatzematge i processament de dades fins al programari, com la gestió del correu electrònic, estan disponibles de forma instantània, sense compromís i sota demanda. Per a BALBONI, 2010: p. 3, suposa l'expressió definitiva de la externalització.

Igualment, no es pot deixar de banda el context econòmic actual, ja que estem en un moment en què cal estrènyer-se el cinturó i cercar les màximes eficiències econòmiques. Per aquesta raó aquest nou model econòmic de computació està assolint un alt grau de penetració en el mercat i està sent objecte d'una inversió global enorme (CATTEDDU i HOGBEN, 2009a: p. 4).

En paraules de GLOTT *et al*., 2011: p. 209, s'espera que el Cloud computing sigui una tecnologia troncal de la Internet del Futur que ofereixi accés a escala d'Internet i orientat a servei a computació, emmagatzematge de dades i recursos de la xarxa virtualitzats, així com serveis de major nivell. En contrast amb el mercat del núvol actual que es caracteritza principalment per proveïdors de *Cloud computing* aïllats, s'espera que la Internet del Futur es caracteritzi per una federació de capacitats Cloud de proveïdors independents transparent – semblant a la interconnexió de xarxa i la compra de trànsit IP pels ISP a la Internet actual.

Com indica l'estudi d'INTECO sobre el *Cloud computing* al sector públic d'Espanya, la implantació del *Cloud computing* sorgeix en un context de forta recessió econòmica internacional, marcat per la necessitat d'estalviar costos i impulsar la competitivitat de les empreses i administracions públiques a través de les TIC.

El *Cloud computing* pot arribar a generar un impacte econòmic, a través de la suma de les 5 principals economies europees, de 763.000 milions d'euros en el període 2010-2015. Aquest impacte econòmic seria el resultat conjunt d'una sèrie de factors: desenvolupament i creació de nous negocis, estalvi de costos operacionals, creació de més de 2,3 milions de llocs de treball directes i indirectes en aquest període i efectes multiplicadors sobre altres sectors de l'economia.

Conscients d'aquest potencial benefici econòmic, i de moltes altres avantatges que pot aportar el *Cloud*, les institucions de la Unió Europea han reconegut en la nova Agenda Digital Europea la necessitat d'impulsar el desenvolupament del mercat del *Cloud computing*. Per això es postula la directriu de desenvolupar una Estratègia Europea del *Cloud* que ha d'impulsar un mercat comú de serveis tecnològics que permeti a Europa competir amb el mercat internacional de les TIC, on actualment predomina un fort posicionament de les empreses nord-americanes (INTECO, 2012: p. 37).

També un recent informe de la ONTSI, 2012: pp. 39-42, identifica avantatges del *Cloud computing* des de la perspectiva de les Administracions Públiques. En concret, indica que poden beneficiar-se dels avantatges i models de negoci potencials del *Cloud computing*. Una entitat pública (Comunitat Autònoma, Administració local, etc.) ha de gestionar la seva funció pública prestant serveis de valor al ciutadà, gestionar recursos públics, relacionar-se amb proveïdors, contractar, produir, etc. de la mateixa manera que una empresa privada, pel que pot aplicar les tecnologies de *Cloud* en la seva cadena de valor més eficient i competitiva (qüestió cada vegada més demandada pels mercats i ciutadans).

És obvi dir que, el núvol (sigui privat o públic) està cridat a ser una de les palanques de modernització i desenvolupament de les administracions per assumir tots aquests reptes durant els propers anys.

L'estalvi de costos tecnològics, la flexibilitat i escalabilitat, la possibilitat del accés a les tecnologies de les administracions més petites i amb menys recursos, la sostenibilitat energètica, etc. són factors comuns de benefici directe de l'adopció del *Cloud computing*, però hi ha molts factors en els que aquest model de servei pot ser de gran utilitat en el desenvolupament de les polítiques públiques i competències atribuïdes com a pròpies i diferencials per a aquest sector:

- El *Cloud computing* es pot conformar com un instrument de facilitació per el desenvolupament i manteniment de polítiques públiques que requereixen un suport tecnològic intensiu, i que no podrien assumir-se en l'escenari econòmic actual en condicions tradicionals: la internacionalització de les empreses, l'administració electrònica, el govern obert, la modernització de la sanitat i educació, etc. requeriran de fortes inversions pressupostàries i de recursos que poden esmorteir si les administracions aposten pels models de *Cloud computing*. Concretament, el *Cloud computing*, pot realitzar aportacions rellevants en les següents polítiques públiques:

    - Polítiques per a la millora de competitivitat de les pimes espanyoles a través de les TIC a través de solucions SaaS en mode de Programari de fonts obertes.

    - Polítiques per a la internacionalització de les pimes espanyoles a través del desenvolupament de mercats electrònics i el desplegament de infraestructures i solucions de comerç electrònic a través de models *Cloud*.

    - Polítiques de transparència, administració electrònica i govern obert, a través de plataformes de open data, portals de participació, etc. El desplegament intensiu d'aquests serveis durant els darrers anys a les administracions espanyoles ha generat un nou paradigma de servei per les àrees d'IT dels organismes públics: els ciutadans es converteixen en usuaris dels recursos tecnològics de les administracions i han de rebre un servei d'alta disponibilitat i rendiment. El *Cloud computing* és una bona alternativa per donar una resposta eficient a l'elasticitat i requeriments de la demanda de serveis electrònics per part dels ciutadans.

- La gestió de polítiques públiques i serveis com la sanitat o l'educació, molt exigents en demanda social i de recursos assignats, són àmbits en què el *Cloud* podria tenir una irrupció i benefici immediat, tant en l'estalvi de costos tecnològics com en la possibilitat de migrar serveis molt costosos en l'actualitat i implementar altres nous a través d'entorns *Cloud* (per plataformes d'e-learning, xarxes de professionals, integració hospitalària, xarxes de pacients, monitorització, telemedicina, etc.).

- La interoperabilitat de la gran quantitat d'informació controlada i emmagatzemada per les administracions i organitzacions públiques. Aquest ampli volum d'informació, al costat de la multiplicitat de sistemes, l'elevat nivell d'estanqueïtat dels mateixos i la informació redundant present en aquests sistemes, fa possible disposar d'un gran marge de millora en temes de eficiència, reducció de costos, i atenció al públic. Per això, una estratègia de

serveis *Cloud* compartits entre diferents organitzacions sota un model d'estandardització tecnològica basada en l'Esquema Nacional de Interoperabilitat permetria un desenvolupament més eficient de les directives i compromisos europeus i nacionals adquirits en aquest àmbit.

- Les directrius d'austeritat i control del dèficit requereixen d'un exhaustiu estalvi de costos de les administracions en totes les línies de despesa corrent i inversió. La despesa tecnològica és molt significativa en moltes administracions i pot ser clarament continguda i reduïda en un temps raonable a través de models de *Cloud computing* gràcies a l'optimització en l'ús dels actius tecnològics.

- A Espanya, el model *Cloud* pot facilitar la generalització dels serveis transversals a tota l'Administració, amb la consegüent millora de la eficiència i la major reutilització de la infraestructura tecnològica de les Administracions Públiques. La tendència en aquest sentit apunta a una progressiva re-definició de l'estructura administrativa cap a centres de serveis compartits més eficients en producció i costos que, de manera gradual, configuraran xarxes privades (o públiques) de serveis comuns a altres unitats i òrgans administratius.

- El model *Cloud* pot posar a l'abast de les entitats locals, típicament menys dotades de recursos tecnològics i humans, mitjans eficients per a la modernització administrativa dels seus processos.

En qualsevol cas, aquesta incorporació del *Cloud* en l'àmbit públic no es pot dur a terme de manera mimètica al que està passant en l'àmbit privat. Tot i que els avantatges abans indicats són aplicables totalment a l'actuació administrativa, no es pot deixar de banda que les administracions públiques actuant per raons d'interès general, i aquesta actuació suposa l'existència d'una sèrie de filtres o requeriments que s'han de tenir en compte, no tan sols en el moment d'adquisició del *Cloud*, sinó especialment en la prestació de serveis públics que es duguin a terme i en els que s'utilitzi aquesta tecnologia o infraestructura en l'àmbit dels serveis públics.

La potestat autoorganitzativa és un dels elements més definidors de l'autonomia d'una administració pública. Però aquesta potestat no es pot exercir de manera indiscriminada, sinó que es troba sotmesa a una sèrie de condicionants, entre els quals es troba el concepte de competència.

Igualment, i a diferència del que passa en l'àmbit del dret privat, les administracions públiques es troben sotmeses a la teoria de la vinculació positiva, el que suposa que tal com veurem, s'entén prohibit per 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.

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

Ja l'Exposició de Motius de la Llei de la jurisdicció contenciós administrativa de 1956 donava el tret bàsic de la discrecionalitat: "la discrecionalidad surge cuando el ordenamiento jurídico atribuye a algún órgano competencia para apreciar en un supuesto dado lo que sea de interés general".

Per aquesta raó, tot i que cada Administració Pública gaudeix d'una autonomia molt gran a l'hora de prendre les seves decisions autoorganitzatives, aquestes s'han d'adequar al que estableix l'ordenament jurídic aplicable. Això suposa, quan parlem del *Cloud*, l'existència d'un doble nivell:

- Un primer nivell seria la decisió discrecional d'optar per incorporar els serveis *Cloud* a les estructures administratives, atenent als evidents beneficis que se'n deriven de la seva implementació.

- Un segon nivell es configuraria per l'establiment d'un marc jurídic que donés plena garantia jurídica a les actuacions administratives que es duguin a terme utilitzant aquesta tecnologia i, d'altra banda, configurar o adequar els serveis *Cloud* al que és l'exercici de potestat administratives, sense que es produeixi cap reducció de les garanties pels ciutadans destinataris dels serveis corresponents.

Aquesta adaptació dels serveis Cloud a la singularitat de l'actuació administrativa és un element rellevant. Tot i que el principi de proporcionalitat ha estat incorporat en les decisions administratives, el que suposa que, en la pràctica, una administració pública pot arribar a fer el que, en la pràctica, és una anàlisi de riscos i beneficis que es deriven d'una determinada decisió (la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, és un clar exemple); hi ha un nucli essencial que és irrenunciable i que, quan parlem de serveis Cloud, han de ser considerats. Estem parlant de conceptes com protecció de dades, jurisdicció competent, ... i d'altres que han de ser valorats a l'hora de prendre la decisió per part de l'administració competent, no tan sols d'utilitzar el Cloud, sinó especialment a l'hora de decantar-se per una de les diferents opcions que, actualment, existeixen en el mercat per proveir-se de serveis Cloud.

Per aquesta raó, abans de entrar en el que serien les decisions o opcions a considerar a l'hora d'incorporar el Cloud a l'actuació administrativa, cal definir prèviament les diferents opcions amb les que ens podem trobar.

## 1.1 Definint el Cloud computing

No resulta simple, en principi, oferir una definició referida al *Cloud computing*, com succeeix de forma freqüent en el cas d'una nova tecnologia. ARMBRUST *et al*., 2009: p. 1, expliquen que el *Cloud computing* es refereix tant a les aplicacions lliurades com a servei a través d'Internet, com al maquinari i programari dels centres de dades que proporcionen aquests serveis. Els serveis anteriors han estat coneguts durant molt de temps com *Software as a Service* o SaaS (programari com a servei), mentre que el maquinari i programari del centre de dades constitueixen el que s'ha anomenat núvol.

VAQUERO *et al.*, 2009: p. 51, defineixen el *Cloud computing* com una gran reserva de recursos virtualitzats fàcilment utilitzables i accessibles (com ara plataformes de desenvolupament de maquinari i / o serveis). Aquests recursos poden ser dinàmicament re-configurats per adaptar-se a una càrrega variable (escala), el que permet també una utilització òptima dels recursos. Aquest conjunt de recursos sol ser explotat mitjançant un model de pagament per ús en què les garanties ofertes pel proveïdor d'infraestructura mitjançant SLA personalitzat.

D'altra banda, a l'hora d'entendre el concepte s'ha de trobar el que és el mínim comú denominador que es trobaria en totes les definicions, i que s'integraria pel que són les característiques comunes. El conjunt de característiques que més s'apropen a aquesta definició mínima serien l'escalabilitat, el model d'utilitat de pagament per ús i la virtualització.

L'Institut Nacional d'Estàndards i Tecnologies dels Estats Units d'Amèrica (en endavant, el NIST), ha definit el *Cloud computing* com un model per habilitar l'accés a través de xarxa, de forma ubiqua, convenient i sota demanda a un conjunt compartit de recursos de computació (per exemple, xarxes, servidors, emmagatzematge, aplicacions i serveis) que poden ser aprovisionats de forma ràpida i lliurats amb un esforç mínim de gestió o d'interacció amb el proveïdor del servei (MELLON i GRANCE, 2011: p. 2), definició que clarament emfatitza característiques de tipus funcional abans que tecnològiques[2], i que ha estat adoptada amb caràcter general per la indústria, les institucions i la doctrina[3].

En aquest sentit, en la visió del NIST, el model de *Cloud computing* es basa en cinc característiques essencials, tres models de servei i quatre models de desplegament, que veurem posteriorment en un cert grau de detall.

Com indica YOO, 2011: pp. 406-407, en qualsevol cas, hi ha un ampli acord en que la computació en núvol es centra al voltant de certs conceptes bàsics. Alguns observadors han assenyalat que la computació en núvol té una visió orientada cap a l'exterior i una altra cap a l'interior (BIRMAN *et al.* 2008). Des de la perspectiva cap a l'exterior d'un usuari final mirant el núvol, el que canvia són les

[2] El propi document del NIST indica que "la definició del NIST caracteritza aspectes importants del *Cloud computing* i es pretén serveixi com a mitjà per a comparacions àmplies de serveis Cloud i estratègies de desplegament, i per oferir una línia base per a la discussió sobre què és *Cloud computing* i com fer servir de la millor manera el *Cloud computing*" (MELLON i GRANCE, 2011: p. 2).
[3] En aquest sentit, cal indicar que el document del NIST ha estat citat més de 350 vegades des de la seva publicació (SCOPUS).

funcions que abans solien ser realitzades per equips que es troben al voltant de la xarxa (per exemple, allotjament de programari i dades) i que ara es desplacen als centres de dades residint en el nucli de la xarxa. Des de la perspectiva introspectiva de com els elements de computació en núvol interactuen amb altres elements de computació en núvol, l'atenció se centra en la capacitat de coordinar i integrar les aplicacions i les dades de funcionament en diversos equips a través de mecanismes que integren un tot sense fissures.

D'aquestes definicions es desprèn que el *Cloud computing* representa un canvi important per a les empreses i organismes públics en la forma de processar la informació i gestionar les àrees de Tecnologies de la Informació (TI). Mitjançant l'ús d'aquest paradigma, les organitzacions poden passar de la gestió TI tradicional (amb quantioses inversions en recursos, incloent maquinari, programari, centres de processament de dades, xarxes, personal, seguretat, etc.), al nou model de gestió TI en el núvol (s'elimina la necessitat de grans inversions i costos fixos), transformant als proveïdors en instruments, que posen a l'abast dels usuaris, de manera flexible i instantània, la capacitat de computació sota demanda (INTECO, 2012, p. 26).

Per aquesta raó, s'ha arribat a dir que el *Cloud computing* és més un concepte de màrqueting o, si es vol, una metàfora (JAEGER *et al.*, 2009), que una tècnica determinada. No obstant això, com veurem, indubtablement existeix una relació forta de dependència amb algunes tecnologies facilitadores, que diferencien aquest model d'altres, com la *Grid computing*.

Aquests autors expliquen que el *Cloud* és, ell mateix, una abstracció emprada per representar Internet i tota la seva complexitat. Quan els administradors de xarxa produeixen diagrames de xarxa s'utilitza la imatge un núvol per referir-se a Internet com a recurs, sense haver d'il·lustrar tota la seva complexitat. Per tant, per aquests autors, el "núvol" del *Cloud computing* representa un poderós i complex recurs, que es troba amagat per als seus usuaris, i posem de manifest que resulta irònic que la implementació d'aquest model de computació ens porti a una discussió sobre localitzacions.

En sentit similar, GARCÍA SÁNCHEZ, 2012:pp. 24-25, indica que no convé oblidar que, més enllà de la metàfora, la realitat tangible d'aquest fenomen la trobarem en grans centres de dades ubicats en diferents llocs del món els gestors dels quals es recolzen en l'ús intensiu de les economies d'escala – optimitzant l'ús de recursos físics i lògics amb elevat cost de capital i operatiu – amb la finalitat de ser capaços d'oferir serveis a preu reduït a un nombre elevat d'usuaris de forma global i utilitzant Internet com a xarxa de comunicacions. Això suposa importants implicacions i riscos en l'àmbit de la legalitat dels procediments, la privacitat, la protecció de dades i la seguretat dels sistemes.

FOSTER *et al.*, 2008: p. 2, sostenen que el *Cloud Computing* se solapa amb la computació en malla, que es basa en la seva columna vertebral i d'infraestructura. L'evolució ha estat el resultat d'un canvi en l'enfocament d'una infraestructura que proporciona emmagatzematge i recursos informàtics (com és el cas de la malla) a un que és basat econòmicament en l'objectiu d'oferir recursos més abstractes i serveis (com és el cas del *Cloud*). Quant a la computació de tipus

utilitari, no és un nou paradigma de la infraestructura informàtica, sinó que és un model de negoci en què els recursos de computació, com ara el càlcul i l'emmagatzematge, s'empaqueten com serveis mesurats similars a un servei públic físic, com l'electricitat i la xarxa telefònica commutada. La computació utilitària és típicament implementada utilitzant altra infraestructura informàtica (per exemple, la malla) amb serveis addicionals de comptabilitat i monitorització.

## 1.2 Les característiques definitòries del nou model computacional

Pel que fa a les característiques essencials d'aquest model computacional, el NIST identifica les cinc següents (MELLON i GRANCE, 2011: p. 2):

1. Autoservei sota demanda, que significa que un consumidor pot aprovisionar de forma unilateral capacitats de computació, com temps de servidor o emmagatzematge de xarxa, segons requereixi i de forma automatitzada, sense requerir una interacció humana amb cada proveïdor de servei.

2. Accés de banda ampla, que significa que les capacitats es troben disponibles a través de la xarxa i són accedides mitjançant mecanismes normalitzats que promouen l'ús per clients heterogenis, lleugers o pesats (com per exemple, telèfons mòbils, tabletes, portàtils i estacions de treball).

3. Compartició de recursos, que significa que els recursos del proveïdor serveixen a múltiples clients emprant un model multi-posseïdor, amb una assignació i reassignació dels recursos físics i virtuals d'acord amb la demanda del consumidor. Existeix un sentit d'independència en la localització en el sentit que el client, generalment, no controla o coneix la localització exacta dels recursos proveïts, però pot ser capaç d'especificar la localització en un nivell superior d'abstracció (per exemple, país, regió o centre de procés de dades). Com exemple de recursos es poden considerar l'emmagatzematge, el processament, la memòria o l'ample de banda.

4. Elasticitat ràpida, que significa que les capacitats poden ser aprovisionades i alliberades de forma elàstica, en alguns casos de forma automàtica, per tal d'escalar ràpidament, cap a l'exterior o a l'interior, de forma commensurada a la demanda. Per al consumidor, les capacitats disponibles per aprovisionar sovint semblen il·limitades i es poden apropiar en qualsevol quantitat i en qualsevol moment.

5. Servei mesurat, que significa que els sistemes *Cloud* controlen i optimitzen de forma automàtica l'ús del recursos sobre la base d'una capacitat de mesura en algun nivell d'abstracció apropiat al tipus de servei (per exemple, emmagatzematge, processament, ample de banda i nombre d'usuaris actius). L'ús dels recursos es pot monitoritzar, controlar i informar, oferint transparència tant al proveïdor com al consumidor del servei utilitzat.

En un sentit similar, indica la Cloud Security Alliance (en endavant, la CSA), que el Núvol és un model a la carta per a l'assignació i el consum de computació […] descriu l'ús d'una sèrie de serveis, aplicacions, informacions i infraestructura composta per reserves de recursos de computació, xarxes, informació i emmagatzematge […] poden orquestrar-se, abastir-se, implementar-se i desmantellar-se ràpidament, i escalar-se en funció de les dimensions per oferir uns serveis de tipus utilitat, una altra definició que també defuig de la tecnologia per centrar-se, més aviat, en una caracterització funcionalista (CSA, 2009).

Des d'una altra perspectiva, també s'ha diferenciat entre el *Cloud* d'emmagatzematge – basat en blocs o en fitxers, el *Cloud* de dades – basat en objectes, columnes o registres, i el *Cloud* de computació, freqüentment organitzats en una arquitectura per capes (GROSSMAN, 2009: p. 25). Igualment podem parlar del *Cloud* de xarxa, on es proveeixen serveis de xarxa virtualitzats (SCHOO *et al*., 2010: p. 5); models que plantegen capacitats i restriccions de seguretat diferents, per exemple en relació amb la confidencialitat de les dades.

Qualsevol paradigma tecnològic que suporti un model de servei basat en aquestes característiques serà, en general, qualificat o percebut dintre del concepte del *Cloud computing*, de forma que resulta necessari tractar les necessitats legals de seguretat des d'una òptica funcional, i posteriorment identificar les capacitats tècniques i els requeriments específics de les tecnologies concretes emprades.

Les tecnologies més emprades en suport del *Cloud computing*, que hauran de ser objecte de les mesures de protecció corresponents, inclouen xarxes d'accés, arquitectures orientades a serveis i clients lleugers, virtualització i hipervisors, i emmagatzematge remot (YOO, 2011:pp. 407-408).

## 1.3 Els models de servei de *Cloud computing*

Pel que fa als models de servei del *Cloud computing*, el NIST identifica els tres següents (MELLON i GRANCE, 2011: pp. 2-3):

1. *Software as a Service (SaaS)*, que es refereix al model en el qual la capacitat proveïda al consumidor permet emprar les aplicacions del proveïdor executades sobre una infraestructura *Cloud*. Les aplicacions són accessibles des de diversos dispositius client indistintament a través d'una interfície de client lleuger, com un navegador web (per exemple, correu electrònic basat en web), o d'una interfície de programa.

   El consumidor no gestiona ni controla la infraestructura *Cloud* subjacent, incloent-hi les capacitats de xarxa, servidors, sistemes operatius, emmagatzematge o aplicacions individuals, amb la possible excepció d'opcions limitades de configuració específica d'usuari.

Entre els exemples d'aquest programari es troben les eines de processament de textos i fulls de càlcul en línia, els serveis de gestió de relacions amb els clients i els serveis de lliurament de contingut web, com Salesforce CRM, Google Docs, etc. (CATTEDDU i HOGBEN, 2009a: pp. 16-17).

L'informe de la ONTSI, 2012: pp. 102-105, especifica, en línia amb altres estudis semblants, diverses solucions que es poden encabir dintre d'aquest model de servei. Tot i l'orientació mercantilista de la descripció de les solucions per aquest estudi, moltes resulten aplicables, amb petites adaptacions, a les Administracions:

- Contingut, comunicació i col·laboració (*Content, Communications and Collaboration,*CCC), incloent-hi:

    - Gestió de continguts empresarials (*Enterprise Content Management, ECM*) – ECM representa tant una estratègia per fer front a tot tipus de contingut no estructurat, com un conjunt de productes de programari per a la gestió de tot el cicle de vida dels continguts empresarials. Inclou la gestió de documents, de registres i de continguts web, la captació d'imatges de la documentació en paper, contingut social i dades no estructurats.

    - Identificació electrònica (*Electronic Discovery, E-discovery*) – Programari que permet la identificació, conservació, extracció, preparació, revisió i producció de la informació emmagatzemada electrònicament, associada als procediments legals i governamentals. La gestió de continguts i registres, la recerca i l'accés a la informació, així com la conservació i el emmagatzematge del correu electrònic.

    - Correu electrònic (*E-mail*) – Solució *Cloud* consistent en un programari que permet la transmissió electrònica de missatges (incloent text i arxius adjunts), des d'un ordinador o equip informàtic a un altre situat dins o fora de l'organització.

    - Recerca d'informació (*Search*) – Programari que ofereix a l'usuari l'opció implementar en la seva pròpia pàgina web, una eina la funcionalitat principal és la de buscar informació i documentació que es trobi disponible a la Xarxa.

    - Col·laboració entre equips (*Team collaboration*) – Eines que ofereixen recursos per a la comunicació i col·laboració entre els diferents membres d'un equip. Entre les seves funcionalitats destaquen les comunitats en línia, les xarxes socials, els fòrums de discussió, els blocs i la missatgeria instantània entre altres.

- Conferències a la Xarxa (*web conferencing*) – Eines que possibiliten la realització de conferències en temps real a través de la Xarxa. Les funcionalitats ofertes per aquestes eines van des del lliurament de contingut fins a serveis integrats d'àudio o control remot d'equips.

- Gestió de la relació amb el client (*Customer Relationship Management*, CRM), incloent-hi:

  - Vendes (*Sales*) – Eines que permeten gestionar la informació dels clients (des d'emmagatzemar i organitzar aquesta informació, fins a integrar, processar i analitzar la mateixa), relacionada amb l'àrea de vendes de l'empresa.

  - Màrqueting – Eina destinada a l'àrea de màrqueting de les empreses, que els permet, igual que altres solucions *Cloud* de tipus CRM, emmagatzemar, organitzar, integrar, processar i analitzar tota la informació dels esmentats clients actuals i potencials.

  - Servei i suport al client (*Customer service and support*) – Eina que permet donar servei d'informació i suport tècnic a l'usuari, emmagatzemant la informació rebuda d'aquest, processant i analitzant per aportar-li la millor solució en el menor temps possible.

- Creació de contingut digital (*Digital Content Creation,* DCC), que és programari destinat al desenvolupament de material digital d'interès periodístic, educatiu i d'entreteniment (animacions, àudio, gràfics, imatges, vídeo, etc.), per a la distribució a través d'Internet o altres mitjans electrònics.

- Planificació de recursos empresarials (*Enterprise Resource Planning*, ERP), incloent-hi:

  - Gestió del Capital Humà (*Human Capital Management*, HCM) – HCM és un conjunt de pràctiques relacionades amb la gestió dels recursos de personal de l'entitat. Aquestes pràctiques es centren en la necessitat de l'organització de proporcionar competències específiques, i s'implementen en tres categories:

    - Contractació de personal.
    - Gestió de la plantilla.
    - Optimització de la plantilla.

  Les eines que permeten la gestió del capital humà de l'entitat inclouen les funcionalitats necessàries per cobrir els processos associats a les nòmines, a la planificació de la plantilla, a la formació, i a la selecció i contractació, així com a la

gestió de l'acompliment, de competències, i de temps i despeses, i a l'administració de beneficis i del personal entre altres.

- Sistema de Gestió financera (*Financial Management System*, FMS) – Són aplicacions que proporcionen visibilitat en la posició financera d'una empresa, mitjançant l'automatització i el suport als processos de qualsevol activitat que tingui un impacte financer en l'entitat. A més, proporcionen informes de dades financeres, segons sigui necessari per les regulacions locals i internacionals. Aquest tipus d'aplicacions inclouen, entre d'altres, les de consolidació financera, les de tresoreria i gestió d'efectiu, les de comptabilitat, les de gestió tributària, quadres de comandament, etc.

- Fabricació i operacions (*Manufacturing and operations*) – Eines destinades al sector manufacturer, les funcionalitats es basen en la organització, el control, el seguiment i la diferenciació del procés de fabricació, de cara a la seva optimització, i a la reducció de costos i augment de marges de benefici que això comporta.

- Paquets de programari d'oficina (*Office Suites*), que inclouen el conjunt de programes destinats a ser utilitzats pels treballadors de la entitat durant la seva operativa diària. Els components del paquet es distribueixen generalment en conjunt, tenen una interfície d'usuari similar i en general poden interactuar entre si. Com a exemple es poden esmentar els paquets informàtics que contenen processadors de text, fulls de càlcul, editors de presentacions, gestors de bases de dades, etc.

- Gestió de la cartera de projectes (*Project and Portfolio Management*, PPM) – PPM és un terme utilitzat pels gestors de projectes i les oficines de gestió de projectes (*Project Management Office*, PMO), per descriure els mètodes de anàlisi i la gestió col·lectiva d'un grup de projectes en curs, previstos o proposats. Les funcionalitats clau sobre les quals es basen les eines PPM són les que segueixen:

  - Establiment de fites, planificació de projectes i seguiment del progrés i dels terminis dels projectes.
  - Gestió dels programes dels projectes.
  - Assignació de perfils i permisos.
  - Anàlisi i priorització de la cartera de projectes.

- Gestió de la cadena de subministrament (*Suply Chain Management*, SCM), incloent-hi:

  - Abastament / Adquisició (*Sourcing / procurement*) – Aquest tipus d'aplicacions s'utilitzen per ajudar a les empreses a entendre i millorar els termes i condicions del comerç, i a comprendre la procedència dels despeses incorregudes per l'empresa.

Aquestes aplicacions, a més ajuden a la selecció de proveïdors, l'anàlisi de l'acompliment dels proveïdors seleccionats, i l'establiment dels termes d'intercanvi per equilibrar els costos, la qualitat i el risc.

Entre els mòduls inclosos en aquest tipus d'aplicacions es troben la adquisició electrònica, el proveïment estratègic, la gestió de contractacions, l'abastament tàctic, i l'anàlisi de despeses entre altres.

- Planificació de la cadena de subministrament (*Supply chain planning*, SCP) – La planificació de la cadena de subministrament és el procés de coordinació de els actius per optimitzar el lliurament de béns, serveis i informació, des del proveïdor al client, aconseguint amb això equilibrar l'oferta i la demanda.

- Un programari de planificació de la cadena de subministrament s'estableix al capdavant d'un sistema de transaccions, per proporcionar-li la planificació necessària, fent ús de la seva capacitat d'anàlisi d'escenaris, dels compromisos de la demanda en temps real, i tenint en compte les possibles limitacions de subministrament.

- Sistema de gestió de magatzems (*Warehouse management system*, WMS) – Un sistema de gestió de magatzems és una part clau de la cadena de subministrament, i té com a objectiu principal controlar el moviment i la acumulació de materials dins d'un magatzem, i processar les transaccions associades, inclòs l'enviament, la recepció, l'entrada en magatzem i la recollida. Els sistemes també dirigeixen i optimitzen l'entrada i gestió del estoc, basant-se en la informació en temps real sobre l'estatus de utilització dels lots.

- Sistema de gestió del transport (*Transportation management system*, TMS) – Sistema utilitzat per planejar els moviments de mercaderies, fer la valoració de càrregues i les compres en tots els modes, seleccionar les rutes i els transportistes adequats, i gestionar les factures i els pagaments associats al transport.

- Compliment de transaccions a nivell mundial (*Global trade compliance*) – Aplicació encarregada de l'homogeneïtzació dels requisits d'informació electrònica de la càrrega, sobre tots els enviaments entrants, sortints i de trànsit; assumpte fonamental per garantir el moviment segur de les mercaderies al llarg dels diferents països.

- Planificació del Servei de Peces (*Service Parts Planning*, SPP) – Les solucions Cloud SPP inclouen la planificació dels processos de subministrament i distribució de peces de manteniment (recanvis i accessoris), dins una xarxa logística integrada.

- Altres solucions, que inclouen:

  - Gestió de despeses (*expense management*) - Sistemes instal·lats per una empresa per processar, pagar, i auditar les despeses incorregudes pels seus empleats. Aquests costos poden incloure, sense limitar-se a aquest tipus de despeses, fins a les despeses de viatge i entreteniment dels empleats, depenent en tots els casos de la empresa en qüestió. La gestió de despeses inclou també les polítiques i procediments que regeixen aquesta despesa, així com les tecnologies i serveis utilitzats per processar i analitzar les dades associades amb ell.

  - Sistema de gestió de compliment (*Compliance management system*, CMS) – Tipus de programari encarregat de realitzar tot el procés de recopilació i avaluació de les dades dels fons, tant de clients com d'inversors, incloent els informes d'auto-monitoratge i verificació, per demostrar si les operacions del fons en qüestió s'ajusten a les normes de compliment emeses per la Comissió de Valors dels Estats Units (US Securitiesand Exchange Commission, USA) o l'Autoritat de Serveis Financers del Regne Unit (Financial Services Authority, UK).

  - Aprenentatge Electrònic (*Electronic-learning, E-learning*) - L'aprenentatge electrònic o e-learning és l'ús d'Internet per a l'aprenentatge fora de l'aula. Els productes *Cloud* d'e-learning són solucions de programari en el núvol que permeten l'automatització i administració de continguts, així com l'educació i l'aprenentatge a través d'Internet. Aquests productes integren els sistemes de gestió d'aprenentatge (*Learning Management Systems*, LMSs), les aules virtuals, els cursos virtuals, i els sistemes de gestió de continguts educatius (*Learning Content Management Systems*, LCMSs).

  - Missatgeria instantània per a empreses (*Enterprise instant messaging*) – Les aplicacions de missatgeria instantània constitueixen una forma de comunicació en temps real, basada en la inserció d'un text directament en un xat de interlocució entre dos o més empleats, que utilitzen els seus ordinadors personals o altres dispositius que disposin de l'aplicació incorporada i accés a la xarxa.

    La informació i documentació intercanviada pels usuaris de l'aplicació es transfereix a través d'una xarxa, com per exemple Internet. Els programes de missatgeria instantània més avançats també permeten millorar les maneres de comunicació, incorporant funcionalitats com la veu en viu, la videotrucada, la inclusió d'enllaços als mitjans de comunicació, o la compartició i visualització d'equips i recursos diversos.

  - Emmagatzematge (*Storage*) – Aquest tipus de programari està constituït per aplicacions que permeten implementar l'emmagatzematge virtualitzat, que consisteix en la fusió de múltiples dispositius d'emmagatzematge en xarxa en el

que per a l'usuari sembla ser una única unitat d'emmagatzematge. La virtualització de l'emmagatzematge és d'ús freqüent en les xarxes locals de emmagatzematge (StorageArea Network, SAN), subxarxes d'alta velocitat dels dispositius d'emmagatzematge compartit, en les que l'aplicació permet realitzar les tasques d'arxivament, còpia de seguretat i recuperació de dades d'una manera més senzill i ràpid.

- Sistema de gestió de vendes (*Retail management system*, RMS) – Són sistemes que ofereixen als minoristes de petites i mitjanes empreses un punt complet de venda. Permet automatitzar no només els processos associats als diferents punts de venda, sinó també les operacions de magatzem, proporcionant amb això als minoristes amb múltiples botigues, el control centralitzat de tots els seus recursos.

2. *Platform as a Service (PaaS)*, que es refereix al model en el qual la capacitat proveïda al consumidor permet desplegar sobre la infraestructura *Cloud* aplicacions creades o adquirides pel consumidor emprant llenguatges de programació, llibreries, serveis i eines suportades pel proveïdor.

   El consumidor no gestiona ni controla la infraestructura *Cloud* subjacent, incloent-hi les capacitats de xarxa, servidors, sistemes operatius o emmagatzematge, però té control sobre les aplicacions desplegades i possiblement opcions de configuració en relació amb l'entorn d'allotjament de les aplicacions.

   Alguns exemples són Microsoft Azure, Force i App Engine de Google (CATTEDDU i HOGBEN, 2009a: p. 17).

   L'informe de la ONTSI, 2012: pp. 102-105, especifica, en línia amb altres estudis semblants, diverses solucions que es poden encabir dintre d'aquest model de servei:

   - Servidor d'aplicacions integrades (*Integrated Application Server*) – Un servidor d'aplicacions és una forma moderna de *middleware* de plataforma, és a dir, és un programari que es troba entre el sistema operatiu per una banda, els recursos externs (com ara un sistema de gestió de bases de dades (DBMS), serveis de comunicacions i Internet) en un altre banda, i les aplicacions dels usuaris en el tercer costat. La funció del servidor d'aplicacions és la d'actuar com a magatzem (o contenidor) per als models de l'usuari de negoci, alhora que facilita l'accés i el funcionament de les aplicacions d'aquests.

   - Integració de dades (*Data Integration*) – Aquestes solucions permeten als desenvolupadors i integradors de sistemes crear, compartir i reutilitzar, les integracions de dades personalitzades i els mapatges de qualitat de les dades, i executar-los en el núvol.

Gràcies a aquestes solucions, els desenvolupadors poden col·laborar de forma activa amb els equips de TI per crear integracions de dades reutilitzables i mapatges de qualitat de les dades en el núvol o en les instal·lacions pròpies. A més, els usuaris de negoci poden configurar ells mateixos les seves regles d'integració de dades, o executar els mapatges construïts pels departaments de TI utilitzant els serveis PAAS d'integració de dades.

- Sistemes de gestió de base de dades (*Database Management System*, DBMS) – El DBMS és un producte amb el qual es controla l'organització, l'emmagatzematge, la recuperació, la seguretat i la integritat de les dades en una base de dades. Com funcionalitats característiques d'aquest tipus de solució PaaS es troben les següents:

    - És capaç d'acceptar sol·licituds de les aplicacions, i indicar al sistema operatiu les dades adequades a transferir.

    - Pot funcionar amb llenguatges de programació tradicionals, o incloure el seu propi llenguatge de programació per al desenvolupament d'aplicacions.

    - Permet que els sistemes d'informació canviïn amb més facilitat a mesura que canvien les necessitats de l'organització.

    - Seguretat de dades: El DBMS prevé l'accés no autoritzat dels usuaris a veure o actualitzar informació a la base de dades.

    - Integritat de dades: El DBMS garanteix que dos o més usuaris no puguin actualitzar el mateix registre a la vegada.

- Control de transferència de fitxers (*Managed File Transfer*, MFT) – Són solucions que faciliten la transferència segura de dades d'un ordinador a un altre a través d'una xarxa (com per exemple Internet). Es caracteritzen, entre altres funcionalitats, per les enumerades a continuació:

    - Admetre diferents protocols d'intercanvi (FTP/S, SFTP, SCP, HTTP/S, etc.).

    - Transferència segura d'arxius a través de xarxes públiques i privades.

    - Emmagatzematge d'arxius de forma segura.

    - Generació d'informes detallats sobre els usuaris i la seva activitat.

- Seguretat d'aplicacions (*Application Security*) - Els proveïdors que ofereixen aquest tipus de servei País proporcionen una solució de seguretat escalable i flexible, que protegeix les aplicacions dels clients de les amenaces externes, que redueix el risc de fuga de dades, i que permet complir, de manera eficient, amb la normativa vigent aplicable.

- Integració de les aplicacions i les relacions negoci a negoci (*Application and Business to Business (B2B) Integration*) – Plataformes que integren les aplicacions de la companyia, amb la relació comercial establerta per mitjà de xarxes telemàtiques, entre dues empreses o companyies.

- Portals d'aplicacions – catàlegs (*AppMarketplaces - catalogs*) – Són plataformes posades a disposició del client per part del proveïdor, on l'usuari pot trobar gran varietat d'eines o aplicacions disponibles al mercat, per al seu ús, entre altres motius, amb fins de negoci, de gestió o amb fins didàctics.

- Portals de plataformes d'experiències d'usuaris (*Portals User Experience Platform,* Portals UXP) – UXP és un conjunt integrat de plataformes, destinat a proporcionar una completa interfície d'usuari i capacitats d'interacció. entre els seus principals característiques i funcionalitats s'inclouen portals web, *mashup* (pàgines web o aplicacions que combinen dades o funcionalitats de dues o més fonts), gestió de continguts, col·laboració, mòbils, anàlisi, recerca, comerç electrònic, plataforma d'aplicacions, marc global de disseny i gestió en el UXP.

- Tecnologia per a la gestió de processos de negoci (*Business Process Management Technology*, BPM Technology) – El BPM es refereix al tipus de gestió empresarial consistent en la integració de els processos, les persones i els sistemes tecnològics de la companyia, per tal de facilitar el desenvolupament de les estratègies de negoci de l'entitat.

- Gestió del cicle de vida de les aplicacions (*AppLifeCycle Management*, ALM) – La plataforma ALM abasta tot el procés de gestió de la vida d'una aplicació informàtica (des del moment de la seva definició, fins ara del seu desplegament i manteniment posterior), mitjançant la governabilitat, el desenvolupament i el manteniment de la mateixa.

- Capa intermèdia de missatgeria (*Messaging Middleware*) - Plataforma que proporciona una interfície entre les aplicacions, permetent enviar les dades d'anada i tornada de l'un a l'altre de forma asíncrona. Les dades enviats per una aplicació es poden emmagatzemar temporalment a l'altra, i remetre a altres programes que els requereixin que estiguin disponibles per dur a terme el procés d'intercanvi de dades.

- Processament extrem de transaccions (*Extreme Transaction Processing*, eXtreme TP) – Tipus d'eines destinades al suport en el disseny, desenvolupament, gestió i manteniment d'aplicacions de processament de transaccions distribuïdes (TP), transaccions caracteritzades per l'alta demanda de rendiment, escalabilitat, disponibilitat, seguretat, capacitat de gestió i requisits de fiabilitat.

3. *Infrastructure as a Service (IaaS)*, que es refereix al model en el qual la capacitat proveïda al consumidor permet aprovisionar processament, emmagatzematge, xarxes i altres recursos fonamentals de computació on el consumidor es capaç de desplegar i executar programari arbitrari, incloent-hi sistemes operatius i aplicacions.

   El consumidor no gestiona ni controla la infraestructura Cloud subjacent, però té control sobre els sistemes operatius, emmagatzematge i aplicacions desplegades, i possiblement un control limitat de components seleccionats de xarxa (per exemple, els tallafocs de host).

   Alguns exemples són Amazon EC2 i S3, Enterprise Cloudde Terremark, Windows Live Skydrive i Rackspace Cloud (CATTEDDU i HOGBEN, 2009 a: p. 17).

   L'informe de la ONTSI, 2012: p. 106, especifica, en línia amb altres estudis semblants, diverses solucions que es poden encabir dintre d'aquest model de servei:

   - Serveis de computació (*compute services*), solucions ofertes pel proveïdor, consistents en oferir al client la possibilitat de augmentar la seva capacitat de computació, sense haver de incórrer en les despeses de capital que suposaria l'adquisició dels equips físics necessaris per maximitzar la capacitat.

   - Serveis d'emmagatzematge (*storage services*), en què un proveïdor lloga espai en la seva infraestructura pròpia de emmagatzematge, per al seu ús per part d'una organització o un persona.

     El principal avantatge de contractar a una empresa un servei de emmagatzematge en el núvol és un estalvi de costos, tant en costos de personal, com de hardware i d'espai d'emmagatzematge físic.

     Per això, aquest tipus de servei és generalment molt emprat en organitzacions de mitja i petita grandària, que no tenen capital o personal tècnic per implementar i mantenir en la seva entitat, la seva pròpia infraestructura d'emmagatzematge.

     A més aquest tipus de solucions *Cloud* ha començat a ser àmpliament utilitzat com a mesura de reducció dels riscos associats a la recuperació de dades després d'un

desastre, proporcionant la retenció de les dades a llarg termini, millorant amb això la disponibilitat i la continuïtat del negoci.

- Serveis de còpia de seguretat (*backup services*), que proporciona, ja sigui remota, en línia o administrada, als usuaris un sistema periòdic de còpia i emmagatzematge d'arxius informàtics a la infraestructura del proveïdor. Aquests arxius poden ser posteriorment recuperats en cas de fallida o canvi dels equips, de pèrdua puntual de dades, o de necessitat de recuperació de dades després d'un desastre.

L'adopció d'un model de servei específic suposarà un repartiment del control i la responsabilitat sobre els components del sistema; si en el model clàssic l'organització manté el control absolut sobre els components, en el núvol l'organització i el proveïdor es repartiran el control sobre els components o bé el compartiran d'acord al model de servei utilitzat (GARCÍA SÁNCHEZ, 2011: p. 27).

Dins d'aquesta segmentació, s'han plantejat distincions més detallades, com SecaaS- seguretat com a servei (CSA, 2011), PasS-privacitat com a servei (ITANI *et al*., 2009) o PaaS- gestió de permisos com a servei (ECHEVERRÍA *et al*., 2010 ), tots ells en l'àmbit d'interès en aquest treball, i un llarg etcètera que ha portat a parlar de la generació "as a service" (BANKINTER, 2010: p. 37).

En tota arquitectura basada en capes de servei, quan més finalista és el servei, menor és la visibilitat i el control dels elements d'infraestructura subjacents, que per ser virtuals poden, a més, circular sense control del client per diversos equipaments, ubicats a proveïdors i territoris imprevisibles per al client, com analitzarem posteriorment.

## 1.4 Els models de desplegament del *Cloud computing*

Finalment, des de la perspectiva del desplegament del serveis *Cloud*, el NIST identifica els següents quatre models (MELLON i GRANCE, 2011: p. 3):

1. *Cloud* privat, en que la infraestructura *Cloud* es aprovisionada per a l'ús exclusiu per part d'una única organització que compren múltiples consumidors (per exemple, unitats de negoci). Pot ser adquirida, gestionada i operada per l'organització, per una tercera part, o una combinació dels dos anteriors, i pot existir o no a les pròpies instal·lacions.

   L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 32, identifica, una sèrie de característiques inherents a aquest tipus d'implementació. Podem citar les següents:

- Ofereix un temps de posada en servei baix i una alta flexibilitat en l'assignació de recursos.

- A diferència del *Cloud* públic, requereix d'inversió de capital per a la implementació de la solució contractada.

- Porta associats sistemes i bases de dades locals.

- Permet la possibilitat d'aprofitar el personal existent i les inversions en sistemes d'informació realitzades amb anterioritat.

- Implica més especificitat en la solució adquirida, ja que està dissenyada per ajustar-se a les necessitats pròpies de l'empresa contractant.

- Permet disposar d'un control total de la infraestructura, dels sistemes i de la informació corporativa tractada per aquests.

D'altra banda, i d'acord amb l'informe sobre seguretat i resiliència en Cloud governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 (CATTEDDU, 2011: pp. 54 i ss.), aquest model presenta les següents debilitats, amenaces, fortaleses i oportunitats (anàlisi DAFO):

Debilitats:

- L'efecte beneficiós de les economies d'escala en els *Clouds* privats és probable que sigui molt menor en comparació amb els núvols públiques (almenys les de gran escala, presents actualment al mercat) o fins i tot amb les comunitàries.

- La possible manca d'una escala adequada també representa un punt feble en l'adquisició i la posada en marxa de mecanismes de seguretat.

- Hi ha, en potència, una menor tolerància als atacs maliciosos que en un *Cloud* públic, partint del supòsit que els recursos disponibles (especialment en termes de capacitat de computació) poden ser menys adequats que els d'un *Cloud* públic. En alguns casos, també és possible que l'experiència interna del proveïdor no sigui suficient.

- Hi ha menys resistència per satisfer les puntes de demanda inesperats, a causa de l'escassetat de recursos. Això requereix planificar la capacitat i una avaluació comparativa abans de traslladar al núvol.

- Sent realistes, és possible que un *Cloud* privat pugui definir un règim de redundància complet, però, és molt poc probable que això sigui igual o millor que el règim de redundància ofert pel núvol pública d'un important proveïdor de *Cloud*.

- La manca de geo-redundància és un problema pel que fa a la continuïtat del negoci. En general, el temps que triga a recuperar-se d'una fallada un núvol privada pot ser bastant superior al d'un *Cloud* públic, llevat que el proveïdor implementi mecanismes i polítiques específics. En aquest sentit, s'ha de definir un acord de nivell de servei adequat amb el proveïdor.

- Sensibilitat de la reputació: la reputació dels governs i els organismes públics pot ser extremadament sensible a la fuga d'informació i a qualsevol incident de seguretat, inclòs l'ús d'una infraestructura propietat de les administracions públiques per llançar atacs maliciosos.

**Amenaces**. Un govern o un organisme públic disposat a crear i utilitzar un *Cloud* privat ha d'estar preparat per enfrontar-se a les següents amenaces:

- Atacs amb motius polítics: mentre que la quantitat d'informació gestionada pel *Cloud* pot no ser atractiva per si mateixa, el deteriorament d'un lloc del govern pot ser atractiu per motius polítics (òbviament, aquesta amenaça no es limita als *Clouds* privats, però un núvol governamental privada podria presentar una concentració molt elevada de recursos i, per tant, l'incentiu per un atacant motivat seria encara més gran).

- Efecte gran germà: el fet que les administracions públiques recopilin i gestionin informació sobre els ciutadans i, a la llarga, de les empreses (en el cas que el *Cloud* s'utilitzi com un viver d'empreses per a les pimes) pot ser percebut, des de la perspectiva de l'usuari final, com una manera possible d'establir un sistema de vigilància i de creació de perfils.

- L'alta volatilitat en la utilització de recursos i els pics inesperats en les sol·licituds podria obligar a un *Cloud* privat a escalar horitzontalment a un núvol públic (*Cloud* híbrid), fora de l'abast de la política de seguretat definida. En aquest cas, el control sobre la informació en el *Cloud* es perd parcialment sempre que no es defineixi la política de seguretat, que marca les normes sobre la informació que es pot exportar.

- Mala planificació: per exemple, la definició dels requisits i la classificació dels actius pot originar una pèrdua de seguretat i integritat quan es passa d'un *Cloud* privat a un *Cloud* híbrida (això al marge dels inconvenients que tot procediment de migració, per sí mateix, ja suposa).

- La definició inadequada dels contractes amb els socis comercials (operador de núvol, socis tecnològics, proveïdors de maquinari i programari, etc.) I la manca de seguiment de l'execució dels contractes pot ser crítica en relació amb la mida del proveïdor.

**Fortaleses**. En un Cloud privat, l'usuari-propietari té, en principi, el control absolut (segons les limitacions econòmiques) sobre el conjunt de característiques de la implementació del núvol, però, hi ha costos (que no poden ser compartits amb altres clients) associats a aquest augment en el control.

La següent llista conté les característiques més importants (sobre seguretat i resistència) que es poden definir en un *Cloud* privat:

- Pràctiques d'avaluació de riscos: és possible seleccionar les metodologies, escales, criteris de mesurament, etc.

- Pegats: és possible programar pegats quan sigui necessari, i també modificar el règim.

- Control d'accés: Granularitat més fina de la gestió i les polítiques d'accés per evitar fuites de dades.

- Registre: és possible controlar el que es registra, on s'emmagatzema, com es protegeix l'emmagatzematge i durant quant de temps es guardarà.

- Auditoria: és possible establir i regular el dret a auditar.

- Control sobre la disponibilitat, fiabilitat, escalabilitat i elasticitat: el client pot especificar el sistema i definir els acords de nivell de servei perquè el núvol privada s'ajusti, dins de les limitacions tècniques, al rendiment de servei requerit.

- Disponibilitat de la interfície de gestió: es pot negociar més fàcilment amb els proveïdors de serveis d'Internet els serveis de primera qualitat per obtenir una xarxa i una connexió millors (p. ex., Prioritat en la represa del servei).

- Pla de continuïtat de negoci: es pot definir el pla i comprovar tots els seus components.

- Respecte de la legislació: una total transparència i control sobre els requisits legals, com la ubicació de dades.

Oportunitats:

- Seguiment: en un *Cloud* privat, els mecanismes de seguiment orientats a l'usuari i les aplicacions es poden implementar realitzant un ajust ràpid dels recursos per cobrir els possibles pics de demanda. A més, es poden controlar totalment els esdeveniments de seguretat d'interès. Com a contrapartida, si l'escala del *Cloud* privat no és l'apropiada, el maneig dels pics de demanda de recursos pot ser bastant complex i no hi ha una solució eficaç per als pics imprevistos. Tanmateix, els recursos del *Cloud* han de ser explotats per millorar el rendiment de les aplicacions que es traslladin al mateix.

- Control d'accés: si cal, es poden adoptar més fàcilment polítiques d'accés basades en sistemes de control d'accés no discrecional (p. ex., MAC – control d'accés obligatori) o RBAC – control d'accés basat en rols) per limitar encara més a cada usuari i minimitzar els fluxos il·legítims entre usuaris.

L'informe de la ONTSI, 2012: p. 43, considera que la pròpia naturalesa de la gestió pública i la criticitat dels processos i informació que gestionen les Administracions fan suposar un model d'adopció en què els sistemes més crítics (gestió tributària, personal, sistemes econòmic-financer, seguretat i defensa, etc.) es migrin cap a xarxes CLOUD privades per a l'administració interna en centres de serveis compartits, aconseguint un important efecte en l'estandardització i compartició de recursos tecnològics entre diferents organismes públics.

2. *Cloud* comunitari, en que la infraestructura *Cloud* es aprovisionada per a l'ús exclusiu per part d'una comunitat específica de consumidors d'organitzacions que tenen preocupacions comunes (per exemple, missió, requeriments de seguretat, polítiques o consideracions de compliment normatiu). Pot ser adquirida, gestionada i operada per una o més de les organitzacions de la comunitat, per una tercera part, o una combinació dels dos anteriors, i pot existir o no a les pròpies instal·lacions.

Per la seva banda, l'informe sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 (CATTEDDU, 2011: pp. 55 i ss.), posa de manifest que aquest model presenta igualment una sèrie de debilitats, amenaces, fortaleses i oportunitats (anàlisi DAFO).

En analitzar un *Cloud* comunitari, s'ha de considerar que, en principi, els seus punts forts i febles es troben entre els d'un *Cloud* privat i els d'un públic. En general, el conjunt de recursos disponibles és més gran que en un *Cloud* privat, amb avantatges evidents en termes d'elasticitat. No obstant això, el conjunt no és tan gran com el d'un *Cloud* públic, i això limita la elasticitat que ofereix un *Cloud* comunitari. D'altra banda, el nombre d'usuaris en un *Cloud* comunitari és molt menor que en un *Cloud* públic, el que té avantatges òbvies en termes de seguretat.

Debilitats:

- Hi ha més competència pels recursos entre els socis, ja que tenen objectius comuns. Alguns dels beneficis derivats del fet de disposar d'un major nombre de recursos es perden perquè els usuaris de la mateixa comunitat poden presentar patrons similars a l'hora d'accedir als recursos, de manera que es poden produir en un mateix espai de temps pics de sol·licituds de recursos per part de diversos usuaris.

- En comparació amb un *Cloud* privat, una comunitat és un objectiu més atractiu per als atacants motivats a causa de la major visibilitat aconseguida pels atacs amb èxit. A més, les aplicacions d'altres usuaris poden proporcionar una via per als atacs.

- El control d'accés i l'autenticació estan debilitats en comparació amb un *Cloud* privat a causa del major nombre d'usuaris.

- El deteriorament del rendiment (IaaS, PaaS i SaaS) a causa de la mala qualitat de la connectivitat (p. ex., zones rurals, especialment en els països del sud i l'est de la Unió Europea) pot reduir la qualitat del servei per a alguns usuaris de la comunitat (que no estiguin ubicats a prop dels punts de subministrament), en comparació amb un *Cloud* privat.

Amenaces:

- Falta d'acord sobre les línies bàsiques de la seguretat i els mecanismes de seguretat: per aprofitar l'oportunitat de compartir mecanismes per protegir i defensar la informació, s'ha de negociar un acord entre tots els membres de la comunitat. La majoria de les vegades, una re-negociació, fins i tot encara que abasti a un nombre reduït d'usuaris, pot ser bastant complexa i no arribar a tenir èxit, atenent a la no necessària coincidència entre les posicions o interessos dels integrants de la comunitat.

- Les comunitats poden créixer massa de pressa, el que a la llarga redueix els avantatges del *Cloud* comunitari en termes de resistència, en comparació amb un *Cloud* privat, o poden créixer molt lentament, el que eventualment afectarà la escalabilitat dinàmica. En aquesta línia, les necessitats d'implementació del model, en termes de temps, no són necessàriament coincidents entre els integrants de la comunitat.

- Més difícil predicció de l'ús de recursos (que en un *Cloud* privat): el major nombre d'usuaris incrementa la complexitat d'anticipar-se a les sol·licituds de recursos de cada usuari. En un *Cloud* comunitari, és més probable que es produeixin errors en la planificació de la capacitat del *Cloud*.

- Una fallada en els mecanismes d'aïllament pot causar la filtració d'informació, que és més difícil de controlar a causa del major nombre d'usuaris.

Fortaleses:

- Requisits i limitacions comuns i perfil de risc: els usuaris d'un *Cloud* comunitari tenen requisits similars des d'una perspectiva de seguretat i rendiment. Això fa que la implementació de les polítiques per satisfer aquests requisits siguin més eficients i rendibles, fins i tot per al proveïdor, el que es tradueix en un menor cost global.

- Els requisits i els perfils de risc comuns simplifiquen la configuració de mecanismes i eines per protegir les aplicacions que s'executen en el *Cloud* d'atacs interns i externs.

- Els usuaris tenen més poder de negociació com a grup (en relació amb el proveïdor de *Cloud*) a causa del major nombre d'usuaris amb necessitats similars.

- Capacitat per establir els criteris d'inclusió: la condició de membre s'atorga d'acord amb la resistència dels membres potencials. Això redueix molt els riscos deguts a atacs d'altres usuaris del *Cloud*.

- Una major escala i una millor resposta als pics elevats de demanda de recursos (en comparació amb un *Cloud* privat): la mida de les agrupacions de recursos pot ser notablement més gran que el d'un núvol privada i això simplifica la gestió dels pics de demanda de recursos.

Oportunitats:

- Els requisits similars que es registren a la comunitat podrien permetre la millora de les polítiques, els paràmetres de referència i les normes de seguretat, així com pràctiques comuns per a l'anàlisi i l'avaluació de riscos, el registre i el seguiment. Això pot donar lloc a implementacions altament eficients que redueixen el cost d'adopció per a cada usuari i propicien una arquitectura més fiable.

- Els sistemes de gestió d'incidents comuns i compartits poden simplificar l'adopció de mecanismes per emmagatzemar i administrar les proves informàtic-forenses.

- L'intercanvi d'informació entre altres membres de la comunitat (les millors pràctiques d'ús, l'experiència d'incidents anteriors, etc.) Pot propiciar una major difusió de les millors pràctiques, ajustada pels membres més experts de la comunitat.

- Es pot obtenir una seguretat més estricta perquè la informació sobre les polítiques de seguretat i el disseny i la implementació del *Cloud* només es comparteix dins la comunitat. En comparació amb un *Cloud* públic, això incrementa la dificultat, per a un atacant, d'adquirir informació per posar en pràctica els seus atacs.

3. *Cloud* públic, en aquest model, la infraestructura *Cloud* es aprovisionada per a l'ús obert pel públic en general. Pot ser adquirida, gestionada i operada per una organització mercantil, acadèmica o governamental, o alguna combinació de les anteriors. Existeix a les instal·lacions del proveïdor de *Cloud*.

Moltes de les aplicacions que actualment es troben més esteses en el Cloud públic són, a més, serveis prestats a consumidors i usuaris. Aquesta prestació directa cap al consumidor o usuari, en què el benefici econòmic sigui l'objectiu principal, fa que en ocasions hi concorrin insuficients coneixements i, el que és més greu, insuficient conscienciació sobre seguretat i privacitat (tot i que hem de pensar que, en última instància, aquesta inconsciència en ocasions es basa en l'anàlisi del cost benefici, preferint assumir riscos en lloc de desenvolupar unes actuacions que, com a regla general, suposaran inversions econòmiques més significatives).

D'altra banda, des d'un punt de vista sociològic, sembla que els usuaris mostren poca preocupació per les conseqüències d'emmagatzematge de les seves informacions al Cloud, especialment en entorns on es genera una certa "il·lusió de privacitat", com les xarxes socials, també ancorades al Cloud (MOHAMMED, 2011, pp. 124-125). En aquest sentit, la informació que circula a la xarxa sense cap tipus de control, però que en primera instància ha estat incorporada de manera voluntària pels seus titulars, poden arribar a configurar un perfil bastant complert d'una determinada persona, publicitant la seva privacitat i sense que hi hagi una veritable consciència dels riscos que existeixen (a títol d'exemple, cada vegada més els processos de selecció de personal utilitzen aquests recursos per determinar o contrastar el perfil d'un determinat aspirant).

En aquest context, es qüestiona quin ha de ser el paper dels governs en la regulació del Cloud, especialment en el cas que els proveïdors no adoptin polítiques clares i transparents sobre l'ús, l'emmagatzematge i la protecció de les dades dels seus clients (NELSON, 2009), més en concret tenint en compte la condició de part contractual necessitada d'una protecció reforçada, que es plasma freqüentment en l'establiment d'un fòrum jurisdiccional convenient i l'aplicació de la seva legislació per sobre de la del proveïdor del servei de Cloud.

L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 31, identifica, com a característiques inherents a aquest tipus d'implementació podem citar les següents:

- Terminis més breus per a la posada en marxa del servei.

- No es requereix fer inversió de capital per a la seva implementació.

- Permet l'externalització, a un proveïdor de serveis cloud, de totes les funcions bàsiques de l'empresa.

- Possibilita l'aprofitament de la infraestructura dels proveïdors de serveis, permetent addicionalment una alta escalabilitat i flexibilitat en la modificació del dimensionament del servei.

- Afavoreix la utilització de conjunts de programari estàndard.

- Porta associades unes quotes inicials de pagament més baixes que la resta d'implementacions. Addicionalment els costos del *Cloud* públic són variables, complint el principi de pagament per ús.

- La informació corporativa es troba allotjada en el núvol públic junt amb la de la resta de clients del proveïdor, el que implica, a més de no poder tenir localitzada físicament i ininterrompudament aquesta informació, imposar al proveïdor una sèrie de requisits d'alta exigència en temes de seguretat i protecció de dades.

Així mateix, d'acord amb l'informe sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 (CATTEDDU, 2011: pp. 49 i ss.), aquest model presenta les següents debilitats, amenaces, fortaleses i oportunitats (anàlisi DAFO):

**Debilitats**. Els principals punts febles d'una solució en el *Cloud* públic per les organitzacions governamentals estan relacionats amb la manca de governabilitat, el gran nombre d'abonats (usuaris) en el *Cloud* i el fort poder de negociació del proveïdor del *Cloud* en la definició del contracte. Més detalladament, alguns dels principals punts febles del model de *Cloud* públic des de la perspectiva d'un organisme públic són els següents:

- L'incompliment legal i reglamentari (retenció de dades, informàtica forense, presentació d'informes): aquestes amenaces s'agreugen en els models SaaS i PaaS, on l'usuari té menor control, governabilitat i visibilitat sobre la infraestructura.

- Manca de control sobre la cadena de subministrament: cal assenyalar que, en el cas de IaaS, el control sobre la cadena de subministrament per a la provisió del servei és més gran que en PaaS i SaaS, però aquest benefici potencial sempre ha de ser comparat amb els costos addicionals generats per la plataforma i la gestió de la seguretat del programari i la resistència.

- Capacitats de registre: els proveïdors del *Cloud* públic normalment no ofereixen una capacitat de registre prou detallada sobre les operacions i l'administració del *Cloud* i, potser el més important, hi ha una manca d'informació sobre resposta davant incidents i informàtica forense.

- Dificultats per accedir a dades d'informàtica forense per determinar la traçabilitat i la rendició de comptes (*accountability*) en els casos en què es duen a terme activitats il·legals.

- Manca de la capacitat de negociació necessària per part de determinats organismes públics en la negociació dels termes i les condicions i en la sol·licitud d'un nivell suficient de transparència per part del proveïdor o proveïdors.

- Requisits legals i reglamentaris específics que, en alguns països, obliguen a les organitzacions públiques a mantenir les dades dins del territori nacional i a reduir el grau de continuïtat del negoci que es pot aconseguir.

- El deteriorament del rendiment (IaaS, PaaS i SaaS) degut a la mala qualitat en l'estructuració d'una aplicació i la seva capacitat per explotar de manera dinàmica els recursos disponibles per tal de manejar els errors o els pics de demanda.

- El deteriorament del rendiment (IaaS, PaaS i SaaS) degut de la mala qualitat de la connectivitat (p. ex., zones rurals, especialment en els països del sud i l'est de la Unió Europea). Això només s'aplica en els casos en què el client està situat en àrees específiques.

- Distribució local limitada dels centres de dades en el territori de la Unió Europea, que pot influir en el rendiment del servei. Aquestes consideracions poden ser especialment certes en una situació en què una autoritat pública estigui situada en un lloc remot (p. ex., ENISA a Creta) que pot patir amb major probabilitat un deteriorament del rendiment a causa de la mala qualitat de la connectivitat.

- Dificultats per transferir dades de retorn a l'usuari o al proveïdor alternatiu elegit de serveis en el *Cloud*. Aquestes dificultats poden ser un problema greu, especialment per als serveis de sanitat, en què una fallada o un retard en la transferència d'informació relacionada amb la salut pot representar no tan sols una seriosa amenaça per l'autoritat sanitària, sinó especialment posar en risc als pacients, i no tan sols en el que es refereix a la intimitat d'aquestes dades.

**Amenaces**. Les majors amenaces a què s'enfronten les autoritats públiques en escollir una solució de *Cloud* públic són:

- Un gran *Cloud* públic és un objectiu atractiu per als atacs, a causa de la ingent quantitat d'informació a la qual els atacants poden accedir després de l'èxit dels seus atacs. La mida d'aquesta informació justifica una inversió fins i tot més gran en temps i en recursos per posar en pràctica l'atac.

- L'impacte dels atacs per amenaces de seguretat internes pot ser bastant elevat a causa de la quantitat d'informació emmagatzemada en el *Cloud*. S'han de conservar els registres detallats de les activitats internes, el proveïdor ha d'adoptar polítiques de rotació en l'ocupació i també s'han d'adoptar polítiques de necessitat de saber.

- Una fallada d'aïllament pot provocar una sortida d'informació (seguiment il·legal), així com problemes de funcionament deguts a la manca d'aïllament dels recursos d'altres abonats. En aquest cas, pot produir-se una pèrdua d'informació com a resultat d'un atac contra un altre usuari del *Cloud* públic.

- La inadequada definició dels requisits i de la classificació dels actius pot provocar l'exposició dels actius a altres usuaris del *Cloud*.

- Es poden aplicar múltiples jurisdiccions quan els llocs del proveïdor estiguin distribuïts entre diversos països.

- Un canvi en el control del proveïdor pot donar lloc a l'adopció de diferents estratègies de seguretat així com a estratègies de comercialització diferents que es tradueixin en una menor qualitat del servei.

- En les solucions SaaS o PaaS es pot adoptar un format propietari per emmagatzemar dades en el núvol. El trasllat a un altre proveïdor pot ser gairebé impossible si no hi ha una eina que tradueixi automàticament les dades al nou format.

**Fortaleses**. El model de *Cloud* públic sembla ser el millor posicionat per oferir una gran resistència, en particular pel que fa a les xifres de rendiment i fiabilitat. De forma més detallada, podem dir el següent:

- Disponibilitat i fiabilitat: la major agrupació de recursos simplifica el maneig i l'emmascarament de fallades en recursos de maquinari i ofereix unes xifres més altes de fiabilitat del servei implementat.

- Tolerància i elasticitat: la major agrupació de recursos simplifica el maneig de la pèrdua de rendiment deguda als pics en la demanda, ja que el servei d'interès pot explotar recursos disponibles per evitar una caiguda en el rendiment per als usuaris finals. No obstant això, això requereix el disseny i la implementació adequats de l'aplicació i el control correcte de l'aplicació per detectar pèrdues en el rendiment de l'agent d'usuari. El seguiment és fonamental per a l'explotació dels recursos del núvol i la consecució del compliment d'objectius.

- Administració de pegats: SaaS pot garantir el millor rendiment en el temps mitjà entre pegats. En SaaS, els usuaris tenen menys responsabilitat, però cal incloure els controls adequats per garantir que els pegats s'apliquen realment. En IaaS i PaaS, els usuaris tenen un major grau de responsabilitat.

- Temps de resposta: els rendiments en termes de fiabilitat i elasticitat que es poden aconseguir mitjançant la correcta re-configuració d'una aplicació fan que sigui possible explotar millor els recursos disponibles de manera que el temps de resposta per a l'usuari final pugui sempre mantenir-se dins d'un interval prèviament definit.

- Continuïtat del negoci: els recursos d'un núvol públic implementat per un gran proveïdor poden ser distribuïts geogràficament. Això simplifica la definició de continuïtat del negoci i les estratègies de recuperació davant desastres.

- Seguretat física: es pot aconseguir un grau molt elevat de seguretat en cada lloc del proveïdor gràcies a que ningú està autoritzat a realitzar una auditoria en el lloc i perquè es pot implementar un fort control sobre l'accés físic.

- Prevenció i detecció d'intrusions: donada la gran quantitat de recursos en el *Cloud*, alguns d'aquests poden dedicar-se a la vigilància de la integritat i la detecció d'intrusions per descobrir els atacs maliciosos sense que per això disminueixi el rendiment final a l'usuari.

- Les fortes mesures de seguretat física poden permetre al proveïdor retardar possibles ordres judicials de compareixença i processos d'obtenció de dades (*e-Discovery*) per part de les autoritats policials d'altres països.

La major part dels beneficis es deuen a la significativa mida de l'agrupació de recursos disponibles i la seva distribució geogràfica. L'homogeneïtat dels recursos utilitzats per construir el *Cloud* pot enfortir i simplificar el disseny i la gestió de tot el sistema. Això implica que els punts forts són directament proporcionals a l'escala del proveïdor del *Cloud*.

D'altra banda, si ens plantegem la possibilitat de què aquestes fortaleses que són aplicables a les empreses del Cloud públic puguin ser traslladables en l'àmbit del *Cloud* privat, hem de decantar per la resposta negativa. No és realista imaginar que, en un futur proper, els proveïdors de *Cloud* públic vulguin oferir serveis de *Cloud* privat més específics als que estan ofertant ara, quan els seus destinataris siguin les administracions públiques, ja que la singularitat de les administracions públiques requeriria unes especificats o adaptacions dels seus sistemes que, pel que fa als costos que suposaria, no en resultaria rendible.

**Oportunitats**. En comparació amb les solucions internes, els *Clouds* públics podrien oferir oportunitats per millorar les pràctiques actuals dels potencials usuaris governamentals, en les àrees de preparació i compliment legal i, més encara, en particular en relació amb:

- Anàlisi i avaluació de riscos.

- Proves de seguretat.

- Supervisió de la seguretat en temps real.

- Informàtica forense.

Això es deu a les següents raons:

- És difícil comptar amb personal intern especialitzat per dur a terme, de manera periòdica, les anàlisis i les avaluacions de risc, així com les proves de seguretat.

- Comptar amb els recursos necessaris per construir un centre d'operacions de seguretat intern per supervisar la seguretat en temps real o bé adquirir aquests serveis en el mercat, és costós.

- Les pressions del mercat o dels competidors que obliguin els proveïdors de núvol pública a oferir funcions de seguretat representarà un valor afegit per als clients.

- Pressió davant el compliment.

Perquè un *Cloud* públic pugui aprofitar aquestes oportunitats, s'han de prendre les següents mesures:

- Control total sobre els inventaris de béns.

- Classificació detallada dels actius físics, informació i serveis.

- Integració entre l'anàlisi / avaluació de riscos i els processos de supervisió de la seguretat en temps real.

- Inspecció eficaç dels empleats del proveïdor.

Com ja hem indicat (ALAMILLO DOMINGO, 2012: p. 53), el *Cloud* públic és el model de desplegament dominant pel que fa a reducció de costos, però veurem que també és el model que més reptes de deslocalització comporta (i, en conseqüència, de potencial manca de privacitat i de compliment normatiu), incloent l'absència de control pels usuaris, l'ús secundari potencial no autoritzat de la informació – com en el cas de la publicitat dirigida per continguts –, la proliferació de dades i moviments transfronterers de dades, i l'aprovisionament dinàmic (PEARSON *et al*., 2009, p. 694).

L'informe de la ONTSI, 2012: p. 44, indica que els serveis de *Cloud* públic també tindran el seu encaix en els models tecnològics de les administracions públiques en àmbits tecnològics de menor criticitat: el correu electrònic d'empleats, les aplicacions d'escriptori, les aplicacions departamentals, els portals i xarxes d'informació i participació pública, etc. són potencialment externalitzables a proveïdors de *Cloud*.

En aquest sentit, és rellevant plantejar-se que no tota o qualsevol actuació administrativa és traslladable al núvol, sinó que, en primera instància, el principi de prudència portaria a traslladar inicialment al cloud aquells serveis o aquelles informacions en què els riscos siguin menys elevats.

4. *Cloud* híbrid, en que la infraestructura *Cloud* és una composició de dues o més infraestructures Cloud diferents (privada, comunitària o pública) que romanen entitats unívoques, però que es troben vinculades per tecnologia estàndard o propietària que permet la portabilitat de les dades i aplicacions (per exemple, el *Cloud bursting*[4] per al balanceig de càrrega entre Clouds).

L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 32, identifica, una sèrie de característiques inherents a aquest tipus d'implementació. Podem citar les següents:

[4]El *Cloud bursting* o núvol d'explosió és un model d'implementació d'aplicacions en el que una aplicació se executa a un núvol privat o centre de dades i explota a un núvol públic quan ho demanen els pics de la capacitat de computació. L'avantatge d'aquest desplegament del núvol híbrid és que una organització només paga pels recursos informàtics addicionals quan es necessiten (AREA, 2010).

- Ofereix una major flexibilitat en la prestació de serveis de TI, alhora que es manté un major control sobre els serveis de negoci i de dades.

- Amb una solució de *Cloud* híbrid, igual que en els casos esmentats anteriorment, s'aconsegueix una ràpida posada en servei.

- Implica major complexitat en la integració de la solució *Cloud*, com a conseqüència de ser una solució que es compon de diferents tipus d'implementació de serveis en el núvol.

- Permet integrar les millors característiques dels diferents tipus de solucions *Cloud*, pel que fa al control de les dades i a la gestió de les funcions bàsiques de l'entitat.

- Permet la selecció, per part del proveïdor, d'infraestructura escalable i flexible, oferint una alta agilitat en el redimensionament de la solució.

- Permet el control intern dels serveis *Cloud* des de la pròpia entitat.

Como anota GARCÍA SÁNCHEZ, 2012: p. 29, aquest tipus de núvols són una possible solució per a la gestió de dades en organitzacions complexes, de manera que les dades crítiques o que es troben sotmeses a requeriments legals específics siguin gestionats per la part privada del núvol al mateix temps que la resta de la informació de negoci és processada en una infraestructura pública o comunitària.

Avançant-nos a les conclusions d'aquesta recerca, sembla que el *Cloud* híbrid (privat o comunitari funcionant en conjunció amb el públic) seria el que permetria a les administracions públiques utilitzar aquesta tecnologia de la manera més eficient, compatibilitzant l'actuació administrativa amb les previsions i prevencions legalment aplicables. En aquest sentit, funcionaria com un model multiservei, en funció de la singularitat i especificats de cadascun dels serveis, tot i que prèviament es requeriria una anàlisi o programació molt exhaustiva de l'arquitectura que es vol dur a terme.

Si no es realitza aquesta planificació prèvia, s'estan assumint els riscos de què la solució inicialment adoptada de *Cloud* híbrid no permeti ampliar o desenvolupar el model. En resum, una solució com aquesta s'hauria de fer sota la perspectiva de futur i l'anàlisi previ de on caldria encaixar els diferents serveis que, en el futur, s'hagin d'incorporar al *Cloud*. D'aquesta manera, estaria prèviament definit el model de desenvolupament, sense assumir el risc de que aquest esdevingui, des dels seus inicis, ineficient.

En qualsevol cas, abans d'entrar en els processos de decisió administratius, una vegada definits els diferents tipus de *Cloud*, cal definir igualment els diferents models de negoci existents en aquest àmbit, el que abordem tot seguit.

## 1.5 Els models de negoci del *Cloud computing*

L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 33, identifica els següents models de negoci:

1. Proveïdor de *Cloud*: Consisteix en la prestació de serveis a través del núvol a subscriptors o intermediaris, és a dir, servei ofert per l'empresa proveïdora al client, ja sigui de forma directa o a través d'un intermediari. La contrapart del proveïdor és el subscriptor, que seria l'usuari dels propis serveis *Cloud*.

2. Intermediari de *Cloud*: Aquest model de negoci consisteix en la prestació de serveis d'intermediació entre els usuaris finals i els proveïdors, en un mercat dinàmic d'oferta i demanda com és el *Cloud computing*.

3. Facilitador de *Cloud*: Aquest model de negoci és un model típicament enfocat al mercat de proveïdors de Cloud. Són empreses que venen programari i maquinari a tercers, perquè aquestes terceres empreses (proveïdors) desenvolupin i ofereixin a l'usuari serveis en el núvol.

4. Auditor de *Cloud*: L'auditor és el model de negoci encarregat de dur a terme les avaluacions independents dels serveis en el núvol, de les operacions associades als sistemes d'informació, del rendiment i de la seguretat en l'ús de la solució *Cloud*.

## 1.6 La implantació del *Cloud computing* a les Administracions Públiques

De l'anàlisi previ anteriorment exposat i del treball de camp dut a terme, es posa de manifest l'important interès que la implantació del *Cloud computing* desperta a les administracions públiques. Els avantatges, especialment des de la vessant de l'eficiència econòmica, fan que les administracions públiques estiguin cercant o analitzant quins són els àmbits de desenvolupament natural d'aquests serveis, sense que els riscos que es puguin assumir siguin excessivament alts. Tot i això, es constata que, a hores d'ara, la seva adopció és encara molt baixa, llevat d'experiències molt concretes, que majoritàriament s'han desenvolupat en l'àmbit del correu electrònic.

En sentit similar es manifesta l'estudi de la ONTSI, 2012: p. 202, que indica que no s'han emprès experiències globals efectives en matèria d'adopció del *Cloud computing* a les Administracions Públiques espanyoles. No obstant això, cal destacar que molts organismes públics estan realitzant una fase prèvia de reflexió i prospectiva dels avantatges i beneficis que pot suposar l'adopció del *Cloud* en l'àmbit dels serveis tecnològics de les Administracions Públiques, així com estan començant a determinar els condicionants tècnics, i especialment jurídics, que caldria tenir present a l'hora d'incorporar el *Cloud computing* a les seves organitzacions.

Cada vegada és més habitual que els plans directors de sistemes o reflexions estratègiques en l'àrea de TI es focalitzin en el *Cloud computing* com a clara alternativa de evolució tecnològica. Per aquesta raó, és d'esperar que, en funció del cost de migració i els avantatges obtinguts, durant els propers anys es percebrà una important dinamització dels projectes i actuacions *Cloud* en l'àmbit del sector públic.

En aquest sentit, l'estudi esmentat indica que al juny de 2011 en el si d'un grup de treball per a la implantació de infraestructures compartides en l'Administració General de l'Estat es va arribar a diverses conclusions sobre el procés de consolidació de serveis i infraestructures de suport i les línies estratègiques que han de prevaler en el futur. D'aquestes conclusions cal destacar les següents:

- Es postula la definició d'un pla director per a l'evolució i racionalització de les TIC a les Administracions Públiques, aplicant les premisses de consolidació i centralització de serveis compartits.

- Aquesta evolució està marcada per un impacte en la gestió i organització del model. Les competències d'aquests serveis han de ser assumides per una unitat i s'han d'articular els models de col·laboració i servei entre els organismes públics (convenis, pagament per ús, etc.).

- L'abast d'aquesta evolució tecnològica ha de ser global i plantejar en un model de *community cloud* per a totes les administracions públiques espanyoles, integrant igualment a Administracions autonòmiques i locals.

- Els serveis que es prioritzen per la seva estandardització seran de tres tipus:

    - La consolidació de les infraestructures, CPDs, entorns i sistemes d'emmagatzematge.

    - La consolidació de les plataformes tecnològiques comunes com el correu electrònic, portals, gestors de continguts, bases de dades, etc.

- La consolidació dels sistemes d'informació que implementen els serveis horitzontals de qualsevol tipologia d'Administració com els recursos humans, la nòmina, els registres, la formació, l'administració electrònica o la gestió economicofinancera, entre d'altres.

Val a dir que aquest estudi de la ONTSI, 2012: pp. 203-204, sembla tenir un enfocament certament orientat a la reconversió de molts dels actuals serveis comuns d'Administració electrònica al nou model, quan argumenta que, depenent del que s'entengui per model *Cloud*, existeixen projectes i experiències que s'han emprès durant els últims anys que es poden acollir i entendre tal com varen ser inicialment configurats o, pel contrari, adequar-se o adaptar-se a la línia de la filosofia que caracteritza al *Cloud computing*.

Des d'aquest punt de vista, s'han emprès actuacions per oferir serveis compartits, les característiques i implementacions dels quals permetran el seu desenvolupament com serveis *Cloud*. I aquesta implementació ha de ser possible al marge de que no hagin estat inicialment etiquetades com *Cloud*, però que en el seu desenvolupament s'adaptin a les condicions d'implementació i servei que són característiques pròpies del *Cloud*. Això seria aplicable, per exemple, als serveis de notificació, signatura electrònica, intermediació de dades o processos de gestió de personal.

L'estudi de la ONTSI, 2012: p. 209, conclou que el *Cloud computing* s'acabarà implantant en les Administracions Públiques espanyoles en un marc temporal no superior a quatre anys, encara que sempre amb un caràcter més conservador que l'adopció en l'àmbit privat.

D'altra banda, es considera que les administracions públiques haurien de prendre un rol impulsor per afavorir la reactivació del sector TIC i optimitzar els costos d'operació de les Administracions Públiques. No obstant això, cal tenir present que el paper impulsor de les administracions públiques no pot ser sempre inqüestionable, especialment si atenem a la situació de dèficit públic en què ens trobem actualment, que ha reduït molt significativament la capacitat inversora de les administracions públiques.

Per aquesta raó, tractant-se d'una tecnologia que s'està estenent de manera molt significativa en l'àmbit privat, tant des de la vessant exclusivament de l'oci i la condició de consumidor o usuari, com des de la vessant de serveis de valor afegit a les empreses, semblaria que s'ha d'aprofitar el paper dels proveïdors i la intensitat comercial i mediàtica del mercat per imposar aquest model de manera efectiva i reduir els terminis d'adopció i adaptació del sector.

Això passaria necessàriament per aprofitar al màxim els serveis ja existents, mirant d'adaptar-los el màxim possible a les singularitats de les administracions públiques, per anar avançant en aquest camp, sota el paradigma de la seguretat jurídica.

Això ens portarà probablement a una multiplicitat de solucions. Així, el futur de les tecnologies de la informació en el sector públic tindrà probablement un caràcter mixt en el qual conviuran sistemes d'informació propis, el *hosting* tradicional i solucions *Cloud* de qualsevol naturalesa de tipus públic i privat.

Per aquesta raó, la necessària existència de múltiples solucions a cadascun dels problemes, serveis o actuacions que hagin de dur a terme les administracions públiques requereix una planificació concreta i clara des dels seus inicis, als efectes de treure el màxim de possibilitats a aquesta nova tecnologia i, d'altra banda, evitar els riscos de mancances de coordinació o de planificació que, en última instància, puguin derivar en ineficiències econòmiques, com a conseqüència de la necessitat de tornar a redissenyar arquitectures, programes o decisions. Molt probablement aquesta situació no afectarà a l'expansió del *Cloud*, ja que és una realitat de futur, però s'ha de tractar d'evitar els riscos que es produeixin ineficiències econòmiques i demores en la implantació i expansió del *Cloud* (el que, en última instància, seria també una ineficiència econòmica).

# 2 Els riscos legals associats a l'ús del *Cloud computing* per part de l'Administració

Ja hem indicat que la incorporació per part de les administracions públiques del *Cloud computing* és una decisió que, sota una adequada planificació, no pot sinó suposar beneficis. Per aquesta raó, qualsevol planificació passa per analitzar, al marge dels beneficis que es puguin derivar, quins són els riscos legals associats al seu us i, en la mesura del possible, adoptar les mesures necessàries per tal que aquests riscos siguin inapreciables. Finalment, cal tenir present que, tractant-se de l'actuació administrativa, hi ha límits que són infranquejables, per molt grans que puguin ser els beneficis econòmics que es derivin. En aquest sentit, el principi de legalitat, el principi de seguretat jurídica, o els drets dels ciutadans reconeguts per l'ordenament jurídic són límits que s'han de considerar en qualsevol decisió a adoptar.

Amb la finalitat de ponderar les decisions a prendre, en aquest capítol introduïm els principals riscos legals associats a aquest paradigma de computació, per a la qual cosa definim, en primer lloc, els conceptes essencials de l'anàlisi de riscos i, en particular, dels riscos legals.

El mètode de treball utilitzat considera, per a cada possible risc, la descripció de l'amenaça legal que suposa (típicament, identificant si la conducta descrita en el cas d'ús potencialment implica la infracció d'una norma jurídica, i per tant, suposa una situació de exposició al perill subjacent a l'amenaça). Així mateix, es valora la probabilitat que es materialitzi aquesta amenaça (de forma qualitativa), i l'impacte (en general, també de forma qualitativa, encara que en el cas de la LOPD i altres regulacions amb un règim estricte d'infraccions és possible emprar el criteri quantitatiu corresponent a l'import de la sanció corresponent).

La fórmula de càlcul de risc més habitual és la següent:

$$Risc_{(amenaça)} = probabilitat * impacte$$

L'anàlisi de riscos es basa en la identificació d'amenaces, que es poden veure com la conjunció d'esdeveniments de perill i situacions d'exposició als esmentats perills. Una amenaça pot estar constituïda per una col·lecció d'esdeveniments de perill, ja que l'amenaça es descriu de manera més genèrica que els concrets perills o situacions que exposició que poden conduir a ella.

Mentre que un esdeveniment de perill ve donat per una acció externa, com un atac o un esdeveniment natural, o bé interna, com a error o omissió propi, una situació d'exposició al perill ve donada per l'actitud de la persona que s'exposa a que el perill es materialitzi, bé per la seva conducta arriscada o falta de diligència deguda.

En una amenaça jurídica, l'esdeveniment de perill consisteix en una conducta de tercer o en una omissió pròpia que deriva en un resultat que es troba tipificat com una infracció de l'ordenament jurídic. La situació d'exposició deriva de la diligència aplicada per complir l'objectiu marcat per la regulació (que pot ser fer alguna acció – normes de obligació – o en abstenir de fer-la– normes de prohibició).

## 2.1 Riscos legals derivats de la deslocalització pròpia del *Cloud computing*

La deslocalització territorial s'identifica com a risc legal principal, en atenció a la dificultat d'aplicar les normes jurídiques, típicament territorials, a l'espai de la xarxa (SANCHO VILLA, 2010; MOLES PLAZA, 2004; DE MIGUEL ASENSIO, 2001;MUÑOZ MACHADO, 2000, entre d'altres), una dificultat que s'exacerba en el cas del *Cloud computing*.

I és que com hem vist anteriorment, el *Cloud*, especialment la infraestructura com a servei – IaaS, es troba principalment suportat per tecnologies de virtualització de servidors, de xarxes i d'emmagatzematge, que condueixen a la creació i interconnexió de grans centres de processament de dades, sovint anomenades "granges de servidors", localitzats en ubicacions amb disponibilitat de terreny per edificar, una imposició tributària moderada, elevada connexió a les xarxes troncals d'Internet i disponibilitat de potència elèctrica al menor cost possible, donat l'elevat consum que aquestes infraestructures requereixen (JAEGER *et al*., 2009); creant una xarxa de centres interconnectats que comparteixen les dades, per exemple per garantir la continuïtat de negoci davant desastres naturals, o per apropar el processament de les dades als usuaris (SCHOO *et al*., 2010, p.4)

La possibilitat d'ubicar centres de dades en qualsevol lloc no només és real, sinó que a més s'aprecia una tendència important a la seva mobilitat, com en el cas dels centres de dades en contenidors de transport intermodal, que es poden transportar a la carta (MILLER, 2006) o fins i tot situar en aigües internacionals (SLAWSKI, 2009), amb totes les implicacions que comportaria l'intent d'inaplicació de les jurisdiccions nacionals.

Si en la infraestructura com a servei pot, com hem vist, ser difícil establir la ubicació física de les dades, en el cas de la plataforma com a servei, i encara més en el cas del programari com a servei, senzillament és impossible.

Els aspectes legals associats a la infraestructura com a servei a considerar inclouen les qüestions jurisdiccionals, la comprensió i l'evolució dels drets dels actors del Cloud - proveïdors i usuaris finals - i les possibles solucions tècniques als anteriors (HAY *et al*., 2011: pp. 5-6), qüestions totes elles molt lligades a la connexió entre la localització de les dades i la ubicació dels centres de processament de dades.

Com s'indica a l'estudi sobre *Cloud computing* publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2009, els governs, igual que el sector privat, també estan interessats en la possibilitat d'utilitzar la computació en núvol per reduir els costos informàtics i incrementar les seves capacitats. Els governs també han de superar obstacles considerables, en termes de percepció pública del processament segur de la informació personal dels ciutadans en les infraestructures de computació en núvol. A més, també hi ha obstacles legals i normatius que impedeixen el canvi de moltes aplicacions de "administració electrònica" al núvol. No obstant això, tant governs com PIME s'enfronten a la realitat que molts dels seus empleats utilitzaran serveis basats en el núvol independentment que això formi part de la seva política oficial (CATTEDDU i HOGBEN, 2009a: p.5).

Aquest estudi identifica riscos legals específics del *Cloud* (CATTEDDU i HOGBEN, 2009a: p.10), associats a la deslocalització pròpia d'aquesta modalitat de prestació de servei, quan es produeixen incidències o irregularitats en la prestació del servei, i la capacitat de reacció davant d'aquestes:

1. Ordres judicials i descobriment electrònic. En cas de confiscació de maquinari físic arran d'una ordre judicial de les forces policials o de demandes civils, la centralització de l'emmagatzematge i el fet que diversos clients comparteixin el maquinari físic implica que hi ha un nombre més gran de clients que corren el risc de que les seves dades es revelin a parts no desitjades. A més, cal tenir present que una mesura de caràcter general com aquesta podria afectar a tercers que, de manera legítima utilitzen els serveis cloud i, en principi, no haurien de resultar afectats per la mesura adoptada.

   Cal assenyalar que, en relació amb aquest extrem, això no ha de suposar que les mesures per al compliment de la llei mitjançant ordres judicials siguin inacceptables (tot i que algunes poden arribar a ser-ho, especialment, en països en què, com indiquem a continuació, les garanties de l'Estat de Dret no han estat plenament desenvolupades), sinó que, en ocasions, les confiscacions legítimes de maquinari (que semblen ser inusuals) poden afectar altres clients que no són objecte de les actuacions repressives, depenent de la manera com estiguin emmagatzemades les dades.

   Per una altra banda, podria ser impossible en un futur proper que les forces d'una única nació confisquessin "un *Cloud*", a la vista dels avenços previstos en relació amb la migració d'hipervisors a llarga distància[5].

   L'estudi avalua aquest risc com alt, ja que considera que la seva probabilitat d'ocurrència és alta i que el seu impacte sobre l'organització seria mitjà, afectant principalment al renom de l'organització, la confiança del client, les dades personals i la prestació del servei, que són actius de valor alt o molt alt (CATTEDDU i HOGBEN, 2009a: p. 48).

[5]Aquesta tècnica permetria reubicar de forma molt ràpida les imatges computacionals dels sistemes carregats al Cloud en un altre espai, el que afectaria a la efectivitat de la mesura.

Les vulnerabilitats identificades són les següents:

a. Manca d'aïllament dels recursos[6].
b. Emmagatzematge de dades a jurisdiccions múltiples i manca de transparència sobre aquest punt.
c. Manca d'informacions sobre jurisdiccions.

2. Risc derivat de canvi de jurisdicció. Les dades dels clients poden allotjar-se en múltiples jurisdiccions, algunes de les quals poden ser d'alt risc. Si els centres de dades estan ubicats en països d'alt risc, per exemple, aquells en què no impera l'Estat de dret el marc jurídic i execució de lleis són impredictibles, els Estats policials autocràtics, els estats que no respecten els acords internacionals, etc., els llocs podrien ser objecte d'incursions de les autoritats locals i les dades o sistemes podrien ser divulgats o confiscats per la força.

   L'estudi avalua aquest risc com alt, ja que considera que la seva probabilitat d'ocurrència és molt alta i que el seu impacte sobre l'organització seria alt, afectant principalment al renom de l'organització, la confiança del client, les dades personals i la prestació del servei, que són actius de valor alt o molt alt (CATTEDDU i HOGBEN, 2009a: pp. 48-49).

   Les vulnerabilitats identificades són les següents:

   a. Manca d'informacions sobre jurisdiccions.
   b. Emmagatzematge de dades a jurisdiccions múltiples i manca de transparència sobre aquest punt.

Per al NIST, la localització física de les dades gestionades pel proveïdor de serveis *Cloud* és una de les qüestions pendents de solució satisfactòria, especialment atenent a la necessitat de compliment de les lleis i regulacions que prohibeixin l'emmagatzematge o el processament transfronterer de dades (NIST, 2011: pp. 8-6), tot i que en les seves recomanacions per a l'ús del *Cloud* figura clarament la regulació per via de contracte negociat de l'obligació del proveïdor de mantenir les dades en el territori o territoris indicats per l'Administració (NIST, 2011: pp. 30-31, 35; JANSEN, 2011).

En sentit similar, l'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 (CATTEDDU, 2011: p. 7) indica que les legislacions nacionals dels Estats membres de la Unió Europea actualment imposen algunes restriccions a la circulació de dades fora del territori nacional i, a més, existeix un problema per a la determinació de la legislació aplicable quan les dades estan sent emmagatzemats i processades fora de la Unió Europea o per un proveïdor de serveis de fora

[6]L'ús de recursos per part d'un client por afectar a l'ús de recursos per part d'un altre client, especialment en atenció a les vulnerabilitats en el model de seguretat de l'hipervisor(CATTEDDU i HOGBEN, 2009a: pp. 58-59).

de la UE. Les principals preguntes que cada organisme públic i, en general cada govern central de la UE han de tenir en compte són:

- Si els marcs legals es poden modificar per facilitar la comunicació, tractament i emmagatzematge de dades fora del territori nacional, sense exposar la seguretat i privacitat dels ciutadans i la seguretat nacional i l'economia a riscos inacceptables;

- Si és així, si les dades dels ciutadans que es desplacen fora del territori nacional és un risc que es pot assumir;

- Si l'equilibri entre els riscos de pèrdua de control sobre les dades i els efectes beneficiosos de la distribució geogràfica és positiu.

En aquesta línia de precaució, cal tenir present que el marc d'assegurament de la informació proposat per ENISA l'any 2009 recomana als Governs, en termes força contundents, no fer ús del Cloud públic excepte en relació amb dades que requereixin un nivell mínim d'assegurament (CATTEDDU i HOGBEN, 2009b: p. 11).

Finalment, per completar aquesta visió general, resulta força interessant recollir algunes de les conclusions de l'estudi publicat per INTECO sobre riscos i amenaces en *Cloud computing* (2011: pp. 30 i ss.):

- La seguretat i la propietat de les dades és un dels aspectes clau en el *Cloud computing*. Els informes mostren una gran preocupació per la propietat i el tractament de les dades ja que aquestes infraestructures poden gestionar les dades en múltiples països el que pot generar conflictes pel que fa al marc legal en què són tractats. També es planteja que aquests entorns, en manejar gran quantitat de dades, poden ser objecte de fuites d'informació, ja siguin intencionades o fortuïtes.

- El compliment normatiu també és un dels pilars de la seguretat en entorns *Cloud*. En aquest cas el problema es presenta a causa de la manca de transparència d'aquestes infraestructures, pel que és molt recomanable que el subscriptor del servei s'informi clarament de com es gestiona l'entorn.

- Per a la creació d'un servei *Cloud* intervé multitud de programari de diferents proveïdors. És a dir, són entorns complexos pel que s'ha de posar especial atenció a les possibles vulnerabilitats del mateix i implantar procediments d'actualització de programari.

- Un altre dels aspectes considerats importants és la identitat i el control d'accés. En general, la majoria de les infraestructures són compartides per múltiples empreses o usuaris i la mala definició dels controls d'accés pot provocar accessos no autoritzats a dades

confidencials. La definició d'una bona política d'identitat i control d'accés basada en polítiques de mínim privilegi és essencial en entorns *Cloud*.

- Finalment, hi ha un denominador comú a tots aquests aspectes esmentats. Es tracta dels contractes d'acord de servei. Totes les recomanacions pel que fa a aquest assumpte indiquen que aquests han de ser revisats i creats específicament, detallant els controls, les normatives, les mesures de protecció, els terminis de recuperació del servei, etc.

Tanmateix, també hi ha autors que consideren que, en relació amb aquest riscos, i com freqüentment succeeix amb les qüestions complexes tècnica i legalment, ràpidament s'han establert simplificacions i generalitzacions excessives de la realitat, termes de moda i lemes dels quals s'abusa per tal de fomentar les agendes polítiques i de competitivitat, incloent-hi la protecció dels llocs de treball local o de les indústries radicades en territori nacional, i un intent de protegir models de negoci establerts de pràctiques disruptives (DETERMANN, 2011: p. 1, que presenta els que anomena dotze mites sobre privacitat de dades al *Cloud*).

Al respecte, la disposició addicional 1ª del Text refós de la Llei de contractes del sector públic, aprovat per Reial decret legislatiu 3/2011, de 14 de novembre (TRLCSP) regula la contractació de serveis en el estranger i, en relació amb aquest extrem, s'indica:

"(...)

2. En los contratos con empresas españolas se incluirán cláusulas de sumisión a los Tribunales españoles.

3. En los contratos con empresas extranjeras se procurará, cuando las circunstancias lo aconsejen, la incorporación de cláusulas tendentes a resolver las discrepancias que puedan surgir mediante fórmulas sencillas de arbitraje. Igualmente se procurará incluir cláusulas de sumisión a los Tribunales españoles. En estos contratos se podrá transigir previa autorización del Consejo de Ministros o del órgano competente de las Comunidades Autónomas y entidades locales".

D'aquesta manera, el caràcter improrrogable de la jurisdicció espanyola serà la regla general, tot i que en determinades ocasiones, especialment en el cas del Cloud públic, en què ens trobem en moltes ocasions davant de contractes d'adhesió, serà una dificultat afegida la singularització de les clàusules de submissió a determinats Tribunals estrangers, en el cas que així es prevegi.

## *2.2* Riscos de protecció de les dades personals al *Cloud*

Pel que fa al Cloud, un dels riscos més considerats i tractats a nivell doctrinal és el corresponent a la protecció de dades de caràcter personal.

L'estudi sobre *Cloud computing* publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2009 indica que el *Cloud computing* planteja diversos riscos específics relatius a la protecció de dades tant per a clients en *Cloud* com per proveïdors en *Cloud*. En alguns casos, pot resultar difícil per al client en *Cloud* (en la seva funció de controlador de dades[7]) comprovar de manera eficaç les pràctiques de gestió de dades del proveïdor[8] en *Cloud*, i en conseqüència, tenir la certesa que les dades són gestionats de conformitat amb la llei (CATTEDDU i HOGBEN, 2009a: p. 10).

Aquest problema es veu exacerbat en els casos de transferències múltiples de dades, per exemple, entre *Cloud* federats. D'altra banda, alguns proveïdors en *Cloud* proporcionen informació sobre les seves pràctiques de gestió de dades. Altres també ofereixen resums de certificació sobre les seves activitats de processament i seguretat de dades i els controls de dades a què se sotmeten, per exemple, la certificació SAS 70.

L'estudi avalua aquest risc com alt, ja que considera que la seva probabilitat d'ocurrència és alta i que el seu impacte sobre l'organització seria alt, afectant principalment al renom de l'organització, la confiança del client, les dades personals i la prestació del servei, que són actius de valor alt o molt alt (CATTEDDU i HOGBEN, 2009a: pp. 49-50).

Les vulnerabilitats identificades són les següents:

1. Manca d'informacions sobre jurisdiccions.
2. Emmagatzematge de dades a jurisdiccions múltiples i manca de transparència sobre aquest punt.

BALBONI, 2010: p. 5, recorda que a més, en opinió del Supervisor Europeu de Protecció de Dades, un dels principals problemes precisament rau en el fet que la directiva de protecció de dades no s'aplica als proveïdors de Cloud establerts fora del territori de l'EEE, per la qual cosa resultaria convenient modificar la regulació[9].

També l'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 identifica els següents aspectes a considerar en relació amb el compliment de la normativa de dades personals (CATTEDDU, 2011: pp. 41-44):

1. Restriccions a l'aplicació de la Directiva 95/46/EC (article 13.1 Directiva 95/46/CE). D'acord amb el que determina l'article 13.1 de la Directiva, els Estats membres poden restringir

[7] Responsable del fitxer o del tractament, en terminologia de la legislació espanyola de protecció de dades.
[8] Que actuaria com encarregat del tractament.
[9] Com es sabut, la Comissió Europea ha presentat un esborrant de Reglament de protecció de dades que resultaria aplicable als proveïdors no establerts a la Unió Europea que adrecessin els seus serveis als ciutadans europeus, de forma semblant al tractament de la legislació aplicable a les relacions de consum.

l'aplicació de determinades previsions de la Directiva en relació amb la seguretat nacional o seguretat pública, o la prevenció i persecució dels delictes. Per tant, en alguns casos les dades gestionades per l'Administració no es troben sotmeses a tota la regulació de la Directiva.

2. Responsable del tractament i encarregat del tractament (articles 2.d i .e Directiva 95/46/CE). Resulta necessari identificar al responsable del tractament i a l'encarregat del tractament, i les seves interaccions per determinar qui és obligat al compliment amb les normes de protecció de dades, com poden exercir els seus drets, quina és la llei nacional aplicable i com poden actuar de forma efectiva les autoritats de protecció de dades.

La Directiva 95/46/EC distingeix de forma clara entre responsable i encarregat quan indica que [...] aplicar aquesta definició [d'encarregat] a l'entorn del *Cloud computing* és un repte important. Inicialment es pot concloure que l'Administració és el responsable i el proveïdor del Cloud l'encarregat. Tot i això, sovint els proveïdors de Cloud determinen els mitjans i, de vegades, la finalitat del tractament, entrant en la definició de responsable.

En sentit similar es manifesta la doctrina. Per a RUBÍ NAVARRETE, 2012: pp. 91 i ss., el punt de partida per determinar la posició jurídica dels participants en la prestació de serveis Cloud és polièdrica, en especial en atenció a les diverses modalitats de desplegament. Així, mentre que en el cas d'una organització que utilitza el Cloud privat ens trobem, en general, amb un responsable del tractament (amb la possibilitat de encarregats de tractament si part de la infraestructura es contracta a tercers), en canvi en la resta de modalitats podem partir de la consideració del prestador com a encarregat del tractament, tot i la forta capacitat de decisió que ostenta sobre la definició i prestació del servei.

De l'aplicació de la LOPD al responsable del tractament, que en el nostre cas resulta indubtable per tractar-se d'Administracions Públiques, l'autor esmentat en deriva l'aplicació de l'article 12 de l'esmentada llei i els articles 20 a 22 del reglament que la desenvolupa.

Per la seva banda, GILBERT, 2011: pp. 4-5, nota l'existència d'una important contradicció entre la enorme capacitat de decisió i organització dels tractaments de dades per part dels proveïdors de serveis de Cloud envers la qualificació d'encarregats del tractament, per la qual cosa, amb base en la Opinió del Grup de Treball 29 de la Directiva, WP 169, considera més adequada la tipificació simultània de client i proveïdor de servei *Cloud* com a responsables del tractament, si bé amb una graduació diferent de les responsabilitats de cadascun en funció del cas concret.

HON *et al*., 2011: pp. 12-15, critiquen que la majoria de contractes de serveis *Cloud* no caracteritzen de forma clara i suficient la seva condició com responsables o encarregats del tractament de les dades de caràcter persones que reben. I defensen que en alguns casos un proveïdor de Cloud no és ni responsable ni encarregat del tractament, ja que la provisió de recursos de computació, en la seva opinió, no té perquè implicar cap accés a

dades que no sigui purament incidental. D'acceptar-se aquest argument, que per una altra banda ens resulta raonable en una interpretació equilibrada de la directiva quant a l'accés a dades per a la prestació de serveis, sempre que realment no s'utilitzés com a via de fugida de la legislació en perjudici dels usuaris, es desplegaria millor aquest nou paradigma computacional.

3. Controls previs (article 20 Directiva 95/46/CE). En funció del tipus de servei i de les dades personals objecte de tractament, d'acord amb la legislació nacional podria ser necessari realitzar controls previs al tractament.

4. Mesures tècniques i organitzatives adequades (article 17 Directiva 95/46/CE): integritat de dades, gestió d'identitat i control d'accés. La integritat de les dades i la disponibilitat són elements essencials en la provisió de serveis de *Cloud computing*. D'acord amb la Directiva 95/46/CE, el responsable del tractament i els seus encarregats d'implementar mesures tècniques i organitzatives per protegir les dades personals contra la seva destrucció accidental o il·lícita o la pèrdua accidental, alteració, divulgació o accés no autoritzat, tenint en compte l'estat de la tècnica i el cost de la seva implementació, aquestes mesures han de garantir un nivell de seguretat adequat en relació amb els riscos representats pel tractament i la naturalesa de les dades a protegir (article 17).

   El problema és que el concepte de "adequat" s'ha interpretat de diferents maneres en els diferents estats membres de la Unió Europea. Així, encara que els proveïdors de serveis en el núvol apliquen molt sovint normes tècniques reconegudes (per exemple, ISO 27001) per assegurar les dades dels clients, aquestes poden no ajustar perfectament als requisits nacionals pel que fa a les mesures que és adequat adoptar. Cal una major coherència i harmonització a nivell de la Unió Europea. A més, val la pena tenir en compte l'elevat nivell de seguretat de les dades que s'ha d'exigir a un proveïdor de serveis en el núvol en un context de sanitat electrònica, amb especial atenció a la gestió d'identitats i el control d'accés.

5. Filtració de dades i notificació d'incidents de seguretat (no obligatori, encara). El marc revisat de la Unió Europea per a les comunicacions electròniques aclareix les responsabilitats dels operadors de xarxes i els proveïdors de serveis, incloent la seva obligació de notificar violacions de la seguretat de les dades personals (articles 4 i 13). La revisió del marc general de protecció de dades iniciat recentment inclourà una possible extensió de l'obligació de notificar les violacions de seguretat de les dades.

   Si les regulacions europees sobre protecció de dades van en aquest direcció, caldrà que s'identifiqui clarament el grau de violació de la seguretat de les dades que s'ha de notificar, a qui s'ha de notificar (client del proveïdor de serveis en el núvol, autoritat competent pel que fa a protecció de dades, interessats) i les modalitats pertinents. Una obligació indeterminada de notificar qualsevol violació (fins i tot les menors o insignificants) de la seguretat de les dades pot perjudicar greument als proveïdors de serveis en el núvol i

generar una alarma innecessària dels governs, les administracions públiques i els ciutadans en general.

6. Transferència de dades a països de fora de l'Espai Econòmic Europeu (articles 25-26 Directiva 95/46/CE). Els models en el *Cloud* suposen que la informació i les dades del client poden implicar la transferència de dades per part del proveïdor de serveis en el *Cloud* des d'un centre de dades a l'Espai Econòmic Europeu (EEE) a un altre que pot estar ubicat en qualsevol part del món. No obstant això, la Directiva 95/46/CE prohibeix les transferències de dades personals des del EEE a països que no garanteixin un nivell adequat de protecció en el sentit de l'article 25.2, llevat que l'interessat hagi donat prèviament el seu consentiment inequívoc a la transferència proposta o s'hagin establert altres procediments de conformitat amb l'article 26 (per exemple, "Contractes tipus per a la transferència de dades personals a tercers països", "Principis de port segur" – on les dades s'estan transferint als Estats Units – o "Normatives corporatives vinculants").

   Cal dir que, tot i les possibles dificultats formals, que representen un cert risc, el marc legal actual espanyol permet sense problemes l'exportació de dades dintre i fora de la Unió Europea. En aquest segon cas, com ja hem avançat, en els següents casos (SANCHO VILLA, 2010; ÁLVAREZ RIGAUDIAS, 2012: pp. 118 i ss.):

   - Sense necessitat d'autorització (article 66.2 RD 1720/2007), si:
   -
     - L'Estat en el qual es troba l'importador ofereix un nivell de protecció adequat.
       - Per declaració del director de l'Agència Española de Protecció de Dades (article 67 RD 1720/2007).
       - Per decisió de la Comissió Europea (article 68 RD 1720/2007), el que actualment cobreix, a més de diversos Estats, el sistema de Port Segur dels Estats Units (Safe Harbor), per decisió 2000/520/CE.
     - La transferència es troba emparada en els supòsits dels apartats a) a j) de l'article 34 de la LOPD. Resulta, en particular, interessant el supòsit del consentiment exprés de l'afectat, que es pot obtenir en el moment de l'alta en el servei.
     -
   - Amb autorització prèvia del director de l'Agència Espanyola de Protecció de Dades, que l'Estat en el qual es troba l'importador no ha estat declarat com un que ofereix un nivell de protecció adequat (article 66.1 RD 1720/2007).
   -
     - L'autorització es pot concedir si el responsable aporta un contracte escrit en què constin les necessàries garanties de respecte a la protecció de la vida privada dels afectats i als seu drets i llibertats fonamentals, i es garanteixi l'exercici dels seus respectius drets (article 70.2, primer paràgraf, RD 1720/2007).

- L'autorització s'ha de concedir[10] si es fan servir els models contractuals aprovats per les decisions de la Comissió Europea 2001/497/CE o 2004/915/CE (transferència de responsable a responsable) o bé 2010/87/UE (transferència de responsable a encarregat).
- L'autorització també es pot concedir en el cas d'ús de Normes Corporatives Vinculants (article 70.4 RD 1720/2007), en aquest cas amb la particularitat del seu reconeixement mutu per part de las resta d'autoritats de protecció de dades.

No obstant això, l'estudi que estem analitzant indica que hi ha problemes amb cadascun d'aquests modes de legitimar una transferència: el fet de basar-la en el consentiment de l'interessat exposa la transferència a les incerteses de la possible retirada del consentiment. D'altra banda, els principis de port segur, que s'apliquen a les dades transferides als Estats Units, poden quedar curts en un entorn de núvol, on els fluxos de dades poden referir-se a països no pertanyents al EEE diferents dels Estats Units. Finalment, les Normatives corporatives vinculants (NCV) encara no han estat plenament recolzades pels proveïdors de serveis en el núvol principals, a causa principalment a deficiències en el procés d'aplicació i aprovació de les aquestes.

Igualment, cal tenir present que els proveïdors en el núvol han generalitzat l'aplicació de contractes tipus o d'adhesió per donar suport a les transferències de dades repetitives o múltiples, raó per la qual però pot ser complicat formalment adaptar o singularitzar aquests contractes, especialment allà on les normatives nacionals imposen requisits administratius addicionals (com ara el deure de obtenir l'aprovació reglamentària del contracte).

En vista d'aquests reptes, en el marc de l'anàlisi o examen de la protecció de dades en l'àmbit de la UE, la Comissió Europea té com a objectiu millorar els mecanismes de transferència de dades a països que no pertanyen al EEE. La Comissió també està encoratjant les iniciatives d'autoregulació, com els codis de conducta o els codis de pràctica. No obstant, en el cas de serveis en el núvol proporcionats als governs i administracions públiques, tots els arguments sobre la sobirania governamental presentats anteriorment seran un factor a considerar en relació amb les transferències de dades.

7. Dret de l'interessat d'accés a les dades (article 12 Directiva 95/46/CE). El responsable del tractament té l'obligació de garantir a l'interessat els drets que estableix l'article 12, per exemple, a obtenir la confirmació de si s'estan processant o no dades relatives a l'interessat, a obtenir informació sobre els propòsits del tractament, les categories de les dades en qüestió, el receptor o les categories dels destinataris als que es comunicaran les dades, a corregir, esborrar o bloquejar les dades processades d'una manera que no sigui compatible amb les disposicions de la Directiva, etc.

[10] Sense perjudici de les potestats de denegació o suspensió previstes a l'article 70.3 del mateix RD 1720/2007, quan es donin els supòsits allà indicats.

> És molt important, especialment quan el proveïdor de serveis en el núvol s'engloba en la definició d'encarregat del tractament, que el proveïdor de serveis en el núvol estableixi una cooperació molt estreta amb els seus clients (és a dir, governs i administracions públiques) per assegurar que aquests últims, en qualitat de responsables del tractament, estiguin en condicions de complir les seves obligacions respecte a la protecció de dades davant dels interessats. És convenient precisar els termes d'aquesta cooperació entre les parts en el contracte corresponent. Sorgeixen qüestions específiques sobre això en el context de la sanitat electrònica, en el que és un fet no només que la Directiva 95/46/CE s'ha posat en marxa d'una manera inconsistent, sinó també que els drets dels pacients estan definits i s'implementen de maneres diferents segons les diferents lleis nacionals que s'apliquin.
>
> Per una altra banda, com a posat de manifest GILBERT, 2012: p. 29, la nova regulació proposada en matèria de protecció de dades aposta per la instauració d'un dret a la portabilitat de les dades (article 18), que inclouria la possibilitat d'obtenir les dades en un format electrònic estructurat i d'ampli ús, sense concretar més detalls tècnics pel tal de no incórrer en infracció del principi de neutralitat tecnològica.

Igualment, podem fer esment del dictamen emés per l'Autoritat Catalana de protecció de dades, en relació amb la consulta formulada per un consell comarcal sobre la contractació del servei *Google Apps for Business,* núm. 24/2012, que tracta la qüestió des de la vessant de protecció de dades de caràcter personal, i fa esment de les mesures de seguretat a adoptar, pel que fa a la figura d'encarregat del tractament, i els diferents nivells de seguretat de les dades que siguin objecte de tractament.

## 2.3 Riscos de confidencialitat i propietat intel·lectual al *Cloud*

La sensibilitat i la propietat de les dades és un element que cal considerar com a possible font de risc en l'adopció del *Cloud*.

L'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011 es refereix de forma específica a la sobirania governamental i al control sobre la informació i les dades (CATTEDDU, 2011: p. 40). En aquest sentit, s'argumenta que per als governs i les Administracions públiques, en general, un dels principals problemes jurídics és la sobirania i el control sobre les dades que gestionen.

Un organisme governamental que té dret a utilitzar dades és responsable de la seva manipulació i s'ha d'assegurar que les seves obligacions de protegir les dades s'estenen contractualment als seus proveïdors externs. Quan la infraestructura d'allotjament *Cloud* s'estén més enllà de la jurisdicció local, l'entitat pública n'ha de considerar les implicacions i les garanties relacionades oferts pel seu proveïdor.

Si les dades governamentals s'estan gestionant a l'estranger per particulars sotmesos a una jurisdicció estrangera, existeix el risc que els tribunals estrangers puguin expedir manaments a l'entitat privada i per tant, arribar a dades del govern. A més, això pot implicar possibles infraccions de les lleis de propietat intel·lectual i de confidencialitat relatives a la informació, les dades, el "saber fer", els drets d'autor o de patent de materials migrats al *Cloud*. En opinió d'INTECO, 2012: p. 54, les qüestions relatives a la propietat intel·lectual dels desenvolupaments, creacions, o altres prestacions que puguin tenir associats drets intangibles a què tingui accés o es desenvolupin per part del proveïdor han de quedar regulades de forma expressa en el contracte.

Aquests problemes s'apliquen per igual a totes les formes de subcontractació, inclosos els actuals acords de subcontractació així com a la prestació de serveis Cloud públic, privat i comunitari. Un organisme governamental, per tant, s'ha assegurar d'imposar mesures de seguretat adequades als seus proveïdors d'externalització, i que existeixen els procediments i mecanismes perquè només les dades rellevants siguin lliurades en resposta a les demandes legítimes de les autoritats judicials. Això inclou la comprovació de si l'evidència ha estat legítimament sol·licitada (per ordre judicial o durant la investigació).

L'estudi publicat pel Parlament Europeu sobre el *Cloud* es refereix als riscos associats a la manca de transparència dels proveïdors en relació amb la seguretat de les dades (FIELDER *et al*., 2012: pp. 50-51), en els següents termes: els usuaris dels serveis de *Cloud computing*, ja siguin empreses o consumidors individuals, tenen el dret a esperar un emmagatzematge segur de les seves dades, així com la integritat de les dades. Sembla, però, que molts proveïdors de serveis no només eviten oferir garanties per a la integritat de les dades, sinó que en realitat rebutgen qualsevol responsabilitat en aquest àmbit, com demostra un estudi de 2010 sobre comparació i anàlisi de contractes de prestació; així, un nombre d'aquests proveïdors especifiquen que la responsabilitat per la preservació i integritat de les dades resideix en el client, mentre que d'altres garanteixen la integritat només en cas de pagament addicional.

Els representants dels consumidors estan d'acord en que hi hagi nivells diferenciats en les proteccions de seguretat, també en termes de costos, d'acord a les necessitats, però sostenen que això no ha d'implicar que les consideracions de seguretat bàsiques, com la integritat de les dades, es puguin comprometre.

A més, el control pel client de les dades en el *Cloud* pot disminuir depenent del model de servei (per exemple, una xarxa social, una eina de col·laboració o un servei de còpia de rescabalament) i diferents proveïdors tenen diferents estàndards de seguretat per al mateix nivells de servei que s'ofereix, fins i tot quan aquest servei és gratuït. Sovint, és difícil de trobar una informació clara sobre mesures de seguretat i protecció de dades, o no està disponibles o són de difícil accés en els llocs dels proveïdors de serveis.

Aquest estudi ha analitzat quinze serveis de *Cloud* públic per consumidors i empreses, anàlisi de la que es desprèn l'existència de diferències significatives en el grau de claredat i detall de la informació subministrada pels prestadors. En diversos casos, no va ser possible trobar informació

mínima sobre aspectes com la seguretat física dels servidors de procés de dades, la ubicació de les dades o els procediments de notificació en cas de divulgacions no autoritzades de dades.

Per la seva part, l'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 50, recorda que quan una Administració pública contracti amb un proveïdor de serveis de *Cloud computing*, haurà de garantir, d'una banda, que els ciutadans poden exercir el dret d'accés a la informació continguda en arxius públics en els termes que estableix la Llei 30/1992, i per altra, que la informació reservada o restringida es protegeix amb la implantació de les mesures de seguretat i de restricció adequades.

## 2.4 Risc de compliment (*compliance*)

El moviment de processos d'execució mitjançant infraestructura pròpia, en sentit ampli, al *Cloud* pot suposar un risc de manca de compliment amb les regulacions, segons exposem a continuació.

L'estudi sobre *Cloud computing* publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2009 es refereix també al que denomina risc de compliment. La inversió en l'obtenció de la certificació (per exemple, requisits reglamentaris o normatius del sector) es pot veure amenaçada per la migració al *Cloud*, si el proveïdor en *Cloud* no pot demostrar el seu compliment dels requisits pertinents, o si el proveïdor en núvol no permet que el client en núvol realitzi l'auditoria (CATTEDDU i HOGBEN, 2009a: p. 10).

En determinats casos, també significa que l'ús d'una infraestructura de *Cloud* públic implica que no poden assolir determinats nivells de compliment (per exemple, amb PCI DSS) i que, per tant, el seu ús simplement no resulta possible.

L'estudi avalua aquest risc com alt, ja que considera que la seva probabilitat d'ocurrència és molt alta i que el seu impacte sobre l'organització seria molt alt, afectant principalment a la certificació, que és un actiu de valor alt. A més, l'estudi considera que hi ha més risc en el cas de fer servir Cloud que en cas de fer servir una infraestructura TI tradicional, tot i que l'impacte seria el mateix en tots dos casos (CATTEDDU i HOGBEN, 2009a: p. 32).

Les vulnerabilitats identificades són les següents:

1. Auditoria o certificació no disponible per als clients[11].
2. Manca de tecnologies i solucions estàndard[12].

[11] El proveïdor de Cloud no pot oferir cap garantia al client a través d'auditoria de certificació. Per exemple, hi ha proveïdors que utilitzen hipervisors de programari lliure o versions modificades d'hipervisors que no disposen de certificació de seguretat d'acord amb Criteris Comuns, certificació que es requerida per algunes organitzacions (CATTEDDU i HOGBEN, 2009a: p. 64).

[12] La manca d'estàndards significa que les dades poden quedar vinculades de forma exclusiva a un proveïdor ("vendorlock-in"), el que suposa un gran risc en cas de cessament d'operacions pel proveïdor (CATTEDDU i HOGBEN, 2009a: p. 61).

3. Emmagatzematge de dades a jurisdiccions múltiples i manca de transparència sobre aquest punt[13].
4. Sistemes de certificació no adaptats a les infraestructures *Cloud*[14].
5. Manca d'informacions sobre jurisdiccions[15].
6. Manca d'integritat i de transparència en els termes d'ús.

BOWEN, 2011, pp: 2 i ss. detalla diverses regulacions el compliment de les quals es pot veure afectat, incloent-hi l'acta Gramm-Leach-Bliley, que imposa obligacions a les institucions financeres en relació amb la privacitat de les dades dels seus clients; l'acta de la Federal Trade Comission, que obliga a protegir les dades dels clients, especialment en relació amb el robatori d'identitat; o l'acta HITECH i l'acta HIPAA, que exigeixen la notificació de pèrdues de dades no xifrades, entre d'altres.

En sentit similar, NG i CARRUTHERS, 2012, identifiquen l'adopció del *Cloud*, sense controls estrictes de compliment, com un risc d'infracció de la regulació aplicable a les institucions financeres del Canadà, continguda a la Guia B-10 de la OSFI.

> Pel que fa a Espanya, també es poden trobar obligacions de manteniment de dades en territori espanyol (o de la Unión Europea). Per exemple, la normativa de facturació electrònica no permet l'emmagatzematge de factures extraterritorialment sense autorització prèvia, el que podria afectar al compliment de les obligacions d'un subjecte obligat que fa ús d'un servei en modalitat SaaS radicat fora del país.

## *2.5* Risc de captivitat del client *(vendor lock-in)*

La possible dependència d'un proveïdor, per exemple per manca d'estandardització o d'interoperabilitat, suposa un risc de captivitat important per als usuaris, que analitzem tot seguit.

L'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011, indica que una solució de *Cloud* ha de ser interoperable, permetent als governs i les administracions públiques migrar als serveis en el núvol d'un proveïdor de serveis en el núvol a un altre sense restriccions tècniques o contractuals o costos de canvi substancials. A més, la interoperabilitat és una condició necessària en el context

[13] La replicació de dades per a la seva distribució per part de xarxes i emmagatzematge redundant sense informació en temps real del lloc d'ubicació de les dades accessible al client introdueix un nivell de vulnerabilitat. Les companyies poden infringir involuntàriament regulacions, especialment si el proveïdor no li ofereix informació clara sobre la jurisdicció d'emmagatzematge (CATTEDDU i HOGBEN, 2009a: p. 65).

[14] No existeix cap control específic de *Cloud*, el que vol dir que les vulnerabilitats probablement passaran desapercebudes (CATTEDDU i HOGBEN, 2009a: p. 64).

[15] Les dades poden emmagatzemar-se o processar-se a jurisdiccions d'alt risc, on són vulnerables a la confiscació per mitjà d'una entrada forçada. Si aquesta informació no es troba disponible per als clients al *Cloud*, no poden prendre mesures per evitar-ho (CATTEDDU i HOGBEN, 2009a: p. 65).

de la sanitat electrònica. D'altra banda, en els contractes s'ha de definir el calendari i les modalitats de les transferències a l'origen d'informació i dades.

És molt important que els governs i les administracions públiques evitin qualsevol forma de "captivitat del mercat", ja que qualsevol falta de disponibilitat (temporal) o ineficiència dels serveis pot donar lloc a importants responsabilitats per als governs i les administracions públiques (CATTEDDU, 2011: p. 45).

Per a l'INTECO, 2012: p. 55, la contractació d'un servei de *Cloud computing* sense estudiar futures interoperabilitats amb altres proveïdors podria provocar grans inconvenients a l'Administració a l'hora d'allotjar o migrar directament el servei a un altre proveïdor amb millors característiques i, per això, aquestes qüestions han de tenir reflex adequat en el contracte, i fins i tot preveure l'aplicació de penalitzacions al proveïdor en cas d'incompliment de les seves obligacions en matèria d'interoperabilitat.

Tal com ja s'ha esmentat anteriorment, això formaria part del que seria la planificació prèvia a l'hora de dotar-se de serveis *Cloud*, la qual no hauria de limitar-se a donar resposta a una necessitat puntual, sinó que hauria de ser capaç de preveure les necessitats futures i, igualment, qualsevol transició o adaptació que no es veiés afectada per problemes d'interoperabilitat que, arribat el cas, suposarien necessàriament o ineficiències econòmiques, o l'abans esmentada situació del client captiu.

## 2.6 Risc de negligència professional

La negligència professional en la prestació del servei suposa un risc legal que, com veurem en aquesta secció, pot impactar en els usuaris.

L'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011, indica que en migrar als serveis en el núvol, els governs i les administracions públiques passen a dependre molt de l'adequació de l'acompliment del proveïdor de serveis, no tan sols de les seves condicions de servei o tècniques, sinó també dels requeriments materials de prestació que inicialment estiguin previstos.

En aquest sentit, a diferència del que passa en l'àmbit privat, en què les deficiències o negligències tenen una incidència que s'ha de resoldre en l'àmbit del dret privat i del principi d'igualtat de les parts, no passa el mateix en l'àmbit del dret públic. En aquest àmbit, els errors o deficiències del proveïdor de serveis en el núvol en la prestació dels serveis poden tenir un impacte molt negatiu sobre els serveis que ofereixen els governs i les administracions públiques als ciutadans. Això es pot traduir no només en pèrdues econòmiques per als governs i les administracions públiques, sinó també en danys a la seva imatge (per tant, mal polític). Aquestes pèrdua econòmica per part de l'administració pública pot produir-se de manera directa i immediata, o per la via de rescabalament econòmic de particulars que hagin patit danys i perjudicis com a conseqüència del que, en última instància, és una actuació administrativa, i exerceixin les seves reclamacions de responsabilitat d'acord amb el que prescriu l'ordenament jurídic (reclamacions que perfectament es poden estendre als danys morals o a la imatge que es puguin haver sofert).

Les clàusules de responsabilitat i indemnització en els acords de nivell de servei (ANS) han d'exercir un paper fonamental en aquest àmbit. Els ANS detallats, en què s'especifiquen de manera complerta els nivells de funcionament del proveïdor de serveis en el núvol, juntament amb les clàusules contractuals que assignen clarament, d'una banda, els drets i deures generals de les parts i, de l'altra, les obligacions i responsabilitats, seran elements bàsics a l'hora d'avaluar els conflictes que es puguin plantejar, així com han de ser presos en consideració per part dels governs i administracions públiques, a l'hora d'adoptar les seves decisions.

Aquests haurien de demanar als proveïdors de serveis en el núvol l'adopció de les mesures oportunes per evitar o detectar errors, així com l'establiment de mecanismes de ràpida resposta davant les incidències que es puguin plantejar. Aquests extrems s'haurien d'assegurar mitjançant l'establiment de clàusules contractuals que prevegin sancions o penalitzacions que puguin arribar a ser considerables en funció del grau de deficiència en els serveis prestats per part del proveïdor de serveis en el núvol (CATTEDDU, 2011: pp. 44-45).

En concret, resulta particularment important evitar la indisponibilitat del servei. D'acord amb l'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: p. 55, és fonamental que tant l'Administració com, si és el cas, els seus administrats, puguin accedir al servei quan ho requereixin. En cas contrari, es podria veure alterada no tan sols la imatge sinó també la productivitat de l'Administració, al no poder-se prestar el servei habitual. Per això, cal definir adequadament els temps d'inactivitat permissibles i les pèrdues d'informació acceptables, mitjançant un Acord de Nivell de Servei (ANS) amb el proveïdor, que contempli percentatges coherents de disponibilitat i mesures compensatòries adequades en cas d'incompliment.

Així mateix, també considera INTECO que el manteniment i gestió de la seguretat és responsabilitat del proveïdor. En cas que hi hagi un accés no autoritzat al centre de processament de dades o es produeixi l'atac d'un *hacker*, la qualitat del servei es pot veure afectada. En aquests casos, el proveïdor haurà de gestionar aquests successos amb celeritat i informar d'ells amb immediatesa a l'Administració perquè aquesta pugui adoptar les mesures que, si s'escau estimi necessàries.

No obstant això, cal tenir present que, per molt ben definida que estigui l'estructura de resposta davant de les incidències, errors o negligències del prestador del servei, les administracions públiques tenen assumida una responsabilitat de caràcter objectiu, davant dels perjudicis que puguin patir els ciutadans quan es relacionen amb aquelles. Per aquesta raó, per molt ben desenvolupats o regulats que estiguin aquests extrems, la responsabilitat primera davant del ciutadà serà sempre la de la corresponent administració pública, la qual no pot al·legar qüestions de caire organitzatiu o intern per exonerar-se de les responsabilitats del que, en última instància, ha estat una actuació administrativa.

En aquest sentit, s'haurà de diferenciar el que són prestacions de serveis *Cloud* que incideixen de manera directa en el ciutadà, en relació amb les quals qualsevol responsabilitat haurà de ser assumida per l'administració pública, sense perjudici de la possible repetició contra el responsable del dany (en aquest àmbit, les repeticions de responsabilitat plantegen igualment problemes); del que són prestacions de caràcter merament intern i que no tinguin un efecte directe de responsabilitat envers tercers (més enllà d'una deficient prestació del servei que no arribi a generar responsabilitat), en aquest segon cas s'haurà d'estar al compliment de les prevencions en que aquest servei *Cloud* hagi estat contractat.

La doctrina recomana, addicionalment, analitzar les necessitats d'assegurança de la responsabilitat per la prestació de serveis de Cloud, de forma alineada amb una anàlisi detallada dels riscos i traslladar aquestes necessitats en forma d'exigències recollides contractualment (GOLD, 2012: pp. 26 i ss.)

## 2.7 Riscos relatius a la subcontractació i canvis de control

La subcontractació de serveis i els canvis de control sobre els prestadors de serveis de *Cloud computing* poden també ser esdevenir un risc legal.

BALBONI, 2010: p. 5, exposa que, degut a la elevada dependència que tenen els clients dels serveis de *Cloud computing*, resulta previsible que seleccionin amb cura els prestadors, basant-se en aspectes com la seva reputació, professionalitat, condicions ofertes o competències tècniques, motiu pel qual poden ser reticents a la subcontractació de serveis rellevants a un tercer que poder no ofereix les mateixes garanties. A més, els canvis de control sobre els prestadors poden també afectar a les garanties o als termes contractuals.

A més, les subcontractacions poden resultar invisibles per als usuaris, de forma que si, durant la prestació dels serveis hi ha una parada deguda al subcontractista, podria resultar molt difícil per a un usuari determinar la identitat, localització i dades accedides pel mateix (BOWEN, 2011: p. 5).

Especialment important resulta determinar aspectes com la viabilitat del prestador de serveis de *Cloud computing*, i protegir l'accés pel usuaris a les seves dades (personals, de negoci o de qualsevol altre tipus), en els escenaris de fallida econòmica, adquisició o fusió del proveïdor (canvi de control) o abandonament de l'activitat (BOWEN, 2011: pp. 6-7).

L'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011, explica que donada la relació altament dependent, és recomanable (i probable) que els governs i les administracions públiques seleccionin acuradament els proveïdors de serveis en el *Cloud*.

L'autor considera que s'han d'evitar les situacions en què un proveïdor de serveis en el núvol subcontracti els serveis pertinents a un tercer o, si més no, s'han d'incloure en el contracte de servei declaracions, garanties o limitacions sobre possibles subcontractistes. De la mateixa manera, el proveïdor de serveis en el núvol ha de notificar sense demora els canvis de control al govern o administracions públiques, que és possible vulgui negociar el dret de rescindir el contracte en cas que passi aquest esdeveniment (CATTEDDU, 2011: p. 45).

## 2.8 Risc de llicenciament

Finalment, avaluarem el risc legal derivat de la transformació del model de llicenciament en el trànsit al *Cloud*.

L'estudi sobre *Cloud computing* publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2009 considera també el que anomena risc de llicenciament, aclarint que les condicions de la llicència, com els acords per lloc, i les comprovacions de les llicències en línia poden no ser factibles en un entorn de *Cloud*. Per exemple, si el cost del programari es factura per instància cada vegada que una màquina nova es instanciada, les despeses de llicència per al client en *Cloud* podrien augmentar exponencialment, tot i estar utilitzant el mateix nombre de màquines durant el mateix període (CATTEDDU i HOGBEN, 2009a: p. 10).

En aquest sentit, CLASSEN i FOGARTY, 2012: pp. 2-3, han identificat de forma molt precisa la problemàtica que suposa l'adequació del model de llicències d'ús al *Cloud computing*, tant des de la perspectiva de l'usuari final com des de la posició del proveïdor de serveis *Cloud*.

En el primer cas, perquè en adquirir un servei enlloc d'una llicència, apareixen riscos nous, alguns dels quals ja hem analitzat anteriorment, com la seguretat de les dades, l'accés a les dades o la privacitat, però també la propietat intel·lectual de les dades carregades pel client (que a més en alguns casos no són seves, sinó que les gestiona o posseeix en virtut d'un títol jurídic concret) i la possibilitat de realitzar transicions de servei d'un proveïdor a un altre, especialment en cas de canvi de control i, en particular, de l'abandonament de l'activitat per part del prestador.

En el segon cas, el problema deriva del fet que habitualment les llicències són per a ús propi, intern o individual, però no permeten ni la seva instal·lació en entorns compartits, o bé operats per tercers, o en escenaris de múltiples o tercers usuaris, la qual cosa impedeix al proveïdor de serveis *Cloud* fer ús d'aquell programari per a la prestació del seus serveis.

D'altra banda, el mateix estudi d'ENISA considera que en els models de servei d'infraestructura com a servei (IaaS) i de plataforma com a servei (PaaS), existeix la possibilitat de produir creacions originals en el *Cloud* (noves aplicacions, programari, etc.). En aquests casos, tal com passa en altres supòsits protegits per la propietat intel·lectual, si la producció d'aquesta creació original no es troba prevista o protegida per les clàusules contractuals apropiades, aquest treball original es pot veure amenaçat per una possible apropiació per part del prestador.

L'estudi avalua aquest risc com mitjà, ja que considera que la seva probabilitat d'ocurrència és mitja i que el seu impacte sobre l'organització seria mig, afectant principalment al renom de l'organització, la confiança del client, la prestació del servei i a la certificació, que són actius de

valor alt o molt alt (CATTEDDU i HOGBEN, 2009a: pp. 50-51). La principal vulnerabilitat identificada és, en aquest cas, la manca d'integritat i de transparència en els termes d'ús.

Finalment, i des d'una altra perspectiva GERVAIS i HYNDMANN, 2012: pp. 67 i ss. han avaluat els reptes legals que deriven, per a la protecció de la propietat intel·lectual dels continguts, la prestació de serveis de *Cloud*, en especial en l'àmbit de la indústria de l'entreteniment i, en concret, de la música en línia. Els autors es plantegen les limitacions de la normativa actual, orientada a la venda d'unitats escasses, i posen de manifest com aquesta assumpció legal resulta falsa en els models de negoci de *Cloud*, el que permetria abusos en la legítima lluita contra la pirateria, perseguint els "pirates" no professionals amb reclamacions de fins a 150.000 $ per cançó il·lícitament obtinguda, a partir de les dades obtingudes de serveis *Cloud* com iTunes, escenari que avui no és encara real, però que ho podria ser ben aviat.

La propietat intel·lectual té un fortíssim component d'aplicació territorial, per la qual cosa posar aquestes situacions en un context extraterritorial pot suposar problemes de seguretat jurídica importants per als usuaris.

D'acord amb l'exposat, són diversos els riscos que se'n deriven de la utilització del Cloud Computing, el que no ha d'impedir la seva implementació, atenent als clars beneficis que se'n deriven, i que igualment han estat objecte d'anàlisi en el projecte de recerca. No obstant això, s'han d'adoptar una sèrie de mesures per mirar de reduir al màxim els riscos esmentats, el que ens ha portat a realitzar una sèrie de recomanacions jurídiques en relació amb l'ús del Cloud computing per part de l'Administració.

# 3 Recomanacions jurídiques en relació amb l'ús del *Cloud computing* per part de l'Administració

L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: pp. 41-42, indica que existeixen factors que condicionen el context nacional en relació amb el desenvolupament d'aquest paradigma computacional:

- Des del punt de vista del desenvolupament del sector a Espanya, cal considerar que ha estat tradicionalment un mercat molt atractiu per a la implantació de centres de desenvolupament i servei de TI. La qualificació dels professionals espanyols i els costos laborals, el posicionament estratègic d'Espanya respecte dels mercats africà i sud-americà, així com l'esforç de les institucions espanyoles pel foment del sector, han fet de l'Estat espanyol un emplaçament molt valorat per a l'establiment de centres de processament de dades.

- Espanya compta amb un escenari jurídic efectiu per a la protecció de dades personals i garantia de seguretat per al desplegament de les tecnologies *Cloud*. El marc de la LOPD empara el desenvolupament del mercat en unes condicions de garantia correctes, quedant aspectes per concretar únicament en l'àmbit de la transferència internacional de dades.

- Les administracions públiques espanyoles estan sent pioneres en la valoració i impuls del model *Cloud*. La conjuntura d'estalvi i optimització de costos en la qual es troben actualment ha propiciat que el *Cloud* es posicioni com un conductor d'eficiències i estalvis. L'efecte prescriptor de les administracions tindrà un efecte tractor sobre el sector, que aprofitarà el seu impuls per al desenvolupament de solucions i serveis *Cloud* en models de col·laboració publico-privada.

- El sector TIC nacional aposta de forma decidida pel desenvolupament del *Cloud computing*. Els principals proveïdors del sector es troben en un profund procés de transformació de negoci, orientant el seu catàleg (allotjament, llicències, productes, serveis, etc.) a models *Cloud* que s'ofereixen de manera més rendible al mercat.

- A més del sector TIC, les operadores de telecomunicacions utilitzen el seu posicionament comercial, la seva experiència de servei i, sobretot, la seva xarxa d'infraestructures de telecomunicacions per posicionar-se en aquest sector. Importants empreses estan assumint inversions significatives per operar en el mercat del *Cloud* computing i, segons experts consultats, és segur que en els propers anys l'oferta tradicional de serveis de telefonia, xarxa o ADSL s'acompanyi de serveis d'infraestructura o aplicacions en modes IaaS o SaaS, tant per a empreses com per a usuaris particulars.

- El *Cloud computing* a Espanya (i en altres economies) no suposa una transició molt agressiva cap a un nou paradigma tecnològic. Durant l'última dècada s'ha consolidat a Espanya el concepte de virtualització de serveis i infraestructures i els models d'externalització tecnològica a través del hosting i l'outsourcing, tant en el sector públic com en el privat, i tant en entitats grans com petites. Aquesta situació determina que el mercat espanyol parteixi d'una situació de certa maduresa i bases prèvies que garanteixen una gestió de canvi i assumpció dels models *Cloud* més naturals.

El mateix estudi palesa que en el context de les administracions públiques espanyoles, la situació de disponibilitat pressupostària i els requeriments d'ajustos de la despesa i dèficit han portat els gestors públics a valorar el *Cloud computing* com a potencial instrument d'estalvi de costos i optimització tecnològica. En aquest sentit, fonts consultades de l'Administració General de l'Estat han informat que s'han emprès anàlisis i estudis en l'àmbit ministerial per promoure una infraestructura de serveis compartits, desplegada a través de tecnologia *Cloud* privada, que permeti integrar i concentrar serveis comuns a totes les administracions en infraestructures i centres de servei compartits.

Aquest plantejament, que encara es troba en fase d'anàlisi estratègica, parteix de la base que el principal estalvi i optimització prové de l'estandardització i concentració de serveis compartits comuns per a diversos organismes públics (considerant fins i tot integrar administracions autonòmiques i locals en el projecte ), i que el *Cloud computing* ha de ser l'instrument tecnològic sobre el qual implementar aquest model (INTECO, 2012: pp. 42-43).

Quines recomanacions poden contribuir a una millor adopció del *Cloud computing*?

## 3.1 Recomanacions de caràcter general

Amb caràcter general, a l'estudi sobre *Cloud computing* publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2009, es realitza una recomanació jurídica de caràcter general referida a la diligència en la contractació del proveïdor (CATTEDDU i HOGBEN, 2009a: p. 7). Així, es diu que la majoria de qüestions legals associades a la computació en núvol se sol resoldre durant l'avaluació (és a dir, en comparar els diferents proveïdors) o la negociació del contracte. El cas més comú de computació en núvol és la selecció dels diferents contractes que ofereix el mercat (avaluació de contractes), en contrast amb la negociació del contracte. Tanmateix, podria haver oportunitats perquè clients potencials de serveis en núvol seleccionin proveïdors amb contractes negociables.

A diferència dels serveis tradicionals d'Internet, es recomana revisar detingudament les clàusules estàndard del contracte, a causa de la naturalesa de la computació en núvol. Les parts del contracte han de prestar especial atenció als seus drets i obligacions pel que fa a les notificacions

d'incompliment dels requisits de seguretat, transferències de dades, creació d'obres derivades, canvi de control i accés a les dades per part de les forces policials. Com que el núvol pot utilitzar-se per subcontractar infraestructura interna crítica, i a que la interrupció d'aquesta infraestructura pot tenir conseqüències de gran abast, les parts han de avaluar detingudament si les limitacions estàndard de responsabilitat s'ajusten a les assignacions de responsabilitat, tenint en compte el ús del núvol per les diferents parts, o les responsabilitats pel que fa a la infraestructura.

En aquest sentit, en defecte de previsions legals o reglamentàries que regulin les prevencions concretes en matèria de seguretat relatives a la computació en núvol, s'haurà d'estar als pactes concrets que els clients i els proveïdors en núvol estableixin, els qual han d'assegurar que les condicions del seu contracte aborden de manera efectiva els riscos de seguretat.

En concret, l'estudi ofereix una llista d'àmbits als quals el client de *Cloud* ha de prestar una atenció especial a l'hora d'avaluar els acords de nivell de servei, els termes d'ús, els acords de llicència d'usuari i altres acords relatius als serveis en *Cloud* (CATTEDDU i HOGBEN, 2009a: pp. 94-95):

1. Protecció de les dades. Cal seleccionar un proveïdor que proporcioni mesures tècniques de seguretat adequades i mesures organitzatives que controlin el processament que tindrà lloc i, garantir el compliment d'aquestes mesures.

2. Seguretat de les dades. Cal prestar atenció a les mesures obligatòries relatives a la seguretat de les dades que poden provocar que o bé el proveïdor en *Cloud* o bé el client es vegin sotmesos a mesures reguladores i judicials si el contracte no aborda aquestes obligacions.

3. Transferència de dades. Cal prestar atenció a la informació que es facilita al client pel que fa a la manera de transferir les dades en el *Cloud* propietat del proveïdor, fora d'aquest *Cloud* i dins i fora de l'Espai Econòmic Europeu.

4. Accés de les autoritats policials. Cada Estat té restriccions peculiars i requisits necessaris per a l'accés de les autoritats policials a les dades. El client ha de considerar la informació que el proveïdor posa a la seva disposició sobre les jurisdiccions en què les dades poden emmagatzemar processar, i avaluar qualsevol risc derivat de les jurisdiccions aplicables.

5. Confidencialitat i no divulgació. S'han de revisar les funcions i obligacions associades a aquesta qüestió.

6. Propietat intel·lectual. en el cas de l'IaaS i del PaaS, es pot emmagatzemar la propietat intel·lectual, incloses les obres originals creades utilitzant la infraestructura de *Cloud*. El client s'ha d'assegurar que el contracte respecta els seus drets sobre qualsevol propietat intel·lectual o treball original en la mesura del possible, sense comprometre la qualitat del

servei ofert (per exemple, les còpies de seguretat podrien ser un element necessari a incloure en una oferta de nivell de servei satisfactori).

7. Assignació de riscos i limitació de la responsabilitat. A l'hora de revisar les seves respectives obligacions contractuals, les parts han de subratllar les obligacions que plantegen riscos considerables per a aquestes, incloent clàusules de compensació econòmica o obligacions d'indemnització per la part que incompleixi una obligació contractual. Així mateix, s'ha d'avaluar detingudament qualsevol clàusula estàndard que impliqui limitacions de responsabilitat.

8. Canvi de control. Resulta necessari garantir la transparència en relació a la capacitat contínua del proveïdor en *Cloud* de complir les seves obligacions contractuals en cas de produir-se un canvi de control, així com preveure la possibilitat de rescindir el contracte.

## 3.2 Recomanacions específiques en cas d'ús per part de l'Administració

L'estudi sobre seguretat i resiliència en *Cloud* governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011, realitza les següents recomanacions (CATTEDDU, 2011: pp. 86 a 89):

1. Es recomana a les administracions públiques adoptar un enfocament esglaonat, amb la capacitat de fer marxa enrere en cada etapa o revisar les premisses prèviament establertes o assumides, ja que la complexitat de l'entorn de *Cloud* introdueix variables desconegudes que podrien ser molt difícils de gestionar, o pot introduir variables en el futur que requereixin l'adaptació als canvis. Els gestors públics de qualsevol nivell han de considerar la interconnexió i les interdependències del sistema (la majoria de les quals poden ser desconegudes), especialment en traslladar simultàniament diversos serveis a un sistema de núvol. Els gestors públics hauran de tenir en compte aquesta qüestió en el context actual, en què l'entorn canvia de manera dinàmica, i els nostres coneixements sobre la vulnerabilitat i els mecanismes d'atac, així com la complexitat dels controls relacionats, són incomplets. Els gestors públics no han de donar per fet que la implementació amb èxit d'una aplicació en un entorn del núvol suposa, de forma automàtica, un indici positiu que aconselli fer moltes altres implementacions, sinó que hauran d'examinar de forma detinguda i individual dels requisits de seguretat i resistència de cada aplicació i comparar-se amb les arquitectures del núvol i els controls de seguretat ja disponibles.

2. Les administracions públiques nacionals han d'elaborar una estratègia sobre computació en el núvol que tingui en compte les implicacions pel que fa a la seguretat i la resistència que tindran aquests models de subministrament de serveis en el context de les seves economies nacionals i serveis per als ciutadans en els pròxims 10 anys. Els qui els adoptin en primer lloc en cada Estat membre podran percebre com possibles bancs de proves, tot i

que serà essencial comptar, almenys en l'àmbit nacional, amb un plantejament coherent i harmonitzat respecte a la computació en el núvol per tal d'evitar: 1 ) la proliferació de plataformes i formats de dades incompatibles (absència d'interoperabilitat de serveis), 2) un plantejament incoherent respecte a la seguretat i la resistència, inclòs un plantejament incoherent i ineficaç respecte a la gestió de riscos i 3) l'absència de massa crítica.

3. L'estudi també recomana a les administracions públiques que estudiïn el paper que exercirà la computació en el *Cloud* en el context de la protecció de les infraestructures de la informació crítica. No és desgavellat pensar que la computació en el núvol, en totes les seves possibles implementacions, prestarà servei, en un futur proper, a una part significativa de ciutadans, petites i mitjanes empreses i administracions públiques de la Unió Europea i, per tant, les infraestructures en el núvol des de les quals es presten aquests serveis han de disposar de protecció.

   En altres paraules, les estratègies nacionals de computació en el núvol hauran de dirigir a comprendre i abordar, entre altres qüestions, els efectes de la interoperabilitat i interdependències dels núvols nacionals i supranacionals, així com a avaluar l'impacte de possibles fallades en cascada, valorar l'oportunitat d'introduir un pla d'informes d'incidències per proveïdors del núvol similar al que ja es va adoptar en el sector de telecomunicacions (en concret, ens referim al mecanisme de generació d'informes que introdueixen els articles 4 i 13 de la recentment adoptada Directiva 2009/140/CE) i preparar-se per possibles gestions de crisi en cas de produir incidents a gran escala d'aquest tipus.

4. L'estudi també recomana a les administracions públiques nacionals i les institucions de la Unió Europea que continuïn investigant el concepte d'un núvol governamental europea com un espai virtual supranacional on pugui aplicar un conjunt de normes coherent i harmonitzat, tant en termes de legislació com de mesures de seguretat, que les puguin promoure la interoperabilitat i l'estandardització. A més, una infraestructura de la Unió Europea d'aquesta amplitud podria emprar-se en el context d'un pla d'ajuda i assistència mútues pan-europeu per a casos d'emergència.

D'acord amb l'estudi citat, més concretament, si els organismes públics decideixen finalment passar-se a la computació en el núvol, han de:

- Tenint en compte l'estratègia nacional, definir els requisits que han de ser objecte de compliment o salvaguarda (dintre dels quals es troben els que han estat plantejats en aquest informe) per identificar quina solució de núvol s'adapta a les seves necessitats. Els gestors públics han de tenir en compte també els factors humans (com ara la conscienciació sobre la seguretat i la resistència, o la resistència als nous models de mesures de seguretat) i els marcs normatius.

- Per a una bona governança, s'ha d'establir un procés de gestió de seguretat de la informació, que inclogui gestió de riscos, una política per a la resistència i seguretat de la informació, gestió d'actius (físics i d'informació), etc., basant-se en les bones pràctiques disponibles.

- Els gestors públics han de centrar-se en un catàleg de serveis generals i una classificació d'actius físics i d'informació. En aquesta línia, per a cada servei i actiu s'han d'especificar els requisits adequats de resistència i seguretat. Sabem que la majoria de les grans institucions no podran completar aquesta tasca en un temps raonable, ja que som conscients que en certs casos encara no tenen una imatge completa dels seus actius. Una alternativa viable, en el context de l'enfocament esglaonat cap a la computació en el núvol, seria començar amb la definició de categories macro d'actius i serveis (per exemple, no sensibles i no crítics, de sensibilitat i criticitat mitjana, etc.) I elaborar una classificació detallada d'actius segons la lògica senzilla que el primer servei a migrar al núvol ha de ser el primer a classificar (abans de la migració).

- Definir nivells acceptables de servei (una referència, per exemple, disponibilitat) per als seus requisits. Utilitzaran les referències per mesurar el rendiment dels seus serveis.

- Identificar el conjunt de controls i el seu grau d'especificitat per assolir un nivell mínim acceptable de garantia de dades i resistència de serveis.

- Assegurar-se que tots els requisits essencials de seguretat, resistència i jurídics estan detallats en els seus requisits de nivell de serveis i especificats en els seus acords de nivell de servei. Aquests han de redactar en planificar una migració de servei. Per exemple, els acords de nivell de servei han d'incloure el dret d'auditar (o almenys l'accés a un informe d'auditoria independent), els mitjans per recuperar dades i aplicacions (és a dir, evitar el bloqueig) i detallar el nivell de supervisió i elaboració d'informes, etc.

- Establir un marc de mesura (incloent indicadors principals d'objectius i rendiment) per avaluar contínuament si es compleix el següent:

    - Objectiu(s) de nivell de servei.

    - Nivell de preparació i capacitat de prevenció en cas d'incidències com errors i atacs maliciosos.

    - Eficiència i efectivitat de la fase de reacció i recuperació després d'un esdeveniment perjudicial.

- Tenir en compte les normatives rellevants nacionals i internacionals que s'apliquen a tercers (per exemple, directives de signatura digital electrònica, garanties de tercers ISO) per garantir la resistència de les comunicacions entre totes les parts implicades en el subministrament del servei (administracions públiques , ciutadans, proveïdors de serveis, grups comercials, així com els sistemes). S'han de garantir l'autenticitat de les identitats de les parts i la seva autorització per realitzar una acció, el moment en el temps (és a dir, segell de data i hora) i la ubicació.

- Aplicar, en els processos de control d'identitats i accés, els principis de necessitat de saber, mínim privilegi i separació de funcions.

- Tenir eines, metodologies i estructures de governança per, p. ex., garantir la diligència deguda.

- Comprovar l'estabilitat financera i solvència dels socis comercials, incloses les línies rellevants de negocis per evitar interrupcions inesperades dels serveis o el bloqueig.

- Garantir que es mantinguin connexions de telecomunicacions, dependències crítiques (per exemple, electricitat), potència de processament i capacitat d'emmagatzematge de manera satisfactòria.

- Comprovar la prioritat de represa de comunicacions de tercers i serveis de núvol en cas d'interrupcions.

- Provar el pla de continuïtat del negoci al llarg de tota la cadena de subministrament de serveis.

- Per a aplicacions molt crítiques, planificar davant la possible indisponibilitat del servei de *Cloud*. Hi ha d'haver un mecanisme per permetre l'accés a serveis de TI fins i tot quan no es trobi disponible la connexió al/s *Cloud*/s.

Per la seva part, l'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: pp. 120 i ss., realitza, entre d'altres, les següents recomanacions:

- Cada organisme ha de definir el seu propi model de confiança per al *Cloud computing*, que sent les bases de l'estratègia i que estigui estructurat al voltant de quatre objectius:

    - Proporcionar un bon nivell de serveis, protegint alhora la confidencialitat i integració de la informació.

  - Assegurar la capacitat dels sistemes d'acceptar un servei d'acord amb els requisits establerts per l'organització.

  - Definir els criteris per mesurar la capacitat de restauració del sistema en cas d'incidents.

  - Assegurar el compliment de la normativa legal específica.

- Sempre que sigui possible, promoure la interoperabilitat a través d'una infraestructura de serveis compartits, desplegats a través de tecnologia *Cloud* privada, que permetin integrar i concentrar serveis comuns a totes les administracions en infraestructures i centres de servei compartits.

- Valorar les decisions de migració a *Cloud computing* en el marc de les determinacions estratègiques i directives de les administracions públiques. Els gestors públics s'han d'implicar en el procés de decisió per garantir la cohesió de l'organització en la transició cap a aquests models.

- Analitzar i detectar les àrees de servei adequades per a la migració i el conjunt d'usuaris que millor s'aprofitarien de les oportunitats ofertes pel *Cloud computing*.

- Avaluar i promocionar el *Cloud computing* dins dels organismes, com a potencial instrument d'estalvi de costos i optimització tecnològica per combatre la situació d'ajust pressupostari i els requeriments de reducció de la despesa i dèficit.

- A nivell europeu, la Unió Europea ha de competir amb el posicionament dels proveïdors nord-americans a través de la implantació d'una estratègia i mercat europeu del *Cloud*. Així, les administracions públiques europees han de ser agents prescriptors i impulsors del mercat del *Cloud* europeu, tant adoptant aquest model en benefici de la seva millora i optimització interna, com desenvolupant instruments normatius i executius per al desenvolupament del sector.

- Desenvolupar nous models i pràctiques de contractació que s'ajustin al context del *Cloud computing* dins el marc de la Llei de Contractes de Sector Públic.

- Implicar en l'estratègia *Cloud computing* a les àrees jurídiques, tecnològiques i operatives per elaborar instruments contractuals que s'adaptin a les necessitats d'aquesta tecnologia.

- Desenvolupar programes de col·laboració públic-privada i consolidar els estàndards tecnològics comuns i oberts que vertebraran l'expansió d'aquesta tecnologia a totes les administracions i organismes públics.

- En els contractes s'han d'acordar, de manera expressa, les mesures de seguretat aplicades, les condicions d'accés a la informació, les mesures de contingència, les casuístiques de subcontractació del servei i les condicions de finalització del contracte i devolució dels actius i serveis contractats.

- Els proveïdors han de garantir, a través del contracte o d'acords de nivell de servei, el compliment de polítiques de seguretat basades en estàndards auditables i sotmetre a controls i revisions de tercers que certifiquin el compliment d'aquestes polítiques. S'ha de garantir mitjançant auditoria o certificat de destrucció / esborrat que el proveïdor cancel·la i elimina les dades pertanyents a l'Administració pública implicada en la finalització del contracte.

- El contracte ha d'estar sotmès a clàusules de penalització en cas d'incompliment dels acords de nivell de servei establerts. La incorporació de l'obligació del proveïdor de contractar una assegurança de responsabilitat civil és una pràctica recomanable quan la criticitat del servei, o de la informació transferida, ho requereix.

Finalment, resulta necessari referir-se a l'informe sobre *Cloud computing* de la ONTSI, 2012: pp. 208-209, que recomana un procediment de migració de serveis al Cloud que, d'altra banda, ofereix interessants reflexions sobre el procediment contractual. Així, es considera necessari:

1. Realitzar una prospectiva de mercat per analitzar les solucions existents i valorar la capacitat real dels proveïdors per respondre a la demanda en modalitat Cloud.

2. Analitzar la rendibilitat de l'esforç a emprendre, definir els impulsors de benefici esperats, el retorn de la inversió i la millora de l'eficiència estimada.

3. Establir un diàleg competitiu segons es descriu en el Text Refós de la Llei de contractes del sector públic, aprovat pel Reial decret Legislatiu 3/2011, de 14 de novembre. Els contractes de col·laboració entre el sector públic i el sector privat es podran adjudicar per aquest procediment.

4. Implicar la capa de direcció de negoci en la presa de decisions i les àrees jurídiques per elaborar instruments contractuals que s'adaptin a les necessitats del *Cloud*.

5. Un cop presa la decisió i implantat el component en *Cloud* ha treballar en l'impacte organitzatiu i la gestió del canvi. el personal assignat a l'operació del sistema ha de ser format en la gestió i supervisió dels acords de nivell de servei i en la realització de auditories de servei.

6. Avaluar el resultat i beneficis reals obtinguts en el procés.

# 4 Adquisició de serveis de *Cloud computing* per part de l'Administració

L'adquisició del Cloud computing per part de les Administracions Públiques es troba sotmesa, per raons òbvies, a les regles aplicables per a l'adquisició de béns o serveis per part de les administracions públiques. Resulta aplicable, per tant, per a l'adquisició de serveis *Cloud* per l'Administració, la normativa de contractació publica, que en principi no planteja diferències significatives en comparació amb altres serveis (CATTEDDU, 2011: p. 40). En aquest sentit, s'ha d'estar a les previsions del Text refós de la Llei de contractes del sector públic, aprovat per Reial decret legislatiu 3/2011, de 14 de novembre (en endavant, TRLCSP).

Com a consideració prèvia, com indica GIMENO FELIU, J.M[16] , el procés de incorporació dels diferents Estats a la Unió Europea ha tingut repercussions importants en el contorn i principis del dret administratiu, el que ha suposat una modificació fonamental de les estructures organitzatives internes dels Estats.

Aquesta modificació s'ha basat en l'establiment d'una unitat de mercat que, correlativament, ha suposat una unificació del marc normatiu existents en tots aquells àmbit que són essencials per assolir el mercat únic. Fins i tot, l'autor arriba a parlar de l'existència d'un Dret Administratiu Europeu que, per la via de la uniformitat del fons normatiu que regula l'activitat dels agents europeus que concorren en el mercat, garanteix el correcte funcionament de les activitats econòmiques més enllà de les barreres frontereres dels Estats membres.

Aquest nucli mínim de normació està creixent de manera exponencialment rellevant com a conseqüència de la dimensió internacional que, cada vegada més, estan adquirint els anomenats serveis públics o serveis d'interès general, si anem a la denominació més moderna de la institució. Això suposa que, de manera habitual, la Comunitat s'està convertint en l'últim responsable o garant del correcte funcionament dels sectors econòmics (configurant-se el Dret Administratiu Econòmic com una branca del Dret Administratiu Europeu), al voltant del qual es configuren o persegueixen, com indica GIMENO FELIU, J.M, els objectius consagrats en el Tractat de la Unió Europea, dintre dels quals podem destacar, en l'àmbit de l'activitat econòmica: l'adaptació al dret de la competència, la lluita contra el falsejament de la competència (mitjançant la transparència i publicitat) i el respecte a les regles del mercat quan l'administració actua com a agent econòmic.

[16] "Problemas actuales de la Administración Municipal desde la perspectiva del derecho comunitario: incidència en la organización administrativa de las normas de contratación pública". Revista Andaluza de Administración Pública núm. 71/2008 (Estudis). Instituto Andaluz de Administración Pública, Sevilla. 2008

Aquests aspectes són rellevants a l'hora d'analitzar el Cloud Computing. D'una banda, és evident la submissió a la normativa de contractes a l'hora d'adquirir els serveis Cloud; d'altra banda, és igualment rellevant el judici de competència, als efectes d'evitar que la transparència, concurrència i publicitat no siguin efectives i, finalment, hi ha altres aspectes que, per raó de la seva internacionalitat, són essencials, com és la protecció de dades.

En qualsevol cas, és evident que l'adquisició de serveis Cloud està sotmesa a la normativa de contractes del sector públic, entesa com a instrument al servei dels poders públics per al compliment dels seus objectius o polítiques públiques, en els termes previstos a la Directiva 2004/18 que, als seus considerandos, realitza una exposició detallada de les finalitats a les que ha de respondre la contractació, no tan sols des de la vessant d'adquisició de béns o serveis en les condicions econòmiques més avantatjoses, sinó també des de la vessant d'incidir en els sectors socials i econòmics, amb l'adquisició dels mateixos.

El concepte d'oferta econòmicament més avantatjosa es troba recollit a l'article 150 del TRLCSP, i es tracta d'una variable que no respon exclusivament al preu.

Aquest ha estat un canvi significatiu de la reforma introduïda al 2007, incorporant al concepte "econòmicament més avantatjosa" les altres variables que han de determinar quina, entre les propostes presentades, és la més adequada, d'acord amb els criteris de valoració continguts als plecs que, òbviament, són inalterables. En aquest sentit, podem fer esment de la sentència del Tribunal de Justícia de les Comunitats Europees (Sala Primera).Cas Emm. G. Lianakis AE altres contra Aikaterini Georgoula i altres, de 24 de gener de 2008[17].

Aquest criteri ha estat igualment recollit jurisprudencialment, com a resum, la sentència del Tribunal Superior de Justícia de Madrid (Sala contenciós administrativa, Secció 3ª), núm. 929/2008 de 27 octubre, tracta molt acuradament la matèria[18].

---

[17] "37. En efecto, los licitadores potenciales deben poder conocer la existencia y alcance de dichos elementos en el momento de preparar sus ofertas (véanse en este sentido, en relación con los contratos públicos de servicios, las sentencias, antes citadas, Concordia Bus Finland [ TJCE 2002, 251] , apartado 62, y ATI EAC y Viaggi di Maio y otros [ TJCE 2005, 345] , apartado 23).
38. Por consiguiente, una entidad adjudicadora no puede aplicar reglas de ponderación o subcriterios relativos a los criterios de atribución que no haya puesto previamente en conocimiento de los licitadores (véase, por analogía, en relación con los contratos públicos de obras, la sentencia Universale-Bau y otros [ TJCE 2002, 369] , antes citada, apartado 99)".

[18] "Las pretensiones actoras no pueden ser atendidas, lo que supone la desestimación de este recurso, por las razones que a continuación se exponen,
Como punto de partida, en orden al enjuiciamiento que nos ocupa, conviene reseñar la doctrina jurisprudencial sobre la materia de que se trata, de la que es fiel exponente la Sentencia de la Sala Tercera del Tribunal Supremo de 11 de Julio de 2.006 dictada en recurso de casación 410/04 ( RJ 2006, 8471) .
Según la misma, es tajante el art. 87 de la Ley de Contratos de las Administraciones Públicas ( RCL 1995, 1485, 1948) (LCAP ) al establecer la necesidad de que los pliegos de cláusulas administrativas particulares del concurso fijen los criterios objetivos que han de servir de base para la adjudicación, los cuales se indicarán por orden decreciente de importancia y por la ponderación que les atribuya. Tal exigencia obstaculiza la discrecionalidad administrativa en la adjudicación del concurso por cuanto la Administración para resolverlo ha de sujetarse a la baremación previamente determinada. Su discrecionalidad solo juega con anterioridad a la adjudicación al decidir con libertad de criterio cuáles son los criterios objetivos más significativos respetando, eso sí, las reglas esenciales que impregnan nuestra actual normativa sobre contratación administrativa a partir de la transposición de las múltiples Directivas sobre la materia: publicidad, libre concurrencia y transparencia administrativa.
Por su parte el art. 89 de la LCAP declara que el concurso se adjudicará tras motivar, en todo caso, con referencia a los criterios de adjudicación del concurso que figuren en el pliego. Constituye pues, la motivación, conforme al art. 54.2 de la Ley de Régimen

En el mateix sentit, sentencia TSJ de Madrid núm. 597/2010 de 5 julio (JUR\2010\311439).

Així ho estableix l'article 150 del TRLCSP, al seu apartat 1, ho diu clarament:

"Para la valoración de las proposiciones y la determinación de la oferta económicamente más ventajosa deberá atenderse a criterios directamente vinculados al objeto del contrato, tales como la calidad, el precio, la fórmula utilizable para revisar las retribuciones ligadas a la utilización de la obra o a la prestación del servicio, el plazo de ejecución o entrega de la prestación, el coste de utilización, las características medioambientales o vinculadas con la satisfacción de exigencias sociales que respondan a necesidades, definidas en las especificaciones del contrato, propias de las categorías de población especialmente desfavorecidas a las que pertenezcan los usuarios o beneficiarios de las prestaciones a contratar, la rentabilidad, el valor técnico, las características estéticas o funcionales, la disponibilidad y coste de los repuestos, el mantenimiento, la asistencia técnica, el servicio postventa u otros semejantes.

Cuando sólo se utilice un criterio de adjudicación, éste ha de ser, necesariamente, el del precio más bajo".

---

Jurídico y Procedimiento Administrativo Común ( RCL 1992, 2512, 2775 y RCL 1993, 246) (LRJPAC) un elemento esencial para evitar la arbitrariedad, al tiempo que permite a los demás interesados conocer los argumentos utilizados por la mesa de contratación para, en su caso, impugnar la adjudicación. En tal sentido resulta claro el contenido del art. 94 de LCAP que obliga no sólo a comunicar a los demás participantes en la licitación la adjudicación del contrato sino, incluso, a notificar, previa petición de los interesados, los motivos del rechazo de su proposición y las características de las proposiciones del adjudicatario determinantes de la adjudicación a su favor. Motivación de la decisión que habrá de ser razonada y fundada con arreglo a los criterios del pliego.

Finalmente, el art. 75.3 de LCAP declara que la adjudicación recaerá en el licitador que, en su conjunto, haga la proposición más ventajosa, teniendo en cuenta los criterios que se hayan establecido en los pliegos. No puede adjudicarse a cualquier concursante sino al que haga la proposición más ventajosa a fin de no incurrir en arbitrariedad, es decir que no puede separarse la Administración de los criterios objetivos especificados en los pliegos del concurso. Si bien como recuerda la STS de 24 de Enero de 2.006 (recurso de casación 7645/00 ) ( RJ 2006, 2726) , con cita de otras anteriores como las de 25 de Julio de 1.989 , 1 de Junio de 1.999 ( RJ 1999, 5849) y 7 de Octubre de 1.999 ( RJ 1999, 8840) , la Administración tiene un margen de discrecionalidad en el momento de valorar la proposición más ventajosa y también puede acudir a una interpretación y aplicación de las cláusulas razonable. Por ello como afirma la STS de 24 de Junio de 2.004 (recurso de casación 8816/99 ) ( RJ 2004, 4986) tampoco puede prescindir de los informes técnicos que apoyan una propuesta de adjudicación mediante apreciaciones subjetivas que no tengan un apoyo real en dichos criterios objetivos.

Lo acabado de exponer evidencia que si bien la Administración ostenta, en un primer momento, un margen de discrecionalidad en la fijación de los criterios que han de reunir los que concurran al concurso así como en la determinación de la puntuación atribuible a cada uno de aquellos, no acontece lo propio con la asignación particularizada a cada uno de los concursantes a la vista de la documentación presentada. En esta segunda fase la administración debe respetar absolutamente las reglas que ella estableció en el correspondiente pliego. Es incontestable que en materia de concursos el pliego de condiciones se constituye en la ley del concurso ( SsTS de 28 de Junio de 2.004, recurso de casación 7106/00 ( RJ 2004, 5448) , y de 24 de Enero de 2.006, recurso de casación 7645/00 ( RJ 2006, 2726) ).

Como se dijo en la STS de 28 de Junio de 2.004 (recurso de casación 7106/00 ), con cita de otra anterior de 4 de Noviembre de 1.997 ( RJ 1997, 8158) , "puede resultar contrario a la buena fe, que debe presidir el contrato, el que se consienta una o varias cláusulas o prescripciones técnicas, aceptando el procedimiento de contratación pública mediante la propia participación y luego, al no resultar, adjudicatario, impugnar la adjudicación argumentado que los actos de preparación consentidos son contrarios al ordenamiento jurídico".

Significa, pues, que aceptadas las bases de la convocatoria solo podemos entrar a examinar si la adjudicación del concurso ha respetado o no los pliegos de condiciones. Como se afirmaba en la STS de 28 de Junio de 2.004 (recurso de casación 7106/00 ) "la naturaleza contractual, y no reglamentaria, de los pliegos de cláusulas explica y justifica que la falta de impugnación convalide sus posibles vicios, a menos que se trate de vicios de nulidad de pleno derecho; e, incluso, en este caso en que puede entenderse que la denuncia no está sujeta a plazo preclusivo, habría de seguirse una acción de nulidad con sujeción a los criterios generales de ésta, siempre que resulta a salvo el indicado principio de buena fe y la seguridad jurídica, a cuya preservación tiende la firmeza de los actos para quienes los han consentido, aspirando incluso, en su día a la adjudicación".

És a dir, l'oferta econòmicament més avantatjosa és la que resulta de la ponderació de tots els criteris fixats per l'Administració, entre els quals es troba el preu.

A partir d'aquesta concepció, com és conegut, l'adquisició d'una prestació o servei per part de l'administració requereix la corresponent tramitació de l'expedient. Així, d'acord amb l'article 93 de la LCSP, la signatura de contractes per part de les administracions públiques requereix la tramitació prèvia de l'expedient corresponent, que l'inicia l'òrgan de contractació motivant la necessitat del contracte.

La necessitat del contracte es troba recollida a l'article 22 de la LCSP ("Necesidad e idoneidad del contrato y eficiencia en la contratación"), conforme al qual,

"1. Los entes, organismos y entidades del sector público no podrán celebrar otros contratos que aquellos que sean necesarios para el cumplimiento y realización de sus fines institucionales. A tal efecto, la naturaleza y extensión de las necesidades que pretenden cubrirse mediante el contrato proyectado, así como la idoneidad de su objeto y contenido para satisfacerlas, deben ser determinadas con precisión, dejando constancia de ello en la documentación preparatoria, antes de iniciar el procedimiento encaminado a su adjudicación.

2. Los entes, organismos y entidades del sector público velarán por la eficiencia y el mantenimiento de los términos acordados en la ejecución de los procesos de contratación pública, favorecerán la agilización de trámites, valorarán la innovación y la incorporación de alta tecnología como aspectos positivos en los procedimientos de contratación pública y promoverán la participación de la pequeña y mediana empresa y el acceso sin coste a la información, en los términos previstos en la presente Ley".

En aquest sentit, aquesta necessitat i idoneïtat resulta especialment significativa en àmbits com són el de la incorporació de les noves tecnologies al funcionament o actuació de les Administracions Públiques, ja que suposa la incorporació de nous paràmetres o formes d'actuació que requereixen una adaptació orgànica i funcional de les estructures administratives i, al mateix temps, una determinació prèvia molt acurada del que es vol aconseguir amb la contractació que es vol dur a terme.

### 4.1.Tramitació de l'expedient

Això es realitza mitjançant la tramitació del corresponent administratiu, en què s'haurà de delimitar clarament l'objecte del contracte, així com les regles que han de regir la contractació. Aspectes, tots aquests, que s'han d'incorporar als plecs de clàusules administratives i de prescripcions tècniques.

Així, a l'expedient de contractació s'incorporaran el plec de clàusules administratives particulars i el de prescripcions tècniques que han de regir el contracte. Així mateix s'haurà d'incorporar el

certificat d'existència de crèdit o document que legalment el substitueixi i la fiscalització prèvia de la intervenció.

Els plecs de clàusules administratives i el de prescripcions tècniques són la llei del contracte, i són bàsiques als efectes de delimitar la contractació que s'ha de dur a terme[19].

En aquest sentit, l'article 145.1 TRLCSP, disposa que les proposicions dels interessats hauran d'ajustar-se a allò previst en el plec de clàusules administratives particulars i que la seva presentació suposa l'acceptació incondicionada del contingut de la totalitat de les esmentades clàusules o condicions, sense reserva alguna.

D'acord amb l'exposat, és essencial tenir predeterminat l'objecte del contracte, i els condicionants tècnics i econòmics d'aquest. Cas contrari, si no es defineixen aquest o no apareixen recollits o delimitats de manera clara en els plecs, serà absolutament impossible conciliar les ofertes presentades amb les veritables necessitats de l'administració i, consegüentment, no s'aconseguirà la finalitat a la que ha de respondre l'administració pública quan contracta.

En qualsevol cas, pel que fa a la contractació dels serveis Cloud, es pot avançar que, en la mesura de què hi ha variables tècniques, econòmiques i financeres que poden incidir no tan sols en la contractació sinó fins i tot en la determinació prèvia de l'objecte d'aquesta, el diàleg competitiu és una eina que sembla adequada per aconseguir les finalitats previstes.

### 4.2. Requeriments de capacitat i solvència

Igualment, cal tenir present que, per raó de la quantia, poden ser exigibles uns determinats requeriments de capacitat i solvència en el licitador i, fins i tot, que estigui prèviament classificat.

La classificació es troba recollida a l'article 13, "Exigència de classificació", quan indica els subjectes que es troben sotmesos a regulació harmonitzada:

"1. Son contratos sujetos a una regulación armonizada los contratos de colaboración entre el sector público y el sector privado, en todo caso, y los contratos de obras, los de concesión de obras públicas, los de suministro, y los de servicios comprendidos en las categorías 1 a 16 del Anexo II, cuyo valor estimado, calculado conforme a las reglas que se establecen en el artículo 88,

[19] Com indica la Sentència del Tribunal Suprem de 19 de març de 2001 (Ar. 2880), "...esta Sala Tercera ha recordado, en sentencia de 6 de febrero de 2001, la consolidada doctrina jurisprudencial en cuya virtud el pliego de condiciones constituye la ley del concurso, debiendo someterse a sus reglas tanto el organismo convocante como quienes soliciten tomar parte en el mismo, especialmente cuando no hubieran impugnado previamente sus bases, pues, en efecto, si una entidad licitante se somete al concurso tal y como ha sido convocado, sin impugnar en ningún momento las condiciones y bases por las que se rija, tomando parte en el mismo, con presentación de su correspondiente oferta, y prestando su consentimiento tanto a las propias prescripciones de la licitación como a la participación de las restantes entidades, carecerá de legitimación para impugnarlo después, contraviniendo sus «propios actos», cuando no resulte favorecida por las adjudicaciones, que obviamente, pretendía".

sea igual o superior a las cuantías que se indican en los artículos siguientes, siempre que la entidad contratante tenga el carácter de poder adjudicador"

En aquest sentit, caldrà determinar prèviament la tipologia del contracte ja que, en funció d'aquesta tipologia, canvien els ombralls a considerar, per determinar si el licitador reuneix, amb caràcter previ, els elements o criteris tècnics o econòmics suficients per poder assolir la realització del contracte, en el cas que resultés adjudicatari:

Si el considerem contracte de subministrament, l'article 15, actualitzat per la Ordre per l'article únic 1 de l'Ordre EHA/3479/2011, de 19 de desembre, disposa:

"1. Están sujetos a regulación armonizada los contratos de suministro cuyo valor estimado sea igual o superior a las siguientes cantidades:

a) 130.000 euros, cuando se trate de contratos adjudicados por la Administración General del Estado, sus organismos autónomos, o las Entidades Gestoras y Servicios Comunes de la Seguridad Social. No obstante, cuando los contratos se adjudiquen por órganos de contratación que pertenezcan al sector de la defensa, este umbral solo se aplicará respecto de los contratos de suministro que tengan por objeto los productos enumerados en el anexo III.

b) 200.000 euros, cuando se trate de contratos de suministro distintos, por razón del sujeto contratante o por razón de su objeto, de los contemplados en la letra anterior".

Pel que fa als contractes de serveis, l'article 16 indica:

"1. Están sujetos a regulación armonizada los contratos de servicios comprendidos en las categorías 1 a 16 del Anexo II cuyo valor estimado sea igual o superior a las siguientes cantidades:

a) 130.000 euros, cuando los contratos hayan de ser adjudicados por la Administración General del Estado, sus organismos autónomos, o las Entidades Gestoras y Servicios Comunes de la Seguridad Social, sin perjuicio de lo dispuesto para ciertos contratos de la categoría 5 y para los contratos de la categoría 8 del Anexo II en la letra b) de este artículo.

b) 200.000 euros, cuando los contratos hayan de adjudicarse por entes, organismos o entidades del sector público distintos a la Administración General del Estado, sus organismos autónomos o las Entidades Gestoras y Servicios Comunes de la Seguridad Social, o cuando, aun siendo adjudicados por estos sujetos, se trate de contratos de la categoría 5 consistentes en servicios de difusión de emisiones de televisión y de radio, servicios de conexión o servicios integrados de telecomunicaciones, o contratos de la categoría 8, según se definen estas categorías en el Anexo II".

Veiem que les quanties són les mateixes tant en l'àmbit del contracte de serveis com de subministrament. En aquest sentit, tan sols s'ha de tenir present que si el Contracte està subjecte a subjecte a regulació harmonitzada, s'ha d'exigir classificació del contractista.

## 4.3. Tipologia del contracte

Com ja hem avançat, cal definir la tipologia del contracte davant del qual ens trobem i, per realitzar aquesta concreció, s'ha de partir prèviament de l'objecte del contracte.

### 4.3.1. Objecte i preu del contracte

L'article 86 del TRLCAP indica que l'objecte dels contractes del sector públic ha de ser determinat i, a continuació, indica l'article 87, en relació amb el preu, que:

"1. En los contratos del sector público, la retribución del contratista consistirá en un precio cierto que deberá expresarse en euros, sin perjuicio de que su pago pueda hacerse mediante la entrega de otras contraprestaciones en los casos en que ésta u otras Leyes así lo prevean. Los órganos de contratación cuidarán de que el precio sea adecuado para el efectivo cumplimiento del contrato mediante la correcta estimación de su importe, atendiendo al precio general de mercado, en el momento de fijar el presupuesto de licitación y la aplicación, en su caso, de las normas sobre ofertas con valores anormales o desproporcionados.

2. El precio del contrato podrá formularse tanto en términos de precios unitarios referidos a los distintos componentes de la prestación o a las unidades de la misma que se entreguen o ejecuten, como en términos de precios aplicables a tanto alzado a la totalidad o a parte de las prestaciones del contrato. En todo caso se indicará, como partida independiente, el importe del Impuesto sobre el Valor Añadido que deba soportar la Administración".

En definitiva, les variables d'objecte i preu són essencials per configurar el contracte.

Sobre aquesta base, s'ha de diferenciar si l'objecte del contracte és l'adquisició d'una infraestructura (IaaS) per a emmagatzematge, quan es contracta una plataforma (PaaS) que tingui per objecte la prestació de serveis mitjançant les aplicacions allà instal•lades, quan es tracta de l'adquisició de software (SaaS), o quan es tracta de l'adquisició integral d'un servei (PraaS).

Aquestes diferents tipologies de contractació incidiran igualment en les obligacions que assumeixi, especialment en matèria de seguretat, el contractista.

### 4.3.2. Contracte típic

Amb caràcter previ, s'ha d'analitzar si ens trobem davant d'un contracte dels previstos al TRLCSP i, consegüentment, sotmès a totes les seves previsions o, pel contrari, ens trobaríem dintre dels contractes atípics, que tan sols es trobarien sotmesos a les previsions de la contractació pública en els aspectes relacionats amb la preparació i adjudicació.

Així, caldria avaluar si ens trobem davant d'un contracte privat, configurat com una cessió d'ús. Cal tenir present que, l'article 4.1 p) de la Llei 30/2007, de 30 d'octubre, de contractes del sector públic, exclou del seu àmbit d'aplicació els contractes de compravenda, donació, permuta, arrendament i altres negocis jurídics anàlegs sobre béns immobles, valors negociables i propietats incorporals, tret que recaiguin sobre programes d'ordinador i hagin de ser qualificats de contractes de subministrament o serveis, que sempre tenen el caràcter de contractes privats i es regeixen per la legislació patrimonial.

A més, indica el TRLCSP que:

"En estos contratos no podrán incluirse prestaciones que sean propias de los contratos típicos regulados en la Sección 1ª del Capítulo II del Título Preliminar, si el valor estimado de las mismas es superior al 50 por 100 del importe total del negocio o si no mantienen con la prestación característica del contrato patrimonial relaciones de vinculación y complementariedad en los términos previstos en el artículo 25; en estos dos supuestos, dichas prestaciones deberán ser objeto de contratación independiente con arreglo a lo establecido en esta Ley".

El paràgraf p) de l'artícle 4.1 TRLCSP és exigència del Dret Comunitari, en particular de la Directiva 2004/18, de 31 de març (considerando 24), que específicament considera «que los contratos relativos a la adquisición o arrendamiento de bienes inmuebles o relativos a derechos respecto de dichos bienes revisten características especiales, debido a las cuales no resulta adecuado aplicar a esos contratos normas de adjudicación».

Per tant, si ens trobéssim davant d'un contracte privat, concretament un contracte d'arrendament, en virtut del qual cada una de les parts s'obliga a transferir temporalment el ús i gaudi d'un immoble a l'altra a canvi d'un preu cert i determinat, es trobaria exclòs de la LCSP i sotmès a la legislació patrimonial.

Respecte als contractes privats disposa l'article 20 del TRLCSP, que es regeixen, quant a la preparació i adjudicació, en defecte de normes específiques, per aquesta Llei i les seves disposicions de desplegament, i supletòriament s'hi han d'aplicar les altres normes de dret administratiu o, si s'escau, les normes de dret privat, segons que correspongui per raó del subjecte o entitat contractant. Pel que fa als seus efectes i extinció, aquests contractes es regeixen pel dret privat.

No obstant l'exposat anteriorment, cal tenir present que un contracte de Cloud Computing difícilment es podrà qualificar com a contracte privat, per diferents raons: en primer lloc, perquè encaixaria en una de les figures típiques dels contractes del sector públic, ja el configurem com a contracte de serveis o contracte de subministrament; en segon lloc, perquè el propi article de la normativa de contractes fa referència a programes d'ordinador, el que aporta un altre element a considerar per excloure la seva naturalesa privada; en tercer lloc, perquè si existeixen altres prestacions accessòries d'altres contractes, i excedeixen del 50% o no són vinculades o

complementàries de la contractació principal, aquestes han de ser objecte de contractació independent.

En qualsevol cas, s'ha de tenir present que, fins i tot configurant-lo com a contracte privat, la preparació i adjudicació estaria sotmesa a les normes de contractació pública, el que elimina en gran part els dubtes que es puguin derivar, tot i que això dependrà, en gran manera, del tipus de Cloud que es vulgui adquirir.

En el cas que ens trobem davant d'un Cloud públic, en què les condicions són fixades unilateralment per una de les parts, tal com passa en els contractes d'adhesió, el marge de maniobra de l'administració serà molt més reduït, i tan sols podrà modular la preparació i adquisició, però els marges de maniobra seran molt més reduïts que en els altres tipus de Cloud (per raons òbvies, un Cloud públic és un model de negoci en massa, en què l'adaptació a les necessitats de l'Administració i les seves particularitats és molt més complicat i, fins i tot, possiblement requeriria unes necessitats addicionals d'inversió que fan menys interessant la prestació per part del contractista).

En qualsevol cas, amb aquesta primera aproximació, ja veiem que són moltes les variables a considerar, el que ens portarà probablement a cercar modalitats de contractació més flexibles, que permetin adaptar-ne millor les necessitats i requeriments de l'Administració a les possibilitats que ofereix el mercat. En aquest sentit, la col·laboració publicoprivada sembla que sigui la modalitat més idònia.

### 4.3.3. Contracte de serveis o de subministrament

A l'hora de configurar un contracte d'adquisició de Cloud, hem d'avaluar si ens trobem davant d'un contracte de subministrament, de serveis, o si seria un contracte que incorpora prestacions pròpies de cadascun d'aquests contractes.

L'article 9 del TRLCSP indica:

"1. Son contratos de suministro los que tienen por objeto la adquisición, el arrendamiento financiero, o el arrendamiento, con o sin opción de compra, de productos o bienes muebles.

2. Sin perjuicio de lo dispuesto en la letra b) del apartado 3 de este artículo respecto de los contratos que tengan por objeto programas de ordenador, no tendrán la consideración de contrato de suministro los contratos relativos a propiedades incorporales o valores negociables.

3. En todo caso, se considerarán contratos de suministro los siguientes:

a) Aquellos en los que el empresario se obligue a entregar una pluralidad de bienes de forma sucesiva y por precio unitario sin que la cuantía total se defina con exactitud al tiempo de celebrar el contrato, por estar subordinadas las entregas a las necesidades del adquirente. No obstante, la

adjudicación de estos contratos se efectuará de acuerdo con las normas previstas en el Capítulo II del Título II del Libro III para los acuerdos marco celebrados con un único empresario.

b. Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios.

c. Los de fabricación, por los que la cosa o cosas que hayan de ser entregadas por el empresario deban ser elaboradas con arreglo a características peculiares fijadas previamente por la entidad contratante, aun cuando ésta se obligue a aportar, total o parcialmente, los materiales precisos.

Pel contrari, els contractes de serveis (art. 10 TRLCSP) estableix que són contractes de serveis els que tenen per objecte prestacions de fer consistents en el desenvolupament d'una activitat o dirigides a obtenir un resultat diferent d'una obra o un subministrament. Als efectes de l'aplicació del TRLCSP, els contractes de serveis es divideixen en les categories enumerades a l'annex II.

Si examinem aquest annex, veiem que l'apartat 7 parla de "Servicios de informática y servicios conexos", el mateix s'ha de dir del número de referència 84 del CPC.

Com indica PALOMAR OJEDA, A.[20], ens podríem trobar davant d'un contracte de subministrament si el configurem com un arrendament –amb o sense opció de compra- de productes (és rellevant el que indica la lletra b de l'apartat 3, a l'hora de triar si ens trobem davant d'un contracte de subministrament o de serveis).

Si el configurem com un contracte de subministrament, hem d'estar al marc jurídic d'aquest contracte i, en particular, són d'especial interès les previsions dels articles 290, 292 i 295 del TRLCSP, referides específicament al manteniment, a l'obligació de lliurament i recepció, i a les facultats d'inspecció.

D'aquest règim jurídic, com manifesta PALOMAR OJEDA, A., tot i que l'obligació de manteniment recau en l'arrendador, resulta complicat per part del contractant l'exercici de les facultats de visionar i controlar els suports posats a la seva disposició, ja que, en la majoria de les ocasions, ens trobarem amb un contracte de simple posada a disposició d'un espai determinat per poder dur a terme funcions d'emmagatzematge.

En aquest sentit, la figura del contracte de subministrament es podria aplicar, sense problema, en aquells supòsits en què l'Administració es limita a contractar Cloud entès com a espai per dur a terme les funcions d'emmagatzematge.

[20] "Incidencia del Cloud Computing en el ámbito de la contratación pública". Monografias Civitas. "Derecho y cloud computing". Ed. Ricard Martinez Martinez, Aranzadi 2012.

A diferència del contracte de subministrament, el contracte de serveis suposa un salt qualitatiu, en la mesura de què no es limita a una adquisició d'una determinada capacitat d'emmagatzematge (que seria exclusivament aplicable en relació amb el Cloud públic), sinó que es traslladaria a aquells altres supòsits en què l'Administració no es limita a l'adquisició d'unes determinades capacitats d'arxiu, condicionades a les condicions de subministrament preestablertes, sinó que vol anar més enllà, satisfent no tan sols aquesta finalitat, sinó també altres prestacions que, en certa mesura, s'aproparien a l'adquisició de programes informàtics a mida.

Amb aquesta modalitat de contractació, seria més factible l'adaptació a les singularitats que es deriven del que és una actuació administrativa, permetent la compatibilitat entre diferents tipologies de Cloud i, fins i tot, adequant una tipologia a les particularitats que es puguin derivar, ja sigui per raó de la naturalesa de les dades més o menys sensibles que hagin de ser objecte de tractament, ja sigui per raó de la tipologia dels serveis o de les infraestructures que es vulguin ubicar al Cloud.

Tal com indica PALOMAR OJEDA, A., la qüestió més rellevant és la que fa referència a la propietat intel·lectual, recollida a l'article 301.2 del TRLCSP, i que és igualment objecte d'anàlisi en el present projecte de recerca:

"Salvo que se disponga otra cosa en los pliegos de cláusulas administrativas o en el documento contractual, los contratos de servicios que tengan por objeto el desarrollo y la puesta a disposición de productos protegidos por un derecho de propiedad intelectual o industrial llevarán aparejada la cesión de éste a la Administración contratante. En todo caso, y aun cuando se excluya la cesión de los derechos de propiedad intelectual, el órgano de contratación podrá siempre autorizar el uso del correspondiente producto a los entes, organismos y entidades pertenecientes al sector público a que se refiere el artículo 3.1".

Igualment, dintre de la determinació del preu, s'haurà d'estar a les previsions de l'article 302 del TRLCSP:

"En el pliego de cláusulas administrativas se establecerá el sistema de determinación del precio de los contratos de servicios, que podrá estar referido a componentes de la prestación, unidades de ejecución o unidades de tiempo, o fijarse en un tanto alzado cuando no sea posible o conveniente su descomposición, o resultar de la aplicación de honorarios por tarifas o de una combinación de varias de estas modalidades".

No es pot deixar de banda que, en aquests casos, la determinació o la concreció d'aquests elements en el plec de clàusules administratives serà essencial per dur a terme una contractació que resulti eficient des del punt de vista de la prestació a obtenir. En qualsevol cas, caldrà igualment tenir present el procediment d'adjudicació que es pugui emprar, ja sigui obert o restringit, o la possibilitat més restrictiva d'aplicar el procediment negociat en els supòsits taxatius establerts pel TRLCSP, que no poden interpretar-se de manera extensiva, tal com ha entès de manera reiterada el Tribunal de Justícia de les Comunitats Europees.

En cas de que el procediment negociat fos possible, caldria tenir present els elements que poden ser objecte de negociació, així com tots els condicionants que aquesta modalitat d'adjudicació porta aparellats.

Segons l'article 169 del TRLCSP, en el procediment negociat l'adjudicació recau en el licitador elegit justificadament per l'òrgan de contractació, després d'efectuar consultes amb diversos candidats i negociar les condicions del contracte amb un o diversos d'ells. Per altra banda, d'acord amb l'article 178.1 de la TRLCSP, en el procediment negociat és necessari sol·licitar ofertes, almenys, a tres empreses capacitades per a la realització de l'objecte del contracte, sempre que sigui possible.

S'ha de tenir en compte l'article 177.2 del TRLCSP que estableix que en els contractes no subjectes a regulació harmonitzada que es puguin adjudicar per procediment negociat perquè la seva quantia és inferior a la indicada a l'article 174 e) s'han de publicar anuncis de conformitat amb el que preveu l'article 142 quan el valor estimat sigui superior a 60.000,00 euros.

D'altra banda, segons l'article 169 del TRLCSP, en el procediment negociat, l'adjudicació recau en el licitador elegit justificadament per l'òrgan de contractació, després d'efectuar consultes amb diversos candidats i negociar les condicions del contracte amb un o diversos d'ells. En virtut del que disposa l'article 178.1 del TRLCSP, és necessari que l'òrgan de contractació sol·liciti ofertes, almenys, a tres empreses capacitades per a la realització de l'objecte del contracte, sempre que sigui possible i el nombre de licitadors capacitats per executar el contracte sigui prou ampli per garantir una competència efectiva, sempre que s'hagin presentat un nombre suficient de solucions o de candidats adequats. Es tracta, així doncs, d'una norma que estableix dos requisits per a la tramitació del procediment negociat. En primer lloc que es sol·licitin ofertes com a mínim a tres empreses i, en segon lloc, que les empreses a les què es sol·liciti oferta estiguin capacitades per a la realització de l'objecte del contracte.

Cap dubte no pot ni ha de plantejar el primer dels requisits, però el segon suscita la qüestió de com s'ha de considerar complert de forma adequada el requisit que les empreses estiguin capacitades per a la realització de l'objecte del Contracte.

Sobre aquest extrem s'ha pronunciat la Junta Consultiva de Contractació Administrativa Estatal a l'Informe 65/2009, de 23 de juliol de 2010:

"Per determinar l'abast del requisit de capacitació és precís acudir a la interpretació finalista del precepte. Així, s'ha de posar de manifest que l'exigència d'aquest requisit no té cap altra finalitat que la d'evitar que el mínim de concurrència que la Llei exigeix per a aquest cas resulti desvirtuat mitjançant la sol·licitud d'ofertes a empreses dedicades a activitats no relacionades amb l'objecte del contracte. D'aquesta forma seria possible excloure la competència sol•licitant l'oferta a tres empreses, de les quals una de sola estigués en condicions d'executar el contracte. Es compliria el requisit del número, però no s'hauria produït una concurrència real. Per evitar aquest efecte, la Llei

exigeix que la sol·licitud d'oferta es dirigeix a empreses que, objectivament, estiguin capacitades per a l'execució del contracte.

D'aquesta forma no es pot convidar qualsevol empresa, sinó aquelles que puguin executar el contracte i, per tant, competir realment en la licitació."

Al mateix informe de la Junta Consultiva de Contractació Administrativa Estatal es planteja la qüestió de si n'hi ha prou amb sol·licitar les tres ofertes a empreses capacitades, o si és necessari en obtenir la prestació d'oferta per totes elles:

"Referent a això, és necessari establir amb claredat el principi que tot procediment d'adjudicació té com a finalitat fonamental permetre l'accés a la contractació pública de totes les empreses que estiguin en condicions de formular una oferta. Per això, les successives Directives comunitàries han posat èmfasi en la publicitat de les licitacions, i per això, el legislador espanyol, anant més enllà fins i tot allò a què l'obligava la norma comunitària, va exigir que, almenys es sol•licitessin tres ofertes en el procediment negociat. No fa falta una lectura detinguda de la Llei per comprendre fins i tot quin punt aquest principi constitueix el fonament de la regulació que la LCSP fa dels diferents procediments d'adjudicació. N'hi ha prou amb recordar el contingut dels articles 1 i 123 per entendre-ho d'aquesta manera.

L'anterior suposa que un procediment d'adjudicació s'adequarà més a l'esperit de la norma quant més garantit estigui el principi de lliure concurrència. Això tractant-se del procediment negociat es compleix a través del requisit de publicitat, quan procedeixi i, en un altre cas, mitjançant la sol·licitud d'ofertes a empreses capacitades. Tanmateix és principi general del Dret que ningú no està obligat a fer impossible ("ad imposiblia nemo tenetur"), raó per la qual, si sol·licitades les ofertes que la Llei exigeix, sol se n'haguessin presentat dos o, fins i tot, una, l'òrgan de contractació no està obligat continuar sol·licitant-ne més a aconseguir que es presentin tres.

Dit això, tanmateix, resulta obligat deixar constància que la bona pràctica des del punt de vista de la gestió exigeix que s'insisteixi en la recerca d'ofertes d'una manera raonable, en cas que alguna o algunes de les primeres sol·licituds no haguessin donat resultat".

Aquests criteris han de ser presos en consideració a l'hora d'acudir, si s'escau, al procediment negociat. Pel contrari, els procediments oberts i restringits, com a procediments ordinaris d'adjudicació, no plantegen aquests problemes, tot i que s'ha de reconèixer que són, en ocasions, menys flexibles, especialment quan existeixen elements tècnics que no són de fàcil predeterminació per part de l'òrgan de contractació.

En qualsevol cas, tal com s'exposa de manera reiterada en el present projecte de recerca, la singularitat de la contractació del Cloud, especialment que es tracta de l'adquisició per part d'administracions territorials molt dimensionades, en què existeixen múltiples variables a considerar, fan recomanables l'aplicació de la col·laboració publicoprivada canalitzada mitjançant el diàleg competitiu.

### 4.3.4. Contracte mixt

D'altra banda, al marge del que s'ha exposat amb anterioritat en relació amb si ens trobem davant d'un contracte de subministrament o de serveis, cal tenir present que no necessàriament un contracte contindrà prestacions enquadrables en un únic contracte, en la mesura de que un contracte pot tenir per objecte prestacions pròpies de diferents. En aquests casos, ens trobaríem davant d'un contracte mixt, en relació amb el qual la normativa de contractes estableix regles per a la determinació del règim jurídic aplicable.

Segons indica l'article 12 del TRLCSP, quan un contracte contingui prestacions corresponents a un altre o altres de diferent classe s'ha d'atendre en tot cas, per a la determinació de les normes que s'hagin d'observar en la seva adjudicació, al caràcter de la prestació que tingui més importància des del punt de vista econòmic.

En aquest sentit, s'haurà d'estar a la prestació que tingui més importància des del punt de vista econòmic, ja sigui de servei o de subministrament, pel que fa a la determinació de les condicions de preparació i adjudicació del contracte corresponent.

D'altra banda, pel que fa als contractes mixtos, cal tenir present l'article 25.2 del TRLCSP que, al referir-se a la llibertat de pactes, estableix que només es poden fusionar prestacions corresponents a diferents contractes en un contracte mixt quan aquestes prestacions estiguin directament vinculades entre si i mantinguin relacions de complementarietat que exigeixin la seva consideració i tractament com una unitat funcional dirigida a la satisfacció d'una determinada necessitat o a la consecució d'un fi institucional propi de l'ens, organisme o entitat contractant.

Amb aquesta finalitat, l'òrgan de contractació haurà de delimitar les prestacions objecte del contracte, i quantificar aquestes, dintre de la documentació que integra l'expedient de contractació, on haurà de justificar que ens trobem davant d'un contracte mixt, però que es regirà per un dels contractes que constitueixen el seu objecte, atenent al que sigui més rellevant, des de la vessant econòmica.

Així, pel que fa a l'adjudicació s'atendrà a les normes del contracte que sigui majoritari, segons estableix l'article 115 del TRLCSP, relatiu als plecs de clàusules administratives particulars, conforme al qual en aquests s'hi han d'incloure els pactes i condicions definidors dels drets i les obligacions de les parts del contracte i les altres mencions requerides pel TRLCSP i les seves normes de desplegament. En el cas de contractes mixtos, s'haurà de detallar el règim jurídic aplicable als seus efectes, compliment i extinció, atenent a les normes aplicables a les diferents prestacions fusionades en els diferents contractes en joc.

### 4.3.5. Acord Marc

També, dintre de les modalitats de la normativa de contractes, s'ha de plantejar igualment la possibilitat d'un acord marc d'homologació.

L'acord marc d'homologació no determina una despesa directa, ja que simplement determina les condicions en base a les quals, l'òrgan o òrgans de contractació, en funció de les seves necessitats, i a l'empara de l'acord marc, demanaran o contractaran els corresponents serveis.

L'article 196 TRLCSP disposa:

"1. Los órganos de contratación del sector público podrán concluir acuerdos marco con uno o varios empresarios con el fin de fijar las condiciones a que habrán de ajustarse los contratos que pretendan adjudicar durante un período determinado, siempre que el recurso a estos instrumentos no se efectúe de forma abusiva o de modo que la competencia se vea obstaculizada, restringida o falseada.

2. Cuando el acuerdo marco se concluya con varios empresarios, el número de éstos deberá ser, al menos, de tres, siempre que exista un número suficiente de interesados que se ajusten a los criterios de selección o de ofertas admisibles que respondan a los criterios de adjudicación.

3. La duración de un acuerdo marco no podrá exceder de cuatro años, salvo en casos excepcionales, debidamente justificados.

Aquest acord marc s'ha de realitzar a l'empara de les previsions legalment establertes i, tal com ja s'ha indicat, no existeix un preu cert, sinó un valor estimat del contracte. En aquest sentit, a l'hora de delimitar el que s'ha d'entendre per quantia, l'article 317 de la mateixa llei de contractes preveu l'autorització del Consell de Ministres per celebrar contractes, "cuando el valor estimado del contrato, calculado conforme a lo señalado en el artículo 88, sea igual o superior a doce millones de euros".

Aquest article, d'acord amb la disposició final 7ª, no té caràcter bàsic.

Igualment, s'ha de tenir present que l'article 12.2.a) de l'anterior llei de contractes, contenia una previsió semblant, tot i que emprava el terme de "pressupost", que ara ha estat substituït pel de "valor estimat".

Pel contrari, en ocasions, per parlar de les autoritzacions per contractar, s'utilitza el terme de pressupost (el tenor literal de l'article 45 de la Llei 16/2008 és: "Si el pressupost del contracte és igual o superior a 12.000.000 d'euros, IVA exclòs").

Aquest concepte de pressupost no es troba definit de manera expressa a la llei de contractes, més enllà de la delimitació del preu que es fa a l'article 75, quan estableix que el preu s'ha de estimar d'acord amb el preu general de mercat, en el moment de fixar el pressupost de licitació. D'altra

banda, el valor estimat de l'article 76 és un concepte més ampli que inclou, entre d'altres, eventuals pròrrogues.

En relació al pressupost, aquest es troba exclusivament definit a l'article 131 del Reglament de contractes, en relació als projectes d'obres, diferenciant el concepte de pressupost d'execució material i pressupost base de licitació (aquest s'incrementa amb determinats conceptes i, entre d'altres, el de l'IVA).

No obstant això, a l'article 195 s'indica, en relació als contractes de serveis, que "en los contratos en que no se especifique su presupuesto base de licitación su valor estimado se calculará de acuerdo con los siguientes criterios:

Cuando los contratos sean de duración determinada, el valor del contrato será el importe total de las prestaciones durante ese período, incluidas sus posibles prórrogas".

D'altra banda, en la pràctica els plecs acostumen a utilitzar un altre terme addicional al preu i al valor estimat, que és el concepte de despesa.

L'informe de la Junta Consultiva de contractació estatal, 26/2008, de 2 de desembre, indica que "La determinación del significado concreto de estos términos debe hacerse en función del contexto en que se incluyen y por tanto, al menos en principio, no cabe hacer una definición genérica. Ello no obstante, y por regla general cabe decir que deberán identificarse con el término que, en función de la fase en que se encuentre el contrato –fase de preparación y adjudicación o fase de ejecución– indique el valor del mismo con arreglo a la Ley. Así en la fase de preparación y adjudicación deberán entenderse los términos como referidos al presupuesto que deba servir de base para la celebración de la licitación pública y en la de ejecución deberá entenderse que los términos utilizados se refieren al precio de adjudicación del contrato, es decir, el que deba percibir íntegro el contratista que hubiera resultado adjudicatario del contrato".

Traslladant aquests criteris a un Acord Marc, i tractant-se de la licitació i adjudicació d'aquests, el pressupost, a l'empara de la previsió de l'article 195 del Reglament, hauria d'incloure les possibles pròrrogues, amb la qual cosa s'identificaria amb el concepte de valor estimat per a la licitació de l'Acord Marc, sense perjudici dels contractes que es puguin atorgar al seu empara.

En aquest sentit, és igualment rellevant tenir present que, atenent a que en moltes ocasions, ens trobarem amb contractes de quantia significativa, hauran de recavar-se les autoritzacions dels corresponents òrgans de Govern .

Igualment, cal tenir present, d'acord amb les potestats autoorganitzatives, els òrgan de contractació en l'àmbit de cadascuna de les Administracions Públiques .

### 4.3.6. Diàleg competitiu: naturalesa

L'objecte del diàleg competitiu és la licitació d'un contracte que té per objecte desenvolupar una o diverses solucions susceptibles de satisfer les necessitats de l'òrgan de contractació, en què les variables econòmiques, tècniques i financeres no ha estat possible que siguin predeterminades per part de l'òrgan de contractació.

La normativa de contractes del sector públic el defineix a l'article 11, quan parla del contracte de col·laboració publicoprivat:

"Son contratos de colaboración entre el sector público y el sector privado aquellos en que una Administración Pública o una Entidad pública empresarial u organismo similar de las Comunidades Autónomas encarga a una entidad de derecho privado, por un período determinado en función de la duración de la amortización de las inversiones o de las fórmulas de financiación que se prevean, la realización de una actuación global e integrada que, además de la financiación de inversiones inmateriales, de obras o de suministros necesarios para el cumplimiento de determinados objetivos de servicio público o relacionados con actuaciones de interés general, comprenda alguna de las siguientes prestaciones:

a.La construcción, instalación o transformación de obras, equipos, sistemas, y productos o bienes complejos, así como su mantenimiento, actualización o renovación, su explotación o su gestión.

b.La gestión integral del mantenimiento de instalaciones complejas.

c.La fabricación de bienes y la prestación de servicios que incorporen tecnología específicamente desarrollada con el propósito de aportar soluciones más avanzadas y económicamente más ventajosas que las existentes en el mercado.

d.Otras prestaciones de servicios ligadas al desarrollo por la Administración del servicio público o actuación de interés general que le haya sido encomendado.

2. Sólo podrán celebrarse contratos de colaboración entre el sector público y el sector privado cuando previamente se haya puesto de manifiesto, en la forma prevista en el artículo 134, que otras fórmulas alternativas de contratación no permiten la satisfacción de las finalidades públicas.

3. El contratista puede asumir, en los términos previstos en el contrato, la dirección de las obras que sean necesarias, así como realizar, total o parcialmente, los proyectos para su ejecución y contratar los servicios precisos.

4. La contraprestación a percibir por el contratista colaborador consistirá en un precio que se satisfará durante toda la duración del contrato, y que podrá estar vinculado al cumplimiento de determinados objetivos de rendimiento".

No hi ha en l'ordenació jurídica comunitària una definició precisa del contracte de col·laboració públicoprivada que vinculi als Estats Membres quant a la seva regulació, ni si més no s'ha arribat a consens respecte a la seva verdadera denominació. La causa fonamental d'aquesta llacuna jurídica no és cap altra que l'enorme disparitat de fórmules associatives utilitzades pels esmentats països per enfrontar-se cada dia a la seva raó de ser, això és, en última instància, la creació de grans infraestructures, la provisió d'equipaments avançats i la prestació de serveis públics cada vegada més complexos.

En aquest mateix sentit s'ha pronunciat la pròpia Comissió Europea en dir que: "L'expressió «col·laboració públicoprivada» (CPP) manca de definició en l'àmbit comunitari. En general, es refereix a les diferents formes de cooperació entre les autoritats públiques i el món empresarial, l'objectiu del qual és garantir el finançament, construcció, renovació, gestió o el manteniment d'una infraestructura o la prestació d'un servei.

Amb l'aprovació de la Directiva 2004/18/CE del Parlament Europeu i del Consell, de 31 de març de 2004, sobre coordinació dels procediments d'adjudicació dels contractes públics d'obres, de subministrament i de serveis, es dóna definitivament cabuda en la normativa de contractació pública europea a la prolixa jurisprudència del TJCE dictada en la matèria.

No obstant això, l'aparició del CPP al nostre país no ha estat conseqüència directa de la transposició de l'esmentada Directiva, sinó més aviat de la voluntat del Govern espanyol manifestada a través de la Resolució d'1 d'abril de 2005, de la Subsecretaria del Ministeri de la Presidència, per la qual es disposa la publicació de l'Acord del Consell de Ministres, de 25 de febrer de 2005, pel qual s'adopten mandats per posar en marxa mesures d'impuls a la productivitat, el mandat de la qual estableix concretament: "El Ministeri d'Economia i Hisenda incorporarà en l'avantprojecte de Llei de Contractes del Sector Públic pel qual es traslladarà la Directiva 2004/18/CE, a més de les normes necessàries per a la completa i correcta transposició de la directiva al dret intern, una regulació dels contractes de col·laboració entre el sector públic i el privat... ".

Entorn dels elements fonamentals que configuren el CPP en general, podem dir que la pròpia Comissió Europea ha fet esforços per sintetitzar les quatre característiques que defineixen el mateix, a saber:

1. La durada relativament llarga de la relació, que implica la cooperació entre el soci públic i el privat en diferents aspectes del projecte que es realitzarà.

2. La manera de finançament del projecte, en part garantit pel sector privat, en ocasions a través d'una complexa organització entre diversos participants. No obstant això, el finançament privat pot completar-se amb finançament públic, que pot arribar a ser molt elevat.

3. L'important paper de l'operador econòmic, que participa en diferents etapes del projecte (disseny, realització, execució i finançament). El soci públic es concentra essencialment a definir els objectius que han d'assolir-se en matèria d'interès públic, qualitat dels serveis proposats i política de preus, mentre garanteix el control del compliment dels esmentats objectius.

4. El repartiment dels riscs entre el soci públic i el privat, al qual se li transfereixen aquells que habitualment suporta el sector públic. No obstant això, les operacions de CPP no impliquen necessàriament que el soci privat assumeixi tots els riscs derivats de l'operació, ni tan sols la major part d'ells. El repartiment precís dels mateixos es realitza cas per cas, en funció de les capacitats respectives de les parts en qüestió per avaluar-los, controlar-los i gestionar-los.

Si analitzem, d'altra banda, les característiques del nostre CPP, el CPP espanyol, a grans trets, compleix perfectament amb els quatre elements estructurals del mateix que ha fixat la Comissió Europea. Vegem, primer, no obstant això, quines són les característiques del CPP segons la LCSP. En aquest sentit, segons l'art. 11 de la mateixa, són contractes de col•laboració entre el sector públic i el sector privat aquells que una Administració Pública encarrega a una entitat de dret privat, per un període determinat en funció de la durada de l'amortització de les inversions o de les fórmules de finançament que es prevegin, la realització d'una actuació global i integrada que, a més del finançament d'inversions immaterials, d'obres o de subministraments necessaris per al compliment de determinats objectius de servei públic o relacionats amb actuacions d'interès general, comprengui alguna de les següents prestacions:

a. La construcció, instal·lació o transformació d'obres, equips, sistemes, i productes o béns complexos, així com el seu manteniment, actualització o renovació, la seva explotació o la seva gestió.

b. La gestió integral del manteniment d'instal•lacions complexes.

c. La fabricació de béns i la prestació de serveis que incorporin tecnologia específicament desenvolupada per tal d'aportar solucions més avançades i econòmicament més avantatjoses que les existents al mercat.

d. Altres prestacions de serveis lligades al desenvolupament per l'Administració del servei públic o actuació d'interès general que li hagi estat encomanat.

D'altra banda, continua l'art. 11 de la LCSP, només podran subscriure's contractes de col·laboració entre el sector públic i el sector privat quan prèviament s'hagi posat de manifest que altres fórmules alternatives de contractació no permeten la satisfacció de les finalitats públiques.

Finalment, segons el mateix art., la contraprestació a percebre pel contractista col•laborador consistirà en un preu que se satisfarà durant tota la durada del contracte, i que podrà estar vinculat al compliment de determinats objectius de rendiment.

Si observem ara, les quatre característiques del CPP segons la Comissió Europea abans enunciades, veurem que la LCSP dota pràcticament dels mateixos elements configuradors al CPP espanyol. En primer lloc, i en relació amb la durada relativament llarga de la relació entre el soci públic i el privat, veurem que, segons l'art. 290 de la mateixa, la durada dels contractes de col·laboració entre el sector públic i el sector privat no podrà excedir de 20 anys. No obstant això, quan per raó de la prestació principal que constitueix el seu objecte i de la seva configuració, el

règim aplicable sigui el propi dels contractes de concessió d'obra pública, s'estarà al disposat a l'article 244 sobre la durada d'aquests.

En segon lloc, i pel que respecta al finançament mixt dels projectes objecte del CPP, veiem que, si atenem al criteri d'absorció que la LCSP utilitza al seu art. 289 per regular les especialitats dels efectes, compliment i extinció del CPP, si el contracte que és en la base del CPP és una concessió d'obra pública, segons l'art. 236 de la LCSP, les obres públiques objecte de concessió seran finançades, total o parcialment pel concessionari, però quan existeixin raons de rendibilitat econòmica o social, o es presentin singulars exigències derivades del final públic o interès general de l'obra objecte de concessió l'Administració podrà també aportar recursos públics per al seu finançament. En el mateix sentit, si el contracte que sustenta al CPP és un contracte de gestió de serveis públics, l'art. 257.1 de la Llei estableix que el contractista té dret a les contraprestacions econòmiques previstes en aquest tipus de contracte, entre les quals s'inclourà, per fer efectiu el seu dret a l'explotació del servei, una retribució fixada en funció de la seva utilització que es percebrà directament dels usuaris o de la pròpia Administració

En tercer lloc, i en relació amb el paper principal que ocupa l'operador privat en l'esquema jurídicocontractual del CPP, hem de ser conscients que la seva participació, al marge de decisions estrictament polítiques, repercutirà favorablement en la gestió del projecte que es pretengui dur a terme. En aquest sentit, són multitud les variacions que podem trobar i que reflecteixen els diferents acords públic-privats que poden dur-se a terme i la combinació de les tasques en ells recollits. Les esmentades tasques són, fonamentalment: Design (dissenyar), Build (construir), Finance (finançar), Operate (gestionar), Own (posseir), Mantain (mantenir) i Transfer (transferir).

En qualsevol cas, és el caràcter subsidiari del propi CPP el que deixa entreveure la seva naturalesa instrumental. En aquest sentit, l'apartat 2 de l'esmentat art. 11 el deixa clar: només podran subscriure's contractes de col·laboració entre el sector públic i el sector privat quan prèviament s'hagi posat de manifest, en la forma prevista a l'article 134, que altres fórmules alternatives de contractació no permeten la satisfacció de les finalitats públiques.

D'altra banda, el propi TRLCSP estableix al seu art. 313 que els contractes de col·laboració entre el sector públic i el sector privat es regiran per les normes generals contingudes en el Títol I del Llibre IV i per les especials corresponents al contracte típic l'objecte del qual es correspongui amb la prestació principal d'aquell, en la qual cosa no s'oposin a la seva naturalesa, funcionalitat i contingut peculiar.

Pel que fa a l'avaluació prèvia, exigida per l'article 134 TRLCSP, s'ha d'acreditar, mitjançant l'aprovació per part de l'òrgan col·legiat constituït a l'efecte el document d'avaluació prèvia en què s'acredita que aquesta és la modalitat de contractació idònia, i constituir per part de l'òrgan de contractació la mesa especial de contractació.

Pel que fa als documents, descriptiu i el programa funcional, que han de utilitzar-se en les diferents fases a seguir, el seu contingut, s'adequa al que, amb caràcter general, integra un

expedient de contractació amb els plecs de clàusules administratives i les prescripcions tècniques que han de regir les fases del diàleg competitiu, amb les particularitats derivades del mateix i, en aquest sentit, el Document Descriptiu ha d'identificar la naturalesa de les necessitats a satisfer i establir els elements jurídics, tècnics i econòmics bàsics que conformen l'objecte de la licitació. Així mateix, ha de contenir la informació sobre el procediment de licitació i els models de formularis necessaris per a què els candidats presentin les seves sol•licituds de participació en la licitació.

Pel que fa al programa funcional, aquest ha d'especificar les necessitats tècniques, jurídiques i econòmiques del projecte, tal com està configurat inicialment.

Aquests dos documents han d'anar evolucionant durant el desenvolupament de l'etapa de diàleg amb els candidats que hagin estat seleccionats, als efectes d'adequar-se a la prestació a realitzar.

En aquest sentit, en la mesura de què existeixen elements econòmics, tècnics i financers que han de ser valorats i establerts prèviament, abans de la delimitació de l'objecte i posterior licitació i adjudicació (entre les empreses prèviament admeses al diàleg competitiu), sembla que aquesta fórmula seria la més idònia a l'hora de concretar quina modalitat de Cloud computing pot ser establerta per part de l'Administració i, fins i tot, compatibilitzar diferents tipologies de Cloud, en funció del servei al que ha d'atendre o les dades de què es tracti.

### 4.4. Contingut del contracte

El TRLCSP, quan regula els procediments de contractació de les administracions públiques espanyoles, dintre dels quals s'inclouen els contractes efectuats per a l'adquisició de serveis Cloud, configura els plecs de clàusules administratives i el contracte que signin l'Administració i el prestador de serveis com la base per la qual s'ha de regular la seva relació.

Ja hem indicat que els contractes que se subscriguin amb els proveïdors de serveis de Cloud Computing seran tipificats, com a regla general, com contractes de serveis, d'acord amb l'article 10 del TRLCSP, podent-se designar un responsable del contracte, com estableix l'article 52 del mateix Text refós. El procediment de contractació serà l'establert en el TRLCSP, que en la seva disposició addicional primera estableix certes particularitats relatives a la contractació a l'estranger, tant en relació amb l'òrgan competent quan es tracti de l'Administració General de l'Estat, com en relació amb les condicions de licitació, adjudicació, com als efectes que se'n derivin.

El contingut mínim que ha de tenir el contracte, així com altres condicions que ha de respectar el mateix, com les prohibicions de contractar i les restriccions d'aptitud, solvència, requisits de durada i altres circumstàncies aplicables, s'estableixen en la norma referida.

Encara que el TRLCSP articula un conjunt d'alternatives i instruments de contractació, els models de servei basats en Cloud Computing requereixen de més flexibilitat i dinamisme en la gestió de la demanda, i així els òrgans contractants han de preveure i instrumentalitzar aquestes alternatives per adaptar-les a aquesta tipologia de servei[21].

Aspectes com el pagament per ús o el dimensionament dinàmic de la demanda a través de contractes flexibles no tenen un encaix fàcil en el marc del TRLCSP, i aquesta situació està exigint a moltes administracions un exercici d'adaptació de plecs de contractació i de gestió del canvi amb les unitats de fiscalització i intervenció per trobar fórmules que permetin contractar i beneficiar-se dels avantatges i oportunitats del cloud al sector públic.

A més, existeixen procediments de contractació per a les administracions promoguts per la Llei de Contractes del sector públic, però no models que contemplin les particularitats que posseeix el cloud computing, ni escenaris pressupostaris per afavorir la col·laboració públicoprivada amb l'objecte d'un impuls del cloud.

Sobre aquesta base, les parts es troben sotmeses al principi de llibertat de pactes, sense perjudici de les limitacions a que es troben sotmeses les administracions públiques com a conseqüència de la seva actuació per raons d'interès general.

Així ho l'article 25 del TRLCSP:

"En los contratos del sector público podrán incluirse cualesquiera pactos, cláusulas y condiciones, siempre que no sean contrarios al interés público, al ordenamiento jurídico y a los principios de buena administración.

Sólo podrán fusionarse prestaciones correspondientes a diferentes contratos en un contrato mixto cuando esas prestaciones se encuentren directamente vinculadas entre sí y mantengan relaciones de complementariedad que exijan su consideración y tratamiento como una unidad funcional dirigida a la satisfacción de una determinada necesidad o a la consecución de un fin institucional propio del ente, organismo o entidad contratante".

D'acord amb el principi de llibertats de pactes, i una vegada acomplerts tots els requeriments que la contractació pública porta aparellada, cal procedir a la signatura del contracte, en què es recullen els elements bàsics de la prestació deguda, la majoria dels quals han estat ja definits als plecs de clàusules administratives (raó per la qual es signen i formen part íntegra del contracte).

L'article 26 del TRLCSP indica quin és el contingut mínim del contracte:

[21] L'estudi sobre el *Cloud computing* al sector públic espanyol publicat per INTECO, 2012: pp. 51-52

Salvo que ya se encuentren recogidas en los pliegos, los contratos que celebren los entes, organismos y entidades del sector público deben incluir, necesariamente, las siguientes menciones:

a.La identificación de las partes.

b.La acreditación de la capacidad de los firmantes para suscribir el contrato.

c.Definición del objeto del contrato.

d.Referencia a la legislación aplicable al contrato.

e.La enumeración de los documentos que integran el contrato. Si así se expresa en el contrato, esta enumeración podrá estar jerarquizada, ordenándose según el orden de prioridad acordado por las partes, en cuyo supuesto, y salvo caso de error manifiesto, el orden pactado se utilizará para determinar la prevalencia respectiva, en caso de que existan contradicciones entre diversos documentos.

f.El precio cierto, o el modo de determinarlo.

g.La duración del contrato o las fechas estimadas para el comienzo de su ejecución y para su finalización, así como la de la prórroga o prórrogas, si estuviesen previstas.

h.Las condiciones de recepción, entrega o admisión de las prestaciones.

i.Las condiciones de pago.

j.Los supuestos en que procede la resolución.

k.El crédito presupuestario o el programa o rúbrica contable con cargo al que se abonará el precio, en su caso.

l.La extensión objetiva y temporal del deber de confidencialidad que, en su caso, se imponga al contratista".

.

Per la seva part, l'apartat 2 de l'article 26.2 aclareix que "el documento contractual no podrá incluir estipulaciones que establezcan derechos y obligaciones para las partes distintos de los previstos en los pliegos, concretados, en su caso, en la forma que resulte de la proposición del adjudicatario, o de los precisados en el acto de adjudicación del contrato de acuerdo con lo actuado en el procedimiento, de no existir aquéllos".

En resum, la contractació dels serveis Cloud requereix una determinació molt clara dels aspectes que han d'integrar la prestació o servei que és objecte d'aquest. Aquesta determinació, quan parlem de les administracions públiques, no pot sinó encabir-se en una estratègia o planificació més ampla de configuració del servei, del programa d'implementació d'aquests, dels beneficis i costos que es poden derivar, i de les eficiències que s'han de derivar de la seva adopció.

Aquesta potestat planificadora, essencialment discrecional, suposa l'establiment d'un programa ö planificació que predeterminarà no tan sols la implementació del Cloud a les organitzacions públiques, sinó que també, arribat el cas, el contingut dels actes administratius emesos pels òrgans administratius, des de la vessant de garantia del compliment de tots els requeriments legalment exigibles als efectes de que l'exercici de potestats administratives sigui legalment

correcte, és a dir, s'adeqüi al marc legal aplicable, sense que el particular vegi malparades les seves garanties.

Finalment, cal tenir present que, aquesta potestat discrecional no deixa de tenir elements reglats. Aquesta diferència no és merament aparent, ja que mentre en les potestats discrecionals existeixen diferents possibilitats, totes igualment vàlides, en les potestats reglades existeix una única possibilitat, ja que la programació informàtica realitzada haurà de respondre de manera idèntica a totes les situacions en que concorrin els requisits jurídicament i tècnicament establerts.

No obstant això, hi ha altres elements que han de ser considerats a l'hora d'incorporar per part de l'Administració Pública els serveis o la informació al Cloud. Dins d'aquests elements a considerar es troba la seguretat de les aplicacions, així com les garanties d'interoperabilitat que, per manament de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, i el posterior desenvolupament reglamentari que s'ha dut a terme, són exigibles.

Així, el mateix estudi d'INTECO, 2012: p. 52, indica que el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica i el Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'interoperabilitat, són aplicables en matèria de seguretat i estàndards d'interoperabilitat en l'àmbit de les administracions públiques.

Ambdues normes recullen disposicions relatives als estàndards i procediments aplicables en matèria de seguretat i interoperabilitat en les administracions públiques, disposicions que els proveïdors de *Cloud computing* han de facilitar i, en molts casos, implementar i gestionar quan prestin serveis a organismes públics.

[...]

El marc d'assegurament de la informació proposat per ENISA l'any 2009 suggereix el següent llistat de qüestions legals a resoldre, amb caràcter general per a la provisió de serveis de *Cloud* (CATTEDDU i HOGBEN, 2009b: p. 24):

- A quin país està ubicat el proveïdor en núvol?
- Està situada la infraestructura del proveïdor en núvol al mateix país o en països diferents?
- Utilitzarà el proveïdor en núvol altres companyies la infraestructura estigui situada fora de la del proveïdor en núvol?
- On estaran ubicades físicament les dades?
- Es dividirà la jurisdicció dels termes contractuals i de les dades?
- Es subcontractarà algun dels serveis del proveïdor en núvol?
- Es contractarà externament algun dels serveis del proveïdor en núvol?

- Com es recolliran, processaran i transferir les dades proporcionades pel client i els clients del client?
- Què passa amb les dades que s'envien al proveïdor en núvol a la finalització del contracte?

El mateix estudi recomana avaluar, en el cas d'aprovisionament de serveis Cloud per a les Administracions Públiques, les següents qüestions (CATTEDDU i HOGBEN, 2009b: p. 11):

- Ofereix el proveïdor informació transparent i un control total sobre la ubicació física actual de totes les dades? Sovint, l'assegurament alt de les dades es veu restringit per la ubicació.
- Suporta el proveïdor el sistema de classificació de dades utilitzat?
- Quines garanties ofereix el proveïdor que els recurs del client estan totalment aïllats (és a dir, no es comparteixen màquines físiques)?
- Si s'assumeix que els clients no comparteixen màquines físiques, en quina mesura es suprimeix del tot l'emmagatzematge, la memòria i altres rastres de dades abans de reubicar les màquines?
- Suporta el proveïdor o fins i tot sol·licita l'autenticació de segon factor amb credencials físiques per l'accés del client?
- Posseeix el proveïdor la certificació ISO 27001/2? Quin és l'àmbit d'aplicació d'aquesta certificació?
- Els productes utilitzats pel proveïdor, estan subjectes a criteris comuns de certificació? A quin nivell? Quin perfil de protecció i objectiu de seguretat s'estableix per al producte?

[...]

D'acord amb l'informe sobre seguretat i resiliència en Cloud governamental publicat per l'Agència Europea de Seguretat de les Xarxes i de la Informació – ENISA l'any 2011, en el moment de preparació del plec seria recomanable plantejar-se les següents qüestions legals (CATTEDDU, 2011: p. 82):

- Pot garantir el compliment de requisits en la zona geogràfica de les dades?
- Si es rep una citació judicial d'obtenció de dades que entra en conflicte amb la jurisdicció local, quins són els mitjans per apel·lar?
- Diligència deguda en el compliment de la regulació. Per exemple: es fan algunes simulacions per verificar el compliment?
- Pot garantir l'accés a registres per demostrar qui ha accedit a quines dades i quan?
- Com garanteix la integritat i el no repudi de registres?
- Els termes proposats de servei expressen clarament qui és responsable de què parts de la política de seguretat i en quins casos?
- Com s'aplica el principi de rendició de comptes (*accountability*)?

- Suposeu que hi ha una clàusula de protecció de dades comercials a la legislació d'un Estat membre de la UE sobre la protecció de dades de ciutadans. A causa d'un incident amb un ciutadà estranger, s'obre una investigació. Les autoritats de l'altre país tindran accés a les dades?
- Com puc controlar el compliment del contracte? Com es mesura el control en temps real del compliment de l'acord de nivell de serveis (com per exemple, jitter, tolerància de càrrega, lliurament?

[...]

Des de la perspectiva del repartiment de les responsabilitats entre les parts contractuals, el marc d'assegurament de la informació proposat per ENISA l'any 2009 considera possible la següent divisió (CATTEDDU i HOGBEN, 2009b: pp. 7-8):

| | Client | Proveïdor de *Cloud* |
|---|---|---|
| Licitud del contingut | Responsabilitat total | Responsabilitat com a intermediari amb les limitacions de responsabilitat previstes a la Directiva 2000/31/CE i la seva interpretació |
| Incidents de seguretat | Responsabilitat per la diligència sobre els actius sota el seu control, d'acord amb les previsions contractuals | Responsabilitat per la diligència sobre els actius sota el seu control |
| Protecció de dades de caràcter personal | Responsable del tractament | Encarregat del tractament |

En resum, la configuració dels serveis al Cloud ha de poder donar resposta a totes aquestes qüestions de manera eficient i sense que, en cap cas, es produeixi cap perjudici o minva de garanties pel que fa als ciutadans, ni cap risc en el tractament de la informació es traslladi al Cloud.

## 5. Altres problemes a considerar.

La incorporació del Cloud en l'actuació administrativa planteja igualment altres problemes.

### 5.1.Problemes des del punt de vista del compliment de la normativa de la competència.

Una de les qüestions que és rellevant, i que ja hem avançat parcialment, són les restriccions a la lliure competència que es poden produir. Tot i que aquestes ho poden ser més des de la vessant de client captiu, cal tenir igualment present l'eventual existència de pràctiques restrictives de la

competència que poden produir-se, com a conseqüència de la posició dominant que determinats actors tenen (evidentment, ens estem referint preferentment al Cloud Públic).

Es pot fer esment del Dictamen del comitè econòmic i social de 26 d'octubre de 2011 "la computación en nube (cloud computing) en Europa", conforme al qual, al marge de les qüestions relatives a debilitats i avantatges del cloud, que es posen de manifest en apartats anteriors de l'estudi, són dos els riscos que s'han de destacar:

- la manca de governança en internet

Tot i això, existeixen empreses que gaudeixen d'una posició dominant (Microsoft i Apple pels equips individuals (ordinador, mòbil, ...) però també Google i Facebook (buscadors i xarxes socials).

Això posa de manifest la necessitat d'estar alerta davant eventuals riscos de posició dominant que es donessin en l'àmbit de la competència.

- la portabilitat

Aquesta és una qüestió que és rellevant no tan sols des de la vessant tècnica sinó també des de la comercial. Per aquesta raó, el Comitè Econòmic i Social recomana l'aplicació de normes obertes ("open standards") i garantir la interoperabilitat dels serveis i les aplicacions, als efectes de fer possible la transferència de dades d'un proveïdor a un altre, i que aquesta es produeixi de manera senzilla, ràpida i sense excessius costos pels usuaris.

### 5.2. Problemes en la pròpia prestació del servei

Tot i que l'Administració, en l'exercici de les seves activitats, gaudeix d'una sèrie de prerrogatives, per raó de la seva actuació en favor de l'interès general, l'exercici de les seves potestats i prerrogatives poden plantejar problemes, com a conseqüència de la deslocalització que el Cloud pot suposar.

Tot i que l'article 307 del TRLCSP indica, en relació amb el contracte de serveis, que "la Administración determinará si la prestación realizada por el contratista se ajusta a las prescripciones establecidas para su ejecución y cumplimiento, requiriendo, en su caso, la realización de las prestaciones contratadas y la subsanación de los defectos observados con ocasión de su recepción. Si los trabajos efectuados no se adecuan a la prestación contratada, como consecuencia de vicios o defectos imputables al contratista, podrá rechazar la misma quedando exento de la obligación de pago o teniendo derecho, en su caso, a la recuperación del precio satisfecho", la capacitat de control del desenvolupament de l'activitat planteja problemes.

PALOMAR OJEDA, A. op. Cit, exposa com a riscos que es poden plantejar, els següents:

1) Seguretat en la conservació de les dades per al compliment de les obligacions en l'àmbit administratiu

Es tracta de donar compliment a la normativa que, en matèria de conservació dels documents administratius, es trobin en suport paper o en suport electrònic, resulta aplicable. En resum, es tractaria de la normativa d'arxivística, que inclouria les previsions de l'Esquema Nacional d'Interoperabilitat

2) Disponibilitat en condicions d'ús i conservació

Es tracta de donar compliment a la normativa que, en matèria de procediment administratiu, té per objecte garantir a l'administrat el dret d'accés als procediments en que ostenta la condició d'interessat (en els supòsits en què aquest dret no es troba restringit), així com la política de protecció de dades de caràcter personal.

### 5.3. Problemes en l'exercici de la competència per part de l'òrgan administratiu

Tot i que en seu del contracte de serveis, l'article 301 del TRLCSP indica que "No podrán ser objeto de estos contratos los servicios que impliquen ejercicio de la autoridad inherente a los poderes públicos".

Aquesta previsió no és obstacle per la prestació de serveis mitjançant el Cloud, ja que aquest últim seria únicament l'instrument material per a la prestació del servei però, en cap cas, ha de suposar el traspàs de la competència per part de l'òrgan administratiu responsable, sota el paràmetre de què la competència és irrenunciable i s'exercirà per part de l'òrgan que la té legalment atribuïda.

Això ens porta igualment a l'anàlisi del concepte de potestat administrativa. El concepte de potestat fou elaborat en contrast amb el concepte de dret subjectiu, dins de la categoria genèrica dels poders jurídics o facultats d'obrar, atribuïdes per l'ordenament jurídic als subjectes, en ordre a interessos o béns per ell protegits.

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 sotmetiment d'altres subjectes als eventuals efectes jurídics derivats de l'exercici de la potestat.

5) I no s'atribueixen en benefici del seu titular, sinó de terceres persones, ja que l'Administració ha d'exercitar les seves potestats per a perseguir l'interès públic. Per aquest motiu, les potestats administratives són potestats-funció, la qual cosa exclou poders absoluts.

Així, seguint a GARRIDO FALLA, la potestat administrativa pot definir-se com un poder d'actuació genèric que, exercitant-se d'acord amb les normes jurídiques, produeix situacions jurídiques en què quedaran obligats subjectes que, amb anterioritat, estaven simplement en una situació abstracta de sotmissió.

En qualsevol cas, per tal que l'Administració pugui exercitar qualsevol potestat és precís:

1) Que prèviament li hagi estat atribuïda per llei.

2) Amb caràcter exprés.

3) I específic.

No obstant, l'exigència de caràcter exprés ha de ser matisada amb la doctrina dels poders implícits o inherents del dret anglosaxó, conforme a la qual, encara que no s'otorguin expressament per la llei, han d'entendre's atribuïts aquells poders que siguin implicació necessària dels expressament atorgats.

Pel que fa al principi de legalitat, com a pilar fonamental de l'Estat de Dret, es caracteritza no només pel reconeixement i tutela dels drets públics subjectius dels ciutadans, sinó també per la forma en què aquest objectiu s'assoleix: mitjançant el sotmetiment de l'Administració a la llei, que constitueix el principi de legalitat, i que es formulà inicialment concebent a la llei com a font i justificació de totes les actuacions dels poders executiu i judicial.

La inicial formulació del principi de legalitat construïda en torn a l'exigència de la llei prèvia, partia de dues clares justificacions:

1) En primer lloc, una de general, basada en la idea roussoniana de que la legitimitat del poder procedeix de la voluntat comunitària quina expressió típica 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[22], el legislador no és plenament lliure a l'hora de decidir el grau de predeterminació amb el que té que utilitzar les potestat administratives, ja que es requereix una densitat normativa mínima que, en determinades matèries, està reservada a la llei. Això es produeix ja que el legislador no pot deixar totalment obertes les seves decisions per tal que siguin completades o concretades per l'Administració, ja que això suposaria el trencament de la reserva de llei, que exigeix que la llei reguli amb suficient densitat les qüestions principals que suscita la matèria reservada.

[22] Muñoz Machado, S. "Tratado de derecho administrativo y derecho público General I". Ed. Iustel 2ª Edición 2006. Pàg. 519

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

No obstant això, cal tenir present que, en l'àmbit del Cloud, l'existència d'una regulació normativa com a requisit previ per a la seva implementació no sembla necessari, com a conseqüència de la flexibilització dels requisits que, en matèria d'aprovació de programes i aplicacions, ha suposat la Llei 11/2007, al marge dels silencis que aquest canvi normatiu ha suposat.

Com a plantejament previ, la Llei 11/2007 va derogar determinats preceptes de la Llei 30/1992, entre ells l'article 45.4, que deia: "Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características".

No obstant això, la Llei 11/2007 no indica si, a partir d'aquesta derogació, s'ha fet innecessària l'aprovació i publicació dels programes. Tan sols es tracta la qüestió a l'article 39 relatiu a l'actuació administrativa automatitzada, conforme al qual hi haurà un òrgan regulador "...para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación."

Això suposaria que, al marge del que es pugui entendre amb caràcter general en l'ambit dels procediments administratius tramitats electrònicament, en l'àmbit de l'actuació administrativa automatitzada no s'ha eliminat l'obligació d'aprovació, sense perjudici de que siguin els òrgans corresponents els que regulin el sistema d'aprovació i difusió dels programes i aplicacions utilitzats en cada cas.

En qualsevol cas, es tractaria d'una qüestió lligada a la potestat autoorganitzativa de cadascuna de les Administracions.

Aquesta aprovació, evidentment, 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.

Cal tenir present que autors com VALERO TORRIJOS, J., fan esment de la defectuosa tècnica legislativa emprada per la Llei 11/2007 en relació a la derogació de l'aprovació dels programes i aplicacions. D'altra banda, indiquen que, al marge de la naturalesa jurídica de l'aprovació dels programes i aplicacions, es tracta d'un requisit essencial per assegurar la plena subjecció a la llei i al Dret de les aplicacions i els serveis de l'administració electrònica des de una perspectiva material, de 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 suposi renunciar a l'ús de les noves tecnologies.

No obstant això, l'aprovació dels programes i 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 disposa: "Los actos de las Administraciones Públicas sujetos al Derecho Administrativo serán ejecutivos con arreglo a lo dispuesto en esta Ley". L'article 57, d'altra banda, continua dient: "Los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa".

Tot i el silenci de la Llei 11/2007, sembla evident que sempre haurà d'existir un acte administratiu, on el funcionari competent prengui la decisió de posar en producció un determinat programa o aplicatiu, als efectes de que pugui ser utilitzat per part dels administrats mitjançant l'accés al tràmit o servei de que es tracti a la seu electrònica corresponent. Evidentment, la qüestió serà que aquest funcionari ha d'estar habilitat a l'efecte, és a dir, facultat per raó de la seva competència per dur a terme aquesta aprovació.

# 6 Glossari

*CLOUD* COMUNITARI(NIST SP 800-145): Model de desplegament en que la infraestructura *Cloud* es aprovisionada per a l'ús exclusiu per part d'una comunitat específica de consumidors d'organitzacions que tenen preocupacions comunes (per exemple, missió, requeriments de seguretat, polítiques o consideracions de compliment normatiu). Pot ser adquirida, gestionada i operada per una o més de les organitzacions de la comunitat, per una tercera part, o una combinació dels dos anteriors, i pot existir o no a les pròpies instal·lacions.

*CLOUD* PÚBLIC (NIST SP 800-145): Model de desplegament en que la infraestructura *Cloud* es aprovisionada per a l'ús obert pel públic en general. Pot ser adquirida, gestionada i operada per una organització mercantil, acadèmica o governamental, o alguna combinació de les anteriors. Existeix a les instal·lacions del proveïdor de Cloud.

*CLOUD* PRIVAT(NIST SP 800-145): Model de desplegament en que la infraestructura *Cloud* es aprovisionada per a l'ús exclusiu per part d'una única organització que compren múltiples consumidors (per exemple, unitats de negoci). Pot ser adquirida, gestionada i operada per l'organització, per una tercera part, o una combinació dels dos anteriors, i pot existir o no a les pròpies instal·lacions.

*CLOUD* HÍBRID(NIST SP 800-145): Model de desplegament en que la infraestructura *Cloud* és una composició de dues o més infraestructures Cloud diferents (privada, comunitària o pública) que romanen entitats unívoques, però que es troben vinculades per tecnologia estàndard o propietària que permet la portabilitat de les dades i aplicacions.

*INFRASTRUCTURE AS A SERVICE – IAAS* (NIST SP 800-145): Model de servei *Cloud*en el qual la capacitat proveïda al consumidor és aprovisionar processament, emmagatzematge, xarxes i altres recursos fonamentals de computació on el consumidor es capaç de desplegar i executar programari arbitrari, incloent-hi sistemes operatius i aplicacions.

INFRAESTRUCTURA DE *CLOUD* (NIST SP 800-145): La col·lecció de maquinari i programari que habilita les cinc característiques essencials del *Cloud computing*. La infraestructura de *Cloud* es pot veure com formada per una capa física i una capa d'abstracció. La capa física consisteix en els recursos de maquinari necessaris per suportar els serveis *Cloud* proveïts, i típicament inclou components de xarxa, d'emmagatzematge i servidors. La capa d'abstracció consisteix en el programari desplegat a través de la capa física, que manifesta les característiques essencials de *Cloud*. Conceptualment la capa d'abstracció es troba a sobre de la capa física.

*PLATFORM AS A SERVICE – PAAS* (NIST SP 800-145): Model de servei *Cloud*en el qual la capacitat proveïda al consumidor és desplegar sobre la infraestructura *Cloud* aplicacions creades o adquirides pel consumidor emprant llenguatges de programació, llibreries, serveis i eines suportades pel proveïdor.

*SOFTWARE AS A SERVICE – SAAS* (NIST SP 800-145): Model de servei *Cloud*en el qual la capacitat proveïda al consumidor és emprar les aplicacions del proveïdor executades sobre una infraestructura *Cloud*. Les aplicacions són accessibles des de diversos dispositius client indistintament a través d'una interfície de client lleuger, com un navegador web (per exemple, correu electrònic basat en web), o d'una interfície de programa.

# 7 Bibliografia

ALAMILLO DOMINGO, Ignacio (2012), "El control de localización de los datos e informaciones en el Cloud", a MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y Cloud Computing*, Civitas, 2012.

ÁLVAREZ RIGAUDIAS, Cecilia (2012), "Condiciones para las transferències Internacionales de datos personales en Servicios de cloud", a MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y Cloud Computing*, Civitas, 2012.

AREA, Eduardo (2010), "¿Qué es el *Cloudbursting*?", 10 de agosto de 2010, http://eduardoarea.blogspot.com.es/2011/08/que-es-el-cloud-bursting.html (disponible el 22/08/2012).

ARMBURST, Michael; FOX, Armando; GRIFFITH, Rean; JOSEPH, Anthony D.; KATZ, Randy; KONWINSKI, Andy; LEE, Gunho; PATTERSON, David; RABKIN, Ariel; STOICA, Ion; i ZAHARIA, Matei, (2009), *Above the Clouds: A Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley, February 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html (disponible el 23/08/2012).

BALBONI, Paolo (2010), *Data Protection and Data Security Issues Related to Cloud Computing in the EU*, Legal Studies Working Papers, n. 022/2010, Tilburg University, August 2010.

BANKINTER (2010). *Cloud Computing. La tercera ola de las Tecnologías de la Información*. Fundación de la Innovación Bankinter, http://www.fundacionbankinter.org/es/publications/cloud-computing (disponible el 23/08/2012).

BOWEN, Janine Anthony (2011), *Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations*, The Computer & Internet Lawyer, Volume 28, Number 8, August 2011.

CATTEDDU, Daniele i HOGBEN, Giles (2009a), *Computación en Nube: Beneficios, riesgos y recomendaciones para la seguridad de la información*, European Network and Information Security Agency (ENISA), Noviembre 2009, http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view (disponible el 23/08/2012).

- (2009b) *Cloud computing: Information Assurance Framework*, November 2009, http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework (disponible el 23/08/2012).

CATTEDDU, Daniele (2011), *Security and Resilience in Governmental Clouds: Making an informed decision*, January 2011, http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds (disponible el 23/08/2012).

CLASSEN, H. Ward i FOGARTY, Marie (2012), *Avoiding Turbulence in the Cloud: Licensing and Contractual Issues for Licensors, Cloud Providers and End Users*, The Computer & Internet Lawyer, Volume 29, Number 2, February 2012.

CSA (2011), *Cloud Security Alliance*. *Security as a Service Working Group*, https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/ (disponible el 23/08/2012).

CSA-ES (2011), *Capítulo español de Cloud Security Alliance. Cloud Compliance Report*, http://www.cloudsecurityalliance.es/noticias (disponible el 23/08/2012).

DE MIGUEL ASENSIO, Pedro A. (2001), *Derecho privado de Internet*, 2ª ed, Civitas, 2001.

DETERMANN, Lothar (2011), *Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations*, The Computer & Internet Lawyer, Volume 28, Number 11, November 2011.

ECHEVERRÍA, Víctor; LIEBROCK, Lorie M.; i SHIN, Donwang (2010), "Permission management system: Permission as a service in cloud computing", en *Proceedings - International Computer Software and Applications Conference*, art. no. 5615248, pp. 371-375.

EUROPEAN COMMISSION (2010). *The Future of Cloud Computing. Opportunities for European Cloud Computing Beyond 2010*, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (disponible el 23/08/2012).

FIELDER, Anna; BROWN, Ian; ALLEWELDT, Frank; KARA, Senda; WEBER, Verena; i MCSPEDDEN-BROWN, Nicholas (2012), *Cloud computing – Study*, Directorate general for internal policies, Policy department A: Economic and Scientific policy, European Parlament, May 2012, http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=73411 (disponible el 23/08/2012).

FOSTER, Ian; ZHAO, Yong; RAICU, Ioan; i LU, Shiyong (2008), "Cloud Computing and Grid Computing 360-Degree Compared", *Grid Computing EnvironmentsWorkshop, GCE '08*, art. no. 4738445, IEEE, 2008.

GARCÍA SÁNCHEZ, Manuel (2012), "Retos de la computación en nube", a MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y Cloud Computing*, Civitas, 2012.

GERVAIS, Daniel J. i HYNDMAN, Daniel J. (2012), "Cloud control: Copyright, Global Memes and Privacy", *Journal on Telecommunications & High Technology Law*, 53, Winter 2012.

GILBERT, Françoise (2010), "Cloud service contracts may be fluffy: Selected legal issues to consider before taking off", *Journal of Internet Law*, Volume 14, Number 6, December 2010.

- (2011), "Cloud service providers as joint-data controllers", *Journal of Internet Law*, Volume 15, Number 2, August 2011.
- (2012), "Proposed EU Data protection regulation: The good, the bad, and the unknown", *Journal of Internet Law*, Volume 15, Number 10, April 2012.

GOLD, Joshua (2012), "Protection in the cloud: Risk management and Insurance for cloud computing", *Journal of Internet Law*, Volume 15, Number 12, June 2012.

GLOTT, Rüdiger; HUSMANN, Elmar; SADEGHI, Ahmad-Reda; i SCHUNTER, Matthias (2011), "Trustworthy clouds underpinning the future Internet", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, LNCS 6656, pp. 209-221.

GRANDISON, Tyrone; MAXIMILIEN, E. Michael; THORPE, Sean; i ALBA, Alfredo (2010), "Towards a formal definition of a computing cloud", *2010 IEEE 6th World Congress on Services*, art. no. 5575825, IEEE, 2010, pp. 191-192.

GROSSMAN, Robert L. (2009), "*The case for cloud computing*", IT Professional 11 (2), art. no. 4804045, 2009, pp. 23-27.

HAY, Brian; NANCE, Kara; i BISHOP, Matt (2011), "Storm clouds rising: Security challenges for IaaS cloud computing", *Proceedings of the Annual Hawaii International Conference on System Sciences*, art. no. 5719003.

HON, W. Kuan; MILLARD, Christopher i WALDEN, Ian (2011), *Who is responsible for 'personal data' in cloud compunting?. The cloud of unknowing, part 2*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011, March 2011, updated April 2012.

INTECO (2011), *Riesgos y amenazas en Cloud computing*, Marzo 2011, http://www.inteco.es/Seguridad/Observatorio/Estudios/ (disponible el 23/08/2012).

- (2012) *Estudio sobre Cloud computing en el sector público en España*, Julio 2012, http://www.inteco.es/Seguridad/Observatorio/Estudios/ (disponible el 23/08/2012).

ITANI, Wassim; KAYSSI, Aymann; i CHEHAB, Ali (2009), "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures", *8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009*, art. no. 5380584, pp. 711-716.

JAEGER, Paul T.; LIN, Jimmy; GRIMES, Justin M. i SIMMONS, Shannon N. (2009), "Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing", *First Monday* 14 (5).

JANSEN, Wayne A. (2011), "Cloud hooks: Security and privacy issues in cloud computing", *Proceedings of the Annual Hawaii International Conference on System Sciences*, art. no. 5719001.

NELSON, Michael R. (2009), "The cloud, the crowd, and public policy", *Issues in Science and Technology* 25 (4), pp. 71-76.

NG, Wesley i CARRUTHERS, Stuart S. (2012), "Canada: cloud computing and Canadian federally regulated financial institutions", *Journal of International Banking Law and Regulation*, 27(3), N57-60.

MELL, Peter i GRANCE, Timothy (2011), *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*. Specia lPublication 800-145, National Institute of Standards and Technology. September 2011,http://www.nist.gov/itl/cloud/ (disponible el 22/08/2012).

MILLER, Rich (2006), "Sun Unveils Data Center In A Box'", http://www.datacenterknowledge.com/ (disponible el 23/08/2012).

MOHAMMED, Derek (2011), "Security in cloud computing: An analysis of key drivers and constraints", en *Information Security Journal* 20 (3), pp. 123-127.

MOLES PLAZA, Ramon J. (2004), Derecho y control en Internet. La regulabilidad de Internet, Ariel Derecho, 2004.

MUÑOZ MACHADO, Santiago (2000), La regulación de la Red. Poder y Derecho en Internet, Taurus, 2000.

ONTSI (2012), *Cloud computing. Riesgos y oportunidades*. Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, Mayo 2012.

PEARSON, Siani i BENAMEUR, Azzedine (2010), "Privacy, securityand trust issues arising from cloud computing", *Proceedings – 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, art. no. 5708519, IEEE, 2010, pp. 693-702.

RUBÍ NAVARRETE, Jesús (2012), "El proveedor de Cloud como encargado del tratamiento", a MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y Cloud Computing*, Civitas, 2012.

SCHOO, Peter; FUSENIG, Volker; SOUZA, Victor; MELO, Márcio; MURRAY, Paul; DEBAR, Hervé; MEDHIOUB, Houssem; i ZEGHLACHE, Djamal (2012), "Challenges for Cloud Networking Security", *2nd International ICST Conference on Mobile Networks and Management*, Springer, 2010.

SANCHO VILLA, Diana (2010), *Negocios Internacionales de tratamiento de datos personales*, Civitas Thomson Reuters, 2010.

SLAWSKI, Bill (2009), "Search on the Seas: Google Water-Based Data Center Patent Granted", *SEO by the Sea*, http://www.seobythesea.com/?p=1357 (disponible el 23/08/2012).

VALERO TORRIJOS, Julián (2012), "La Administración frente al Cloud. Especial consideración de la administraciónelectrónica", a MARTÍNEZ MARTÍNEZ, Ricard (coord.), *Derecho y Cloud Computing*, Civitas, 2012.

VAQUERO, Luis M.; RODERO-MERINO, Luis; CÁCERES, Juan; i LINDNER, Mark (2009), "A Break in the Clouds: Towards a Cloud Definition", *ACM SIGCOMM Computer Communication Review*,Volume 39, Number 1, January 2009.

YOO, Christopher S. (2011), "Cloud Computing: Architectural and Policy Implications", *Review of Industrial Organization* 38, 2011, pp. 405-421.