

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

RESUM

Es pot definir 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

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.

Pel que fa a les característiques essencials d'aquest model computacional, són les següents:

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, tabletas, 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.

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. Igualment podem parlar del Cloud de xarxa, on es proveeixen serveis de xarxa virtualitzats; models que plantegen capacitats i restriccions de seguretat diferents, per exemple en relació amb la confidencialitat de les dades.

Pel que fa als models de servei del Cloud computing, es poden identificar els tres següents:

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.

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.

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).

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.

Finalment, des de la perspectiva del desplegament dels serveis *Cloud*, s'identifiquen els següents quatre models:

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.
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.
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*.
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 úniques, però que es troben vinculades per tecnologia estàndard o propietària que permet la portabilitat de les dades i aplicacions (per exemple, el *Cloud bursting* per al balanceig de càrrega entre Clouds).

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.

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 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.

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; d'altra banda, els usuaris poden accedir a uns serveis amb un alt grau d'eficiència amb un cost assumible.

En aquest sentit, 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 esmoreir si les administracions aposten pels models de *Cloud computing*.

Aquest model permet implementar 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.

Fruit de l'anàlisi 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.

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).

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.

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. Mentre que el primer nivell està configurat per la decisió administrativa, de caràcter discrecional, d'incorporar els serveis *Cloud* a les

estructures administratives, atenent als evidents beneficis que se'n deriven de la seva implementació; el segon nivell es configuraria per l'establiment d'un marc jurídic que donés plena garantia jurídica a les actuacions administratives que es duuguin 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.

Per raó dels beneficis que es deriven del *Cloud computing*, el projecte de recerca ha analitzat les diferents tipologies del *Cloud* i, d'acord amb la doctrina desenvolupada en la matèria, s'ha dut a terme una anàlisi de les debilitats, amenaces, forteses i oportunitats que se'n deriven de cadascun d'aquests.

Aquesta tasca d'anàlisi, basat en l'experiència, ha de permetre avaluar, a l'hora de prendre la decisió del tipus de *Cloud Computing* que es vulgui adoptar, quina opció permetria atendre, en més gran mesura, les necessitats, requeriments i altres condicionants que, en l'exercici de les seves actuacions i presa de decisions, correspon complir a les administracions públiques.

No obstant això, aquesta incorporació del *Cloud computing* per part de l'Administració no deixa de suposar riscos. Per aquesta raó, s'han analitzat i detectat una sèrie de riscos que es poden produir,

En primer lloc, cal tenir present els riscos derivats de la deslocalització pròpia del *Cloud computing*. En la mesura de què Internet és universal, es fa difícil, d'entrada, ubicar els serveis del *Cloud* en un determinat espai físic. Això planteja la dificultat d'aplicar les normes jurídiques, típicament territorials, a l'espai de la xarxa.

Aquesta deslocalització plantejarà problemes de jurisdicció, que s'hauran de solucionar mitjançant la incorporació dels criteris de submissió a la jurisdicció aplicable que siguin exigibles i, com a regla general, incorporar la submissió a la jurisdicció espanyola. En qualsevol cas, el model de *Cloud* pel qual s'opti determinarà un grau inferior o superior de complexitat en l'adaptació dels requeriments particulars.

Mentre que en el *Cloud* públic la singularització del posicionament de l'Administració Pública resulta molt complicat, en els altres models, especialment en el *Cloud* privat, aquesta possibilitat seria molt més factible, com a conseqüència de que l'òrgan de contractació té una facultat decisòria molt més amplia a l'hora de delimitar l'objecte del

contracte i les particularitats que s'han de seguir en el seu desenvolupament i execució.

Un altre dels aspectes de gran rellevància és el referent a la protecció de dades de caràcter personal, pel que fa a l'aplicació de la normativa vigent, en relació amb el responsable i l'encarregat del tractament de les dades que siguin objecte del servei de Cloud, amb les mesures que s'han d'adoptar (en particular, les mesures de seguretat corresponent), així com la problemàtica que es pot derivar quan, atenent a la deslocalització, es produeixi una transferència internacional de dades.

Igualment, s'han analitzat els riscos de confidencialitat i propietat intel·lectual. En aquest camp, ens tornem a trobar amb els problemes que la deslocalització i la manca de control de les infraestructures d'emmagatzematge poden suposar.

Així, si ens trobem davant de dades governamentals que 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 especialment sensibles. 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 .

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 rescabament) 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.

Un altre dels riscos és el que es deriva dels problemes que es poden derivar per a l'assoliment d'una determinada certificació de qualitat. Així, la inversió en l'obtenció d'una determinada 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.

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.

Igualment, podem fer esment dels riscos que poden existir de creació d'una situació de client captiu. Així, la possible dependència d'un proveïdor, per exemple per manca d'estandardització o d'interoperabilitat, suposa un risc de captivitat important per als usuaris.

En aquests casos, es tracta de trobar solucions de caràcter preventiu, amb una contractació originària que impedeixi o redueixi al mínim els problemes que es puguin derivar en el cas de migració.

No obstant això, com a conclusió reiterada al llarg d'aquesta recerca, el marge de maniobra de que disposa l'administració és molt més reduït quan ens trobem davant d'un Cloud Públic, que no pas quan ens trobem davant d'altres models de Cloud, en que les facultats de control per part de l'Administració Pública és molt més gran.

D'altra banda, és evident el risc que es deriva de la negligència professional, per part del prestador del servei, que pot impactar en els usuaris.

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). Aquesta pèrdua econòmica per part de l'administració pública pot produir-se de manera directa i immediata, o per la via de rescabament 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).

Als efectes de fer front aquestes situacions, és important preveure o incloure en la contractació, clàusules de responsabilitat i indemnització en els acords de nivell de servei (ANS), els quals han d'exercir un paper fonamental en aquest àmbit.

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 alegar 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.

Cal tenir igualment presents els riscos derivats de l'eventual subcontractació de serveis i els canvis de control sobre els prestadors de serveis de Cloud computing.

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, arribat el cas, 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.

Finalment, podem fer esment dels riscos derivats del llicenciamnt. Així, 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

Això suposa la necessària adaptació 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 en lloc 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 dels seus serveis.

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.

Amb caràcter general, 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.

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.

Pel que fa a les Administracions Públiques, es recomana 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.

Per aquesta raó, 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 propers anys.

Així, si els organismes públics adopten la computació en el núvol, han de definir els requisits que han de ser objecte de compliment o salvaguarda 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.

En aquesta línia, han de definir nivells acceptables de servei i 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.

Finalment, han d'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 i establir un marc de mesura

(incloent indicadors principals d'objectius i rendiment) per avaluar contínuament si es compleix les condicions preestablertes.

D'altra banda, en l'exercici de les seves potestats autoorganitzatives, 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: 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; i assegurar el compliment de la normativa legal específica.

Finalment, pel que fa a l'adquisició de serveis Cloud per part de les Administracions Públiques, aquesta es troba sotmesa, per raons òbvies, a les regles aplicables per a l'adquisició de béns o serveis per part de les administracions públiques. Resulten aplicables, per tant, per a l'adquisició de serveis Cloud per l'Administració, 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).

A partir de la submissió a aquesta normativa, l'adquisició d'una prestació o servei per part de l'administració requereix la corresponent tramitació de l'expedient, que l'inicia l'òrgan de contractació motivant la necessitat del contracte.

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. Per aquesta raó, hauran de reflectir els condicionants econòmics i tècnics que permetin que l'Administració esculli la proposició econòmicament més avantatjosa, en els termes definits a la normativa de contractes.

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 concloure 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.

Aplicant la normativa de contractes, serà essencial determinar els criteris de classificació i solvència, així com delimitar acuradament l'objecte i preu del contracte.

Des del punt de vista de la contractació pública, és igualment rellevant definir la tipologia del contracte. En aquesta matèria, s'ha analitzat si ens trobem davant d'un contracte de serveis o de subministrament, per concloure que, en funció del que sigui objecte de contractació, ens trobarem més en línia amb una de les dues modalitats, diferenciant si es tracta de l'adquisició d'una simple capacitat d'emmagatzematge en un entorn de Cloud públic (contracte de subministrament) o, pel contrari, ens trobarem en la majoria o la resta dels casos davant d'un contracte de serveis (o en la modalitat d'un contracte mixt, tal com s'analitza).

El projecte de recerca analitza igualment el contracte de col·laboració publicoprivada, per concloure que és la forma més adequada per a l'adquisició d'aquest servei per part de les grans organitzacions públiques, atenent als múltiples factors que entren en joc. Així, 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.

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.

Finalment, s'analitza 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 .

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.

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.

Finalment, l'estudi fa un breu anàlisi d'altres problemes que es poden derivar en la implementació del Cloud: tant des del punt de vista de la normativa de competència, problemes en la pròpia prestació del servei, i en l'exercici de la competència per part de l'òrgan administratiu.

En resum, l'estudi ha dut a terme una anàlisi del Cloud Computing des de la vessant conceptual i pràctica, delimitant les diferents tipologies existents i els beneficis i riscos que se'n deriven de cadascun d'ells, als efectes d'aportar els elements de judici suficients per optar per una determinada modalitat de prestació del servei. A partir d'aquesta delimitació, i atenent a una adequada planificació, és quan es pot procedir a l'adquisició o configuració dels serveis emprant el Cloud, els quals s'han d'adequar a les previsions de la normativa de contractes del sector públic.

Barcelona, 8 de setembre de 2012