IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monogràfic «VI Congrés Internet, Dret i Política. *Cloud Computing*: El Dret i la Política Pugen al Núvol»

ARTICLE

Informàtica en núvol i protecció de dades

Ramón Miralles

Data de presentació: octubre de 2010
Data d'acceptació: octubre de 2010
Data de publicació: desembre de 2010

Resumen
La informàtica en núvol (*cloud computing*) és una arquitectura de prestació o aprovisionament de serveis de tecnologies de la informació i la comunicació que està agafant força protagonisme, i que segons els analistes en els propers anys es consolidarà tant pel que fa als usuaris individuals de la Xarxa i de serveis en línia, com a les empreses, que afectarà la seva manera d'utilitzar les TIC.
En relació amb els usuaris de la Xarxa, la informàtica en núvol té molts punts de connexió amb el Web 2.0, i en relació amb les empreses, està estretament lligada als processos d'externalització (o *outsourcing*) dels serveis TIC.
En aquest article s'identifiquen i analitzen les qüestions més rellevants del binomi informàtica en núvol i protecció de dades de caràcter personal.

Palabras clave
cloud computing, protecció de dades, llibertats, privacitat, informàtica en núvol, encarregat tractament, transferències internacionals

Tema
Dret fonamental, protecció de dades, societat de la informació

Cloud computing and data protection

Abstract
Cloud computing is an architecture for carrying out and/or providing services for information and communication technologies which is playing an increasingly prominent role. According to analysts, among companies and individual users of the Internet and online services, its application will be consolidated over the next few years.
In relation to Internet users, cloud computing has many connections with the web 2.0, and for companies it is closely linked to outsourcing of ICT services.
This article identifies and analyses the major questions regarding binomial cloud computing and private data protection.

Keywords
cloud computing, data protection, freedom, privacy, data processing requests, international transferences

Topic
Basic rights, Data protection, Information society

La informàtica en núvol o *cloud computing* és una arquitectura de prestació o aprovisionament de serveis de tecnologies de la informació i la comunicació, que en els últims dos anys està agafant força protagonisme. Segons els analistes, en els propers anys es consolidarà tant pel que fa als usuaris individuals de la Xarxa i serveis en línia com a les empreses, i en tots dos casos afectarà la seva manera d'utilitzar les tecnologies de la informació i la comunicació (TIC).

En relació amb els usuaris de la Xarxa, la informàtica en núvol té molts punts de connexió amb el Web 2.0 i, per a les empreses, està estretament lligada als processos d'externalització dels serveis TIC.

El meu primer contacte professional amb el concepte d'*informàtica en núvol* va ser mitjançant un document, de maig del 2008, concretament un llibre blanc o *white paper* de l'oficina del Comissionat d'Informació i Privacitat d'Ontàrio (Canadà), que porta el títol de «Privacy in the clouds».[1]

El document en si mateix no aporta, en aquests moments, una reflexió rellevant quant a la protecció de dades personals i la informàtica en núvol, ja que té un caràcter molt introductori i es dedica fonamentalment a la identitat digital a Internet. Per tant, no aborda en profunditat ni de forma àmplia la privacitat en relació amb la informàtica en núvol, però a mi em va servir per a prendre contacte amb aquest nou concepte.

Hi ha un altre document, també de l'IPC d'Ontàrio, que sí que aborda amb més profunditat la qüestió de la privacitat i la informàtica en núvol. Porta el títol de «Modeling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach» i es va publicar el maig del 2010; tots dos es poden baixar al lloc web de l'IPC.

En el que sí que posa èmfasi el primer dels documents a què he fet referència, a la seva introducció, és al fet que l'autodeterminació informativa és un concepte que ha de ser promogut i protegit en un context en què hi ha importants quantitats d'informació de caràcter personal (el document parla de quantitats «il·limitades») que passen dels individus a les organitzacions, i d'aquestes a altres organitzacions. I jo hi afegiria que aquesta característica d'il·limitada no fa referència exclusivament a la quantitat d'informació, sinó també al tipus i als formats de la informació.

Després tornaré a referir-me a l'autodeterminació informativa, que com veurem es veu especialment afectada per les característiques de processament de la informació de la informàtica en núvol.

Ara voldria continuar, en clau introductòria, amb una breu referència a l'origen de la informàtica en núvol. Des de l'òptica de les telecomunicacions, s'entén per *cloud* o *núvol* el conjunt de dispositius i infraestructures de comunicacions pels quals, de manera «impredictible», passa la informació quan es vol transmetre d'un punt a l'altre de la xarxa Internet. Aquesta falta de predicció afecta tant el nombre de dispositius com el tipus; de fet, tots els elements que es troben al mig d'aquest intercanvi d'informacions s'han representat gràficament, tradicionalment, per un «núvol».

1. La comissària d'Informació i Privacitat d'Ontàrio (IPC, Information and Privacy Commissioner, http://www.ipc.on.ca) és la Sra. Ann Cavoukian, que ha ocupat diferents càrrecs a l'IPC des de l'any 1987; al llarg de la seva carrera professional, s'ha destacat per prestar una atenció especial als aspectes tant tecnològics com organitzatius de la protecció de dades, perquè considera que la tecnologia té un paper clau en la protecció de la privacitat. Per això, ha promogut i ha participat en un bon nombre de publicacions on es tracten qüestions tecnològiques relacionades amb la privacitat i la protecció de dades. Per exemple, és força coneguda per haver treballat conceptes com el de *privacy by design* o el de *privacy enhancement technologies* (PET).

El punt d'inici de la comunicació és conegut (un usuari o procés inicia una transacció), i el de destí també (un servidor dóna resposta a la transacció), i així successivament. Però el camí que seguirà la informació transportada entre tots dos punts respon a unes regles que, si bé són fixades per un protocol tècnic (TCP), tenen resultats impredictibles *a priori*; d'aquesta manera, a la pràctica podem intuir per on passarà la informació, però sense poder-ne estar del tot segurs.

Cal afegir-hi un altre element, que és que, tot i que en essència aquests dispositius es dediquen a gestionar el trànsit de la informació entre origen i destí, no se'ns pot escapar que durant aquest trànsit la informació es pot sotmetre a tractaments que vagin més enllà de facilitar la transmissió de paquets d'informació.

Vull recordar que hi ha un debat obert en relació amb l'ús de tecnologies d'inspecció de paquets (*deep packet inspection*, DPI). És a dir, la capacitat que tenen alguns equipaments de xarxa que no són punt final de comunicacions de tractar, no només les capçaleres dels paquets que ha de retransmetre per la Xarxa, sinó també, convenientment configurat, d'analitzar-ne el contingut.

De fet, la circumstància que les dades personals es puguin tractar exclusivament a efectes de trànsit per la Xarxa està prevista a la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades personals (LOPD). Quant a la determinació de l'àmbit territorial d'aplicació, a l'art. 2.1.a preveu que l'LOPD és aplicable quan el responsable del tractament, tot i no estar establert en el territori de la Unió Europea, utilitzi mitjans situats en territori espanyol, llevat si aquests mitjans s'utilitzen únicament amb la finalitat de trànsit.

Ara bé, en el moment que el «núvol» deixa de ser exclusivament un mitjà de transport de la informació, per a passar a tenir capacitat de processament de la informació, s'hi afegeix el *computing*; tot i que en realitat la capacitat de processament no recau exactament en el «núvol», sinó en aplicacions, plataformes i infraestructures disponibles a la Xarxa i que, en alguns aspectes, es comporten com els dispositius del «núvol» a què he fet referència.

La informàtica en núvol implica que en el processament d'informació hi concorren una sèrie de característiques que tenen com a conseqüència directa que l'origen, i especialment el destí, d'una transacció deixa de tenir uns valors absoluts, per a passar a ser relatius: la informació no sempre és on realment sembla i no sempre es tracta allà on sembla que s'està processant.

La definició d'*informàtica en núvol* que generalment serveix de base per a dotar de contingut aquest concepte és la del NIST[www1] (Institut Nacional d'Estàndards i Tecnologies, una agència del Departament de Comerç dels Estats Units, creada el 1901). L'última versió d'aquesta definició d'*informàtica en núvol* elaborada pel NIST és de juliol del 2009.

Segons aquesta definició, hi ha cinc característiques que defineixen la informàtica en núvol:

- Autoservei: l'usuari pot utilitzar més capacitats de processament o emmagatzemament de la informació, sense demanar-ho expressament al proveïdor del servei.
- Ampli accés a la Xarxa: es pot accedir a la Xarxa des de diferents dispositius i xarxes.
- Agrupació i reserva de recursos: hi ha un conjunt de recursos compartits pels usuaris, d'acord amb les seves necessitats puntuals, que implica que en cada moment els recursos reservats poden ser diferents.
- Rapidesa i elasticitat: es pot accedir als nous recursos de forma immediata i aparentment il·limitada.
- Servei mesurable i supervisat: se'n controla l'ús i en tot moment es pot conèixer, de manera transparent, el nivell de recursos utilitzats en cada moment.

Aquesta capacitat de procés en el «núvol» està connectada amb la tendència d'externalització dels serveis TIC de les organitzacions i la reconversió d'aquests serveis en el que s'anomena una *utility computing*.

En relació amb aquesta qüestió, recomano la lectura de l'article de Nicholas Carr[2] publicat en l'MIT Sloan Management Review (Massachusetts Institute of Technology),

2. Nicholas Carr és autor del *best-seller* del 2008 del *Wall Street Journal* titulat *El gran canvi: cablejant el món, des d'Edison fins a Google*, que és considerat un dels llibres més influents en relació amb la informàtica en núvol (http://www.nicholasgcarr.com/info.shtml)

[www1] http://www.nist.gov

d'abril del 2005, que amb el títol «The End of Corporate Computing»[www2] descriu els motius que han de portar les organitzacions a deixar de considerar les TIC un actiu de la seva propietat, per a passar a tractar-les com un servei que compren.

Al seu article, Carr fa un paral·lelisme entre el procés de transformació de l'ús de les TIC que han de seguir les organitzacions per a ser competitives, amb la transformació que es va produir a principis del segle xx, quan les empreses industrials va començar a tancar i a desmantellar les fonts d'energia utilitzades per les seves indústries i que eren de la seva propietat (rodes d'aigua, màquines de vapor, generadors elèctrics, etc.).

Aproximadament a partir del 1880, va començar a ser possible la producció comercial d'electricitat; el 1902, als Estats Units hi havia unes 50.000 plantes de generació privada d'energia i només hi havia 3.600 estacions que poguessin vendre energia a d'altres, amb moltes limitacions i inicialment a un preu alt. Però entre el 1907 i el 1920 la quota de producció d'energia elèctrica per a ser comercialitzada va passar del 40% al 70%, i el 1930 ja arribava al 80%.

Els motius d'aquesta ràpida adopció d'un nou model de subministrament d'energia per a les indústries eren senzills: uns costos més baixos i una complexitat de gestió més petita, que permetia que les indústries es poguessin centrar en el seu negoci.

Per a Nicholas Carr, al seu article del 2005, hi ha tres avenços tecnològics clau en la transformació de les TI: la virtualització, la graella de càlcul o grid computing i els serveis web que, combinats amb l'augment de capacitat de les xarxes de comunicacions i la fibra òptica, donen com a resultat un escenari idoni per a dur a terme aquesta transformació, de manera que l'obstacle més important no serà la tecnologia, sinó l'actitud de les organitzacions a l'hora d'assumir aquest nou model d'ús de les TIC en els seus negocis.

El cert és que la informàtica en núvol ja és una realitat per als usuaris de la Xarxa, a títol individual. Els principals casos d'ús de la informàtica en núvol impliquen companyies i serveis com Facebook, Amazon, Nasdaq o Google. En un informe del Pew Research Center[3] de setembre del 2008 s'assenyalava, en relació amb l'ús de la informàtica en núvol, que el 69% dels usuaris d'Internet dels Estats Units emmagatzema dades o utilitza aplicacions basades en serveis d'informàtica en núvol.

L'explosió real de la informàtica en núvol serà provocada per aquest model d'ús de les TIC per part de les empreses.[4] Tal com el mateix NIST inclou a la seva definició, la informàtica en núvol és un paradigma que encara està en evolució.

Arribats a aquest punt, ja podem començar a parlar d'alguns elements clau a l'hora de parlar d'informàtica en núvol i protecció de dades: l'obtenció de serveis TIC prestats per tercers, especialitzats en el processament d'informació, el que en el context de la protecció de dades coneixem com l'*encarregat del tractament*.

I també podem avançar un segon element de rellevància, que, si bé no sempre hi serà present, si s'és conseqüent amb el paradigma de la informàtica en núvol i el que implica d'estalvi de costos sí que tindrà molt de pes. Aquest segon element serà la prestació d'aquests serveis per part d'empreses globals, ubicades en aquells llocs del món on la instal·lació de centres de procés de dades orientats a la informàtica en núvol resulti més rendible. Això sovint implicarà l'aplicació de la figura del moviment internacional de dades personals, també prevista a la normativa en matèria de protecció de dades de caràcter personal.

Més endavant tornaré a analitzar amb una mica més de detall aquestes dues qüestions, però ara voldria afegir alguns altres comentaris de caràcter general.

3. http://pewresearch.org/. Un recent informe d'aquest centre d'investigació (juny del 2010) recull l'opinió dels experts que el 2020 la majoria d'usuaris d'Internet utilitzarà aplicacions basades en la informàtica en núvol, en lloc de les aplicacions d'escriptori (http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx).
4. En aquest sentit, resulta d'especial interès la tasca de Salesforce, en relació amb l'ús empresarial de la informàtica en núvol. Vegeu http://www.salesforce.com/es/cloudcomputing/ i http://www.youtube.com/watch?v=VOn6tg3e1t4.

[www2] http://sloanreview.mit.edu/the-magazine/articles/2005/spring/46313/the-end-of-corporate-computing/

Tot i que tant la Directiva 95/46/CE, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, com la Llei orgànica de protecció de dades preveuen aquestes dues circumstàncies (encarregat del tractament i moviment internacional de dades), el seu plantejament en relació amb el tractament de la informació és «pre-Internet»; és a dir, un escenari de bases de dades centralitzades, tant físicament com lògicament (maquinari i programari), situades en centres corporatius de processament de dades instal·lats físicament en els locals de l'organització responsable del tractament.

De fet, les mateixes autoritats de control europees reconeixen que, tot i que les previsions de la Directiva 95/46/CE es van fer d'una manera tecnològicament neutra, i que sembla que des de l'any 1995 han anat resistint la contínua evolució de les tecnologies i les xarxes, hi ha complexitats aportades per aquesta evolució que generen certa incertesa quant a l'assignació de responsabilitats en el tractament de les dades de caràcter personal i quant a l'abast de les legislacions nacionals aplicables.

No hem d'oblidar que en el context de la protecció de dades personals resulta essencial la identificació del responsable del tractament, ja que això garanteix que hi ha una persona que té assignades una sèrie d'obligacions concretes derivades del tractament i, per tant, hi ha algú a qui es pot exigir el compliment d'aquestes obligacions.

Molts dels serveis en línia que han emergit com a conseqüència de l'ús intensiu i massiu de la Xarxa, en els darrers anys, han posat al límit la legislació europea en matèria de protecció de dades; en algun cas, fins i tot ha esdevingut insuficient per a donar resposta a les noves situacions que sorgeixen a Internet. Per això el grup d'autoritats de control que crea l'art. 29 de la Directiva (conegut com a *grup de l'art*. 29) ha hagut d'anar analitzant i dictaminant sobre determinades qüestions.[5] De fet, en el programa de treball 2010-2011 del grup de l'art. 29 s'inclou explícitament analitzar la informàtica en núvol en relació amb la protecció de dades de caràcter personal.

En l'àmbit internacional, i per tant més enllà del context europeu, les autoritats de control de privacitat i protecció de dades també han mostrat la seva preocupació per aquestes qüestions. Resulta d'especial rellevància la proposta conjunta per a la redacció d'estàndards internacionals per a la protecció de la privacitat, en relació amb el tractament de dades de caràcter personal, acollida per la 31a. Conferència Internacional d'Autoritats de Protecció de Dades i Privacitat (5 de novembre del 2009, Madrid). Aquesta proposta és el resultat d'una resolució prèvia de la 30a. Conferència, que plantejava la necessitat urgent de protegir la privacitat en un món sense fronteres, i d'assolir una proposta conjunta per a l'establiment d'uns estàndards internacionals sobre privacitat i protecció de dades personals.

El diferents models de servei d'informàtica en núvol, ja sigui com a servei de programari (SaaS), de plataforma (PaaS) o d'infraestructura (IaaS), impacten directament sobre una qüestió clau en la definició del dret a la protecció de dades de caràcter fonamental: l'autodeterminació informativa.

Tot i que en funció del model de desplegament del núvol l'impacte és més gran o més petit: núvol públic, privat, híbrid (dos núvols diferents o més) o comunitari.

Aquesta autodeterminació informativa, tal com la van definir les sentències 290/2000 i 292/2000 del Tribunal Constitucional, de 30 de novembre de 2000, implica:

- En primer lloc, que «el dret a la autodeterminació informativa és un dret actiu de control sobre el conjunt d'informacions relatives a una persona».

5. El Document de treball relatiu a l'aplicació internacional de la legislació comunitària sobre protecció de dades al tractament de les dades personals a Internet per a llocs web ubicats fora de la Unió Europea, aprovat el 30 de maig del 2002; el Dictamen 1/2008, sobre qüestions de protecció de dades relacionades amb el motors de cerca; el més recent Dictamen 5/2009, sobre les xarxes socials en línia; o el de començament d'aquest any, Dictamen 1/2010, sobre els conceptes de *responsable del tractament* i *encarregat del tractament*, en són alguns exemples rellevants. En aquest darrer document es fa una referència directa a la informàtica en núvol i a les dificultats que pot implicar per a aquesta assignació de responsabilitats en matèria de protecció de dades. A http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/ s'hi troben tots els documents aprovats pel grup de l'art. 29.

- En segon lloc, que «el dret a la protecció de dades garanteix als individus un poder de disposició» sobre les seves dades personals.
- I en tercer lloc, que aquest poder de disposició sobre les pròpies dades personals no val res si l'afectat desconeix quines dades seves són les que tenen tercers en el seu poder, qui són aquests tercers i amb quina finalitat tenen les seves dades.

I aquest inconvenient és un dels primers que s'han detectat en relació amb la informàtica en núvol: la pèrdua efectiva de control sobre les dades, ja que, més enllà dels vincles contractuals o de subscripció amb les empreses que presten aquests serveis, desapareix o «s'ennuvola» el lligam o certesa sobre la ubicació física de la informació i les condicions de processament i, en conseqüència, poden quedar afectades les garanties de confidencialitat i de seguretat de la informació situada al núvol.

I aquesta preocupació no l'expressen únicament les autoritats de control, ja que tal com recull un document de l'NIST, de juliol del 2009, «Effectively and Securely Using the Cloud Computing Paradigm» ('Ús eficaç i segur de la informàtica en núvol'), un dels reptes de la informàtica en núvol és la seguretat, tot i que el mateix document valora que «cloud security is a tractable problem».

O, en la mateixa línia, un estudi més recent, de juny d'aquest any, també d'IDC però molt més proper ja que es va realitzar amb grans empreses i organitzacions a Catalunya, evidencia que un dels inhibidors a les empreses per a fer el salt al núvol és la preocupació per la falta de confidencialitat de les dades (amb una puntuació de 4,4 sobre 5, i a molta distància de la resta d'inhibidors).

I, per acabar, un document de la Cloud Security Alliance[6] (CSA), «Top Threats to Cloud Computing v1.0», de març del 2010, que identifica les set principals amenaces que poden afectar el desplegament de la informàtica en núvol, entre les quals inclou la pèrdua o fuga de dades (*data loss* o *leakage*).

Que la seguretat en la informàtica en núvol és una qüestió de la qual cal ocupar-se ho evidencien els treballs de diferents organitzacions, que en estudis de més o menys profunditat han treballat recentment aquesta qüestió. A part d'alguns ja esmentats, podem destacar els següents:

- «Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud computing», del Fòrum Mundial de Privacitat[www3] (febrer del 2009).
- «Cloud Computing. Information Assurance Framework» i «Cloud computing. Benefits, risks and recommendations for information security», d'ENISA[www4] (tots dos de novembre del 2009).
- «Guía para la seguridad en áreas críticas de atención en cloud computing», de la CSA[www5] (també de novembre del 2009).
- «Modeling cloud computing architecture without compromising privacy: a privacy by design approach», del Comissionat d'Informació i Privacitat d'Ontàrio[www6] (maig del 2010).

En acabar aquesta part introductòria, no voldria deixar passar l'oportunitat d'evidenciar altres riscos, derivats també d'aquesta pèrdua de control, que tenen a veure amb l'ús de les dades personals amb fins de seguretat pública, ja que sens dubte la informàtica en núvol pot esdevenir també una oportunitat perquè els cossos i forces de seguretat puguin exercir un control més gran sobre la població, a fi de protegir la ciutadania d'actes violents vinculats a la seguretat pública i a la seguretat dels estats.

Els recomano que visitin el lloc web Statewatch[www7] (observatori de l'activitat dels estats i de les llibertats civils a Europa) i que facin una lectura del document del Consell de la Unió Europea, d'abril del 2010, en relació

6. La Cloud Security Alliance té per finalitat promoure l'ús de les millors pràctiques en seguretat en el context de la informàtica en núvol, organització de la qual per cert recentment s'ha creat el capítol espanyol, un dels primers a escala mundial (http://www.cloudsecurityalliance.org/).

[www3] http://www.worldprivacyforum.org
[www4] http://www.enisa.europa.eu
[www5] http://www.cloudsecurityalliance.org/
[www6] http://ipc.on.ca
[www7] http://www.statewatch.org

amb l'ús d'un «instrument estandarditzat, multidimensional i semiestructurat de recollida de dades i informació relacionada amb els processos de radicalització a la Unió Europea» (Enfopol 99), que té per objecte «evitar que les persones es converteixin en terroristes, abordant factors i causes profundes que puguin conduir a la radicalització i el reclutament tant dintre com fora d'Europa».

I és que no hem d'oblidar que el dret a la protecció de dades personals té un caràcter instrumental per a l'exercici d'altres drets fonamentals, i íntimament connectat amb les llibertats públiques i individuals. Per tant, hem de tenir present que quan parlem de protegir les dades personals o d'autodeterminació informativa parlem, en definitiva, de llibertat.

Entrant ara en els aspectes pràctics i més tècnics de la regulació en matèria de protecció de dades que, en relació amb la informàtica en núvol, cal tenir en compte des d'una perspectiva de compliment legal, ja n'he avançat la primera qüestió que cal analitzar: fins i tot en la modalitat de desplegament privat de la informàtica en núvol, si la infraestructura del núvol la gestiona un tercer ens trobarem amb el cas d'un «tractament per compte de tercers», és a dir, amb la figura d'encarregat de tractament, situació regulada a l'art. 12 de la LOPD.

Això, sense entrar a discutir sobre les dificultats que en alguns casos es poden donar en la determinació de qui és el responsable d'un tractament, ja que certes situacions no fan tan evident l'assignació d'aquesta responsabilitat. En el context de la directiva europea, té a veure amb aquella persona física o jurídica que determina les finalitats i els mitjans de tractament de les dades personals.

El Dictamen 1/2010 del grup de l'art. 29, al qual ja he fet referència,[7] aborda aquesta qüestió en profunditat i amb exemples connectats directament amb la informàtica en núvol; en definitiva, es considera que, per a la determinació del responsable del tractament, no només s'han de tenir en compte les relacions jurídiques, sinó també les situacions fàctiques, de manera que cal analitzar les circumstàncies de cada cas per a assignar la responsabilitat sobre el tractament.

Abans de continuar amb l'encarregat del tractament, hi ha una qüestió que voldria tractar breument, concretament sobre l'àmbit d'aplicació de la LOPD: en quin moment, a un tractament per compte d'un tercer, hi són d'aplicació els requisits i condicions de l'art. 12 de la LOPD, que regula la figura de l'encarregat del tractament.

L'àmbit d'aplicació de l'LOPD és regulat a l'art. 2, que preveu que la LOPD és d'aplicació quan:

- El tractament s'efectua en territori espanyol, en un establiment del responsable del tractament; aquí la territorialitat té un pes específic important, que en el cas de la informàtica en núvol pot plantejar seriosos dubtes quant a la seva verificació; com dèiem, som davant d'una òptica clàssica del que són els centres de processament de dades.
- El responsable del tractament no té establiment a territori espanyol, però en aplicació de les normes de dret internacional públic li és aplicable la normativa espanyola.
- El responsable del tractament no està establert en el territori de la Unió Europea, però utilitza mitjans de tractament situats a territori espanyol (amb l'excepció que només sigui amb la finalitat de trànsit). Com a resultat de la tasca interpretativa del grup de l'art. 29, per exemple l'ús de galetes (cookies) es considera ús de mitjans situats en el territori de l'ordinador de l'usuari on s'instal·len les galetes (vegin WP56, sobre l'aplicació internacional de la legislació comunitària de protecció de dades).

L'art. 3 del Reglament de desplegament de la LOPD, aprovat pel Reial decret 1720/2007, de 21 de desembre (RLOPD), aporta alguns elements addicionals en relació amb l'àmbit territorial d'aplicació del reglament, que afegeix tres qüestions que convé comentar:

1) Si el responsable del tractament no té un establiment a territori espanyol, però té un encarregat del tractament ubicat a Espanya, li és d'aplicació el títol viii del Reglament, és a dir, les mesures de seguretat.
2) Si el responsable del tractament no està establert en el territori de la Unió Europea, però utilitza mitjans situats a territori espanyol, aquest responsable del tractament ha de designar un representant establert en territori espanyol.

7. Veure nota 5.

3) I que per *establiment* s'ha d'entendre qualsevol instal·lació que permeti l'exercici efectiu i real d'una activitat, amb independència de la forma jurídica adoptada.

Continuant amb el tractament per compte de tercers, a fi que la figura d'encarregat de tractament entri en joc i que, per tant, es consideri que no hi ha una comunicació de dades, ha d'existir necessàriament una relació jurídica que vinculi responsable i encarregat de tractament i que delimiti, de forma precisa, quina serà la seva activitat en relació amb el tractament de dades personals que realitza l'encarregat per compte del responsable del tractament.

En situacions en què un tercer presti serveis d'informàtica en núvol, diferent per tant del responsable del tractament, i sigui d'aplicació la LOPD, cal aplicar en tota la seva extensió el que preveu el capítol iii del RLOPD (art. 20, 21 i 22).

Una de les obligacions que estableix el RLOPD a l'art. 20.2 és que el responsable del tractament ha de vetllar perquè l'encarregat del tractament compleixi el que preveu el reglament. Per tant, cal articular aquests mecanismes de supervisió, que en certes circumstàncies seran difícils d'implementar, especialment quan l'encarregat del tractament pugui tenir una posició dominant en el mercat.

Una altra qüestió d'interès, que regula l'art. 21, és la subcontractació de serveis, que parteix del principi general que l'encarregat del tractament no pot subcontractar a un tercer cap tractament que li hagi estat encomanat pel responsable del tractament. Ara bé, sí que ho pot fer si obté autorització del responsable del tractament, i sempre que aquesta subcontractació la faci en nom i per compte del responsable del tractament.

Hi ha algunes condicions que permeten exceptuar l'autorització del responsable del tractament:

- Que ja estigui especificat en el contracte de serveis que regula l'encàrrec, i que s'indiqui l'empresa que es subcontractarà o, si no és possible aquesta determinació *a priori*, l'encarregat ha de comunicar al responsable quina empresa pensa subcontractar abans de procedir a la subcontractació.
- Òbviament, el subcontractista s'ha d'ajustar a les instruccions del responsable del tractament, donades a l'encarregat del tractament.
- Que l'encarregat i el subcontractista formalitzin un contracte; llavors el subcontractista tindrà la consideració d'encarregat de tractament.

Una vegada finalitzada la prestació contractual, també serà d'aplicació el règim previst en relació amb la conservació de dades per part de l'encarregat del tractament; com a regla general, les dades s'han de destruir o retornar al responsable, llevat que alguna previsió legal obligui l'encarregat del tractament a conservar-les. Això sí, les dades han d'estar bloquejades, és a dir, no es poden sotmetre a cap tipus de tractament que vagi més enllà de la mateixa conservació i de les mesures de seguretat derivades d'aquesta obligació de conservació.

Voldria recordar, en aquest punt, que el concepte de tractament en el context de la protecció de dades té una configuració àmplia, ja que es considera *tractament* qualsevol operació o procediment tècnic que permeti recollir, gravar, conservar, elaborar, modificar, consultar, utilitzar, bloquejar o cancel·lar les dades, així com les cessions de dades que es derivin de comunicacions, consultes, interconnexions i transferències de dades (art. 3, lletra c de la LOPD i art. 5.1, lletra t del RLOPD).

Una vegada abordada la qüestió de l'encarregat del tractament, ja sigui perquè ens presta serveis de núvol d'aplicació (programari), de plataforma o d'infraestructura, la segona qüestió de rellevància que cal abordar té a veure amb el fet que es pugui arribar a produir un moviment internacional de dades com a conseqüència de l'ús de serveis en el «núvol». Si es dóna aquest cas, és d'aplicació el que preveu el títol V de la LOPD (art. 33 i 34) i el títol VI del RLOPD (de l'art. 65 al 70).

Com a principi general, s'estableix que no es poden fer transferències de dades personals a països que no proporcionin un nivell de protecció equiparable al de la LOPD.

Aquesta transferència internacional es pot realitzar si, a banda de complir el que preveu la LOPD, així ho autoritza el director de l'AEPD. El procediment per a sol·licitar aquesta autorització el regula el RLOPD (de l'art. 137 al 144).

No cal autorització si el país on està establert l'importador de les dades ofereix un nivell adequat de protecció; aquesta determinació de nivell adequat la fa el director de

l'AEPD, mitjançant resolució i per a un país en concret. Tampoc cal aquesta autorització si el nivell adequat ha estat declarat per una decisió de la Comissió Europea; aquí també s'inclou, per exemple, l'acord de port segur amb els Estats Units.

També hi ha tota una sèrie de casos concrets que són excepcions a la necessitat d'autorització del director de l'AEPD. Aquestes excepcions es regulen a l'art. 34 de la LOPD (tractats i convenis internacionals, auxili judicial, serveis relacionats amb la salut, transferències dineràries, consentiment inequívoc de l'afectat, necessària en relacions contractuals, interès públic, procediment judicial o petició des de registres públics).

En cas que l'autorització sigui necessària, cal presentar un contracte escrit, entre importador i exportador, en el qual constin les garanties de respecte necessàries per a la protecció de la vida privada. A aquests efectes hi ha tota una sèrie de decisions de la Comissió Europea, relacionades amb els continguts d'aquests tipus de contractes (art. 70.2).

Les transferències internacionals s'han de notificar, per a inscriure-les en el registre general de protecció de dades en registrar el tractament que preveu la transferència internacional. Les autoritzacions de transferències internacionals també s'inscriuen, en aquest cas d'ofici.

En relació amb les transferències internacionals, poden resultar d'interès els estudis realitzats per algunes organitzacions en relació amb els diferents nivells d'exigència en matèria de protecció de dades.

Així, tenim el mapa global de la protecció de dades que ja fa uns anys que publica *Privacy International,*[www8] 12 i un de nou, que amb un certa orientació de màrqueting ha elaborat recentment Forrester Research,[www9] 13 acompanyat de la pregunta de si sabem on són les nostres dades al núvol (*Do you know where your data is in the cloud*?).

Per acabar, hi ha un cas especial d'autorització de transferència internacional, previst a l'art. 70.4 del RLOPD, per al cas que es produeixi en el si de grups multinacionals d'empreses. En aquest cas, cal que aquests grups hagin adoptat el que es coneix com a *normes corporatives vinculants*, o *binding corporate rules* (BCR), en les quals constin les garanties de respecte necessàries per a la protecció de la vida privada i el dret fonamental a la protecció de dades, així com els principis i exercici de drets previstos al LOPD.

Aquestes normes o regles han de ser vinculants per a les empreses del grup i exigibles segons l'ordenament jurídic espanyol, i les pot exigir tant l'AEPD com les persones afectades.

El grup de l'art. 29 també té publicats alguns documents en relació amb les BCR. A efectes introductoris, resulten d'interès el «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules», el «Working Document Setting up a framework for the structure of Binding Corporate Rules» i el «Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules», tots de juny del 2008.

Segons dades de l'AEPD, entre l'any 2000 i el juliol del 2007 es van autoritzar un total de 148 transferències internacionals, i el 2007 es van notificar al registre de protecció de dades un total de 8.483 moviments internacionals de dades.

Per acabar, voldria apuntar només una qüestió final, però essencial, relacionada amb la salvaguarda del dret fonamental a la protecció de dades de caràcter personal, en aquelles situacions en què aquest dret es pugui veure vulnerat en ambients d'informàtica en núvol, en què es poden donar situacions de multiterritorialitat i, per tant, amb dificultats per a resoldre de forma efectiva les possibles vulneracions; sens dubte, és un tema que hauran d'abordar les autoritats de control, especialment les de la Unió Europea, quant a coordinació entre autoritats, intraeuropees i extraeuropees.

En conclusió, els aspectes més rellevants relacionats amb el compliment legal que cal abordar o tenir en compte quan connectem protecció de dades i informàtica en núvol tenen a veure amb:

[www8] http://www.privacyinternational.org/ i el mapa a http://www.privacyinternational.org/survey/dpmap.jpg.
[www9] http://www.forrester.com/rb/research i el mapa a http://www.forrester.com/cloudprivacyheatmap.

1) La pèrdua de control sobre el tractament de la informació, tant per part de les persones afectades com per part del responsable del tractament, i les conseqüències que se'n puguin derivar (seguretat, confidencialitat, exercici de drets, etc.).
2) Les dificultats d'encaixar jurídicament i amb suficient agilitat les situacions de tractament de les dades per compte de tercers: l'encarregat del tractament del núvol i les possibles subcontractacions.
3) Les problemàtiques derivades del moviment internacional de dades.
4) I per acabar, la resolució efectiva dels incidents relacionats amb la vulneració del dret fonamental a la protecció de dades personals en situacions de multiterritorialitat.

Citació recomanada

MIRALLES, Ramón (2010). «Informàtica en núvol i protecció de dades». En: «VI Congrés Internet, Dret i Política. *Cloud Computing*: El Dret i la Política Pugen al Núvol» [monogràfic en línia]. *IDP. Revista d'Internet, Dret i Política*. Núm. 11. UOC. [Data de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-miralles/n11-miralles-cat>

ISSN 1699-8154

Sobre l'autor

Ramón Miralles
ramon.miralles@gencat.cat

Coordinador d'Auditoria i Seguretat de la Informació. Autoritat Catalana de Protecció de Dades.

Autoritat Catalana de Protecció de Dades
C/Llacuna, 166, 8a planta
08018 Barcelona, Espanya