CNS 24/2012

Dictamen en relació amb la consulta formulada per un consell comarcal sobre la contractació del servei *Google Apps for Business*

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per un consell comarcal sobre la contractació del servei *Google Apps for Business* i la seva adequació a la normativa de protecció de dades.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

El Gerent del Consell Comarcal manifesta, en el seu escrit de consulta, que, per tal de millorar l'espai de les bústies de correu electrònic dels seus treballadors, de la gestió del correu brossa i de la gestió de les còpies de seguretat, així com per tal d'utilitzar calendaris per organitzar la seva feina i treballar amb documents de manera col·laborativa, es planteja contractar amb l'empresa *Google Ireland Limited* els serveis que ofereix en aquest sentit mitjançant *Google Apps for Business.*

D'acord amb allò establert al web de la companyia Google (www.google.com/apps/intl/es/business), els serveis *Google Apps for Business* permeten la utilització d'eines de comunicació i col·laboració senzilles i eficaces en línia (com ara, *Gmail for business, Google Docs, Google Calendar, Google Sites*...) amb la finalitat de simplificar la configuració, minimitzar el manteniment i reduir els costos de les tecnologies de la informació de les empreses o de les entitats que els contractin.

La utilització d'aquests serveis que operen en Internet (habitualment sota un model d'aprovisionament de serveis TIC tipus *Cloud computing* o "computació en el núvol"), és a dir, sense necessitat d'instal·lar *software* o de disposar d'un servidor propi (només cal disposar de connexió a Internet), precisen de la recollida i del tractament de dades de caràcter personal, les quals són emmagatzemades en els servidors gestionats pel proveïdor d'aquests serveis, sovint ubicats a l'estranger.

Des de la vessant del dret a la protecció de dades personals, i d'acord amb el funcionament descrit, cal tenir en compte, d'entrada, que la contractació d'aquests serveis "en el núvol" gestionats per un tercer, quan la seva prestació implica tractar dades personals dels fitxers o dels sistemes del responsable del fitxer o tractament, constitueix el que la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) anomena "un accés de dades per compte de tercers" (article 12).

En aquest sentit, resulta necessari identificar tant al responsable del fitxer o tractament com a l'encarregat del tractament, així com les seves interaccions, per tal determinar la responsabilitat de cadascú en el compliment de les normes de protecció de dades.

Segons l'article 3.d) de la LOPD s'entén per responsable del fitxer o tractament *"la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament"*.

Si bé és cert que, en l'àmbit de la "computació en el núvol", en determinades circumstàncies resulta complex identificar qui és el responsable del tractament, atès que normalment els proveïdors d'aquests serveis tendeixen a determinar unilateralment els mitjans i, fins i tot en alguns casos, els fins dels tractaments, s'entén que els clients es configuren com els responsables del tractament, en la mesura que són els titulars dels fitxers en què inicialment es troben recollides les dades que seran transmeses i que legitimen el seu tractament.

Així mateix, s'entén que la capacitat de què disposa el responsable del tractament per decidir sobre la finalitat, el contingut i l'ús del tractament de les dades es manifesta en la seva capacitat per decidir dur a terme la contractació d'aquests serveis, quina modalitat de "computació en el núvol" contractar (privada, pública, híbrida o comunitària) i quin dels diferents models de servei de "computació en el núvol" contractar (de software (SAAS), de plataforma (PASS) o d'infraestructura (IAAS)).

Per la seva part, l'article 3.g) de la LOPD defineix, com a encarregat del tractament*, "la persona física o jurídica, l'autoritat pública, el servei o qualsevol altre organisme que, sol o conjuntament amb altres, tracti dades personals per compte del responsable del tractament"*.

En el supòsit que ara s'examina, doncs, pot dir-se que el Consell Comarcal és el responsable del fitxer o tractament, mentre que l'empresa Google Ireland Limited, prestadora dels serveis *Google Apps for Business*, adoptaria la postura d'encarregat del tractament.

Sent així, la transmissió d'informació personal des del Consell Comarcal a l'empresa Google Ireland Limited, que inclourà no només dades dels empleats públics sinó probablement també, atès l'exercici de les seves competències, dades de ciutadans (fins i tot, podria ser el cas de dades de caràcter sensible (article 7 LOPD)), no tindrà consideració de comunicació o cessió de dades en els termes establerts a l'article 3.i) de la LOPD.

Ara bé, per a que això sigui possible cal que, d'acord amb l'article 12 de la LOPD, se celebri un contracte d'encarregat del tractament entre ambdues entitats, en què es determini de manera expressa:

a) Que l'encarregat del tractament ha de tractar les dades d'acord amb les instruccions del responsable del tractament.
b) Que no pot aplicar ni utilitzar les dades amb una finalitat diferent de la que figuri en el contracte, ni comunicar-les a altres persones, ni tant sols per a la seva conservació.
c) Les mesures de seguretat que l'encarregat està obligat a implementar.
d) El retorn o la destrucció de les dades, un cop complerta la prestació contractual.

Atès que el responsable del fitxer o tractament és una administració pública, cal tenir en compte que l'aplicació d'aquest precepte de la LOPD també vindria imposada pel Reial decret legislatiu 3/2011, de 14 de novembre, pel qual s'aprova el Text refós de la Llei de contractes del sector públic, en què s'estableix (Disposició addicional 26a, apartat 2) que *"para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento"*, sent necessari que, en qualsevol cas, les previsions del citat article 12 de la LOPD constin per escrit.

A més, caldrà donar compliment a les previsions que el Reglament de desplegament de la LOPD, aprovat per Reial decret 1720/2007, de 21 de desembre (RLOPD), estableix també en aquest sentit.

En concret, l'article 20 del RLOPD, relatiu a les relacions entre el responsable i l'encarregat del tractament, disposa que:

"1. L'accés a les dades per part d'un encarregat del tractament que sigui necessari per a la prestació d'un servei al responsable no es considera comunicació de dades, sempre que es compleixi el que estableixen la Llei orgànica 15/1999, de 13 de desembre, i el present capítol.
El servei prestat per l'encarregat del tractament pot tenir o no caràcter remunerat i ser temporal o indefinit.
No obstant això, es considera que existeix comunicació de dades quan l'accés tingui per objecte l'establiment d'un nou vincle entre el qui accedeix a les dades i l'afectat.
2. Quan el responsable del tractament contracti la prestació d'un servei que comporti un tractament de dades personals sotmès al que disposa aquest capítol ha de vetllar perquè l'encarregat del tractament compleixi les garanties per al compliment del que disposa aquest Reglament.
3. En cas que l'encarregat del tractament destini les dades a una altra finalitat, les comuniqui o les utilitzi incomplint les estipulacions del contracte a què es refereix l'apartat 2 de l'article 12 de la Llei orgànica 15/1999, de 13 de desembre, també es considera responsable del tractament, i ha de respondre de les infraccions en què ha incorregut personalment.
No obstant això, l'encarregat del tractament no incorre en responsabilitat quan, prèvia indicació expressa del responsable, comunica les dades a un tercer designat per aquell, a qui ha encomanat la prestació d'un servei conforme al que preveu el present capítol."

Per la seva part, l'article 21 del RLOPD, en relació amb la possibilitat de subcontractar els serveis, estableix que:

"1. L'encarregat del tractament no pot subcontractar amb un tercer la realització de cap tractament que li ha encomanat el responsable del tractament, llevat que n'ha obtingut autorització per fer-ho. En aquest cas, la contractació sempre s'ha d'efectuar en nom i per compte del responsable del tractament.
2. No obstant el que disposa l'apartat anterior, és possible fer la subcontractació sense necessitat d'autorització sempre que es compleixin els requisits següents:
a) Que s'especifiquin en el contracte els serveis que puguin ser objecte de subcontractació i, si això és possible, l'empresa amb la qual s'ha de subcontractar.
Quan no s'identifiqui en el contracte l'empresa amb la qual s'ha de subcontractar, és necessari que l'encarregat del tractament comuniqui al responsable les dades que la identifiquin abans de procedir a la subcontractació.
b) Que el tractament de dades de caràcter personal per part del subcontractista s'ajusti a les instruccions del responsable del fitxer.
c) Que l'encarregat del tractament i l'empresa subcontractista formalitzin el contracte, en els termes previstos a l'article anterior.
En aquest cas, el subcontractista és considerat encarregat del tractament, i li és aplicable el que preveu l'article 20.3 d'aquest Reglament.
3. Si durant la prestació del servei és necessari subcontractar-ne una part i aquesta circumstància no s'ha previst en el contracte, s'han de sotmetre al responsable del tractament els aspectes assenyalats a l'apartat anterior."

D'altra banda, l'article 22 del RLOPD, estableix, pel que fa a la conservació de les dades per part de l'encarregat del tractament, que:

"1. Una vegada complerta la prestació contractual, les dades de caràcter personal han de ser destruïdes o retornades al responsable del tractament o a l'encarregat que aquest ha designat, com també qualsevol suport o documents en què consti alguna dada de caràcter personal objecte del tractament.

No pertoca la destrucció de les dades quan hi ha una previsió legal que n'exigeixi la conservació, cas en què s'ha de procedir a la devolució de les dades amb la garantia del responsable del fitxer de la conservació esmentada.
2. L'encarregat del tractament ha de conservar les dades, degudament bloquejades, mentre no es puguin derivar responsabilitats de la seva relació amb el responsable del tractament."

Per tant, cal tenir present que la contractació de la prestació d'aquests tipus de serveis "en el núvol" requereix l'existència d'un contracte d'encarregat del tractament amb el contingut mínim determinat en aquests preceptes.

Ara bé, cal tenir en compte que l'existència d'aquest contracte per si sol no pressuposa que el tractament de les dades es dugui a terme en aquest àmbit amb totes les garanties exigides en la normativa de protecció de dades personals. El dret fonamental a la protecció de dades personals o a la "autodeterminació informativa" (article 18.4 CE) consisteix en un poder de disposició i de control sobre les dades personals, que faculta a la persona que n'és titular decidir quines d'aquestes dades vol proporcionar a un tercer, així com conèixer qui disposa de les seves dades i per a què o poder oposar-se al seu tractament (STC 292/2000, de 30 de novembre), però de res serveix aquest poder de disposició sobre les pròpies dades personals si l'afectat o, fins i tot, el responsable desconeixen la forma com es tractaran les seves dades.

Aquesta és una situació que es pot donar en el món de la "computació en el núvol" i per això correspon al Consell Comarcal, com a responsable, la tasca de garantir als afectats que les seves dades personals seran en tot moment tractades de conformitat amb la legislació vigent en matèria de protecció de dades. Això l'obliga, inexcusablement, a fer una anàlisi prèvia de l'impacte de la contractació d'aquests serveis en la privacitat, amb especial atenció als riscos per a la seguretat i la integritat de la informació, i a escollir un proveïdor que, alhora, sigui capaç de garantir el compliment de la normativa de protecció de dades, tal i com es recull en el Dictamen 5/2012, d'1 de juliol, sobre el *Cloud Computing,* del Grup de Treball de l'Article 29 de la Directiva Europea 95/46/CE, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals (disponible al web http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm).

En aquest sentit, a continuació, s'analitzen alguns dels riscos en concret que, des de la vessant de la protecció de dades personals, pot comportar la contractació del servei *Google Apps for Business*, prenent com a referència les condicions d'alta en el servei (www.google.com/apps/intl/es/business/).

Abans però, cal posar de manifest la dificultat que existeix, en el cas examinat, per determinar quines són les condicions exactes de la prestació d'aquests serveis i a les que se sotmetrà, en concret, el responsable del tractament (el client) amb la seva contractació.

En principi, i així ho assenyala el Consell Comarcal en el seu escrit de consulta, les condicions d'alta en el servei són les recollides en el *"Acuerdo de Google Apps for Business de Google Ireland Limited"*, disponibles a l'adreça www.google.com/apps/intl/es/terms/premier_terms_ie.html. Ara bé, aquest acord conté una remissió (un enllaç) a unes altres condicions recollides en el "*Acuerdo de Google Apps for Business (online)" i* disponibles a l'adreça www.google.com/apps/intl/es/terms/premier_terms.html que, a la vegada, remeten a unes condicions addicionals de servei.

Ambdós acords, si bé són similars, no contenen exactament les mateixes clàusules (per exemple, en el primer la contractació té lloc amb una societat constituïda a Irlanda (*Google Ireland Limited*), mentre que en el segon la contractació té lloc amb una societat constituïda a Califòrnia (*Google Inc.*)). A més, tant l'un com l'altre contenen

diversos enllaços amb remissions a altres consideracions que també s'han de tenir en compte a l'hora de contractar el servei, algunes d'especial transcendència per a la protecció de dades personals, com ara, la política de privacitat fixada per Google (www.google.com/intl/es/policies/privacy/).

Aquesta disparitat de condicions no permet determinar amb claredat en quins termes i condicions exactes es durà a terme la contractació dels serveis *Google Apps for Business*, fet que, sens dubte, dificulta aquesta anàlisi prèvia dels riscos per a la seguretat i la integritat de la informació.

IV

Com s'ha apuntat en l'apartat anterior, qualsevol tractament de dades personals -i la "computació en el núvol", sens dubte, comporta un tractament de dades- requereix que es dugui a terme sempre amb ple respecte als principis i les obligacions establertes a la normativa de protecció de dades.

Entre aquests principis, cal destacar, especialment, el principi de qualitat (article 4 LOPD), segons el qual *"les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut"* (apartat 1), sense que es puguin utilitzar "*per a finalitats incompatibles amb aquelles per a les quals les dades hagin estat recollides. No es considera incompatible el tractament posterior d'aquestes dades amb finalitats històriques, estadístiques o científiques"* (apartat 2).

Aquest principi, junt amb el del consentiment (article 6 LOPD), resulta cabdal en el dret fonamental a la protecció de dades dels afectats (article 18.4 CE), tal i com es desprèn de la resta de previsions de la mateixa LOPD, com ara, en establir el dret d'informació, en què cal informar de la finalitat del tractament o fitxer (article 5 LOPD), en prohibir la creació de determinats fitxers amb dades especialment protegides (article 7 LOPD) o en considerar responsable a l'encarregat del tractament en cas que es produeixi un canvi en la finalitat (article 12 LOPD). En l'àmbit de la "computació en el núvol" resulta igualment d'aplicació, per la qual cosa és necessari establir amb claredat la finalitat o finalitats concretes per les quals seran tractades les dades personals, per part de les terceres empreses prestadores d'aquests serveis. En aquest mateix sentit, es manifesta el Grup de Treball de l'Article 29 de la Directiva 95/46/CE en el citat Dictamen 5/2012, d'1 de juliol, sobre *Cloud Computing* (apartats 3.4 i 4.1).

Si s'examinen, en aquest sentit, les condicions d'ús del servei de *Google Apps for Business* de Google Ireland Limited que s'assenyalen a la consulta i que estan disponibles a l'adreça electrònica www.google.com/apps/intl/es/terms/premier_terms_ie.html es pot comprovar, d'entrada, que es tracta d'unes condicions generals o estàndards que la companyia Google Ireland Limited fixa de manera unilateral. Pel que fa, en concret, a la finalitat del tractament de les dades, es redueix a establir que:

> *"1.4. Políticas de privacidad. El Cliente acepta que Google procese los datos personales de sus Usuarios finales como parte de los Servicios dentro del ámbito de las capacidades de dichos Servicios, las cuales se estipulan en las Políticas de privacidad de Google. El Cliente, por lo tanto, solicita a Google que le proporcione los Servicios y procese los datos personales de los Usuarios finales en virtud de las Políticas de privacidad de Google y Google, por su parte, se obliga a llevar a cabo estas acciones. Las Políticas de privacidad de Google se incorporan al presente Acuerdo por referencia. El Cliente acepta proteger la privacidad de los Usuarios finales mediante el cumplimiento de una política, que será debidamente comunicada y que en ningún caso protegerá menos que las propias Políticas de privacidad de Google."*

És a dir, segons aquesta condició d'ús del servei, el client (el Consell comarcal) accepta que Google tracti les dades personals dels usuaris finals (treballadors públics i ciutadans) de conformitat amb la política de privacitat que estableix la mateixa companyia Google, una política de privacitat que, tal i com reconeix Google, pot ser modificada en qualsevol moment (apartat 14.1 *"Definiciones"* de les condicions).

A banda d'aquest fet, cal assenyalar que es tracta d'una política de privacitat dissenyada per al conjunt de serveis prestats per Google i no així específicament per al servei de *Google Apps*, de tal manera que les previsions contemplades en ella podrien no encaixar amb el funcionament previst per a aquest servei.

Tot això origina una evident incertesa sobre les condicions exactes en què les dades personals serien tractades per l'encarregat (Google Ireland Limited) i, alhora, posa en evidència que el responsable del tractament o del fitxer (el client) no sembla tenir capacitat suficient per decidir la forma en què vol que es dugui a terme aquest tractament, tal i com exigeix l'article 12.2 de la LOPD.

Si s'examina, en concret, aquesta política de privacitat a què ens remet Google (www.google.com/intl/es/policies/privacy/) -que, recordem, com en ella es recull (apartat *"Modificaciones"*) pot ser modificada en qualsevol moment de manera unilateral-, es desprèn que accedirà a tota la informació emprada pel personal del Consell Comarcal en la realització de les seves funcions (la qual pot fer referència també a ciutadans i, fins i tot, a dades sensibles), ja sigui perquè es facilita directament a Google, ja sigui perquè és Google qui l'obté quan el Consell Comarcal utilitza els seus serveis (dades del dispositiu emprat, dades de registre, dades sobre la ubicació física, *cookies*, etc.).

La finalitat per la qual es recolliria tota aquesta informació seria per *"prestar, mantener, proteger y mejorar dichos servicios, desarrollar nuevos servicios y velar por la protección de Google y de nuestros usuarios. También utilizamos estos datos para ofrecerte contenido personalizado como, por ejemplo, resultados de búsqueda y anuncios más relevantes"*.

En relació, en concret, amb l'oferiment d'aquests anuncis personalitzats, Google estableix, tot seguit, que només preveu no associar *cookies* o identificadors anònims quan es traci de dades especialment protegides.

Així mateix, adverteix que podrà *"combinar la información personal de un servicio con la información de otros servicios de Google, incluida la información personal, para que puedas compartir contenido con usuarios que conozcas más fácilmente, entre otros usos."*

A més, si es revisa el llistat de preguntes i respostes sobre seguretat i privacitat (FAQ) que la mateixa companyia ha elaborat, ateses les nombroses qüestions que en aquest sentit s'han plantejat sobre els seus serveis i, en particular, sobre el servei de *Google Apps* (http://support.google.com/a/bin/answer.py?hl=es&answer=60762), veiem que Google també preveu explorar i indexar dades dels usuaris, tals com documents i missatges de correu electrònic, amb aquesta mateixa finalitat de millorar les principals funcions dels seus productes de *Google Apps*.

D'acord amb aquestes consideracions, per tant, no es pot descartar que, a partir de la informació recollida, Google pugui elaborar perfils força precisos sobre les persones que fan servir els seus serveis.

Així doncs, a l'hora de contractar aquests serveis s'ha de tenir en compte que les actuacions previstes per Google poden excedir la finalitat principal per la qual el Consell comarcal li encarrega el tractament de les dades. En aquest sentit, i en la mesura que el tractament respongui al compliment de finalitats diferents a aquella que

justificà la recollida inicial de les dades per part del Consell Comarcal, ens podríem trobar, per tant, davant una vulneració del principi de qualitat de les dades, en la seva vessant de finalitat (article 4.2 LOPD).

Així mateix, cal tenir en compte que aquest mateix principi de qualitat de les dades, en la seva vessant d'exactitud (article 4.5 LOPD), exigeix que les dades personals siguin cancel·lades un cop hagin deixat de ser necessàries o pertinents per a la finalitat per a la qual han estat recollides o registrades. En el cas d'un tractament de dades per compte del responsable, la normativa estableix la necessitat d'establir en el contracte d'encarregat previsions concretes sobre el retorn o la destrucció de les dades, un cop complerta la prestació contractual (articles 12.3 LOPD i 22 RLOPD).

L'única referència a aquest extrem la trobem en l'esmentat llistat de preguntes i respostes sobre seguretat i privacitat (FAQ), en què es limita a dir que, en cas de deixar d'utilitzar els seus serveis, el client "debería" poder endur-se les seves dades. Aquesta previsió, evidentment, no pot considerar-se en cap cas suficient des del punt de vista de la normativa de protecció de dades.

D'altra banda, i encara relacionat amb aquest principi, convé destacar la previsió de Google, en la seva política de privacitat, de poder "*sustituir los nombres que hayas asociado con anterioridad a tu cuenta de Google de modo que se te identifique de forma coherente en todos nuestros servicios*".

Si bé, per aplicació d'aquest principi, cal mantenir les dades exactes i posades al dia de manera que responguin amb veracitat a la situació actual de l'afectat (article 4.3 LOPD), cal posar de manifest que la modificació d'aquestes dades s'haurà de realitzar, en tot cas, d'acord amb la voluntat del seu titular (l'usuari).

V

Tenint en compte el funcionament propi d'aquests serveis que operen en el "núvol", basat en un emmagatzematge simultani de la mateixa informació en diversos servidors en centres de processament de dades, un altre risc que pot amenaçar la seguretat de les dades personals i que el responsable del tractament o fitxer ha de tenir en compte abans de dur a terme la seva contractació és el de la deslocalització de les dades o dels fluxos d'informació que hi poden tenir lloc. La incertesa sobre la ubicació física real de la informació personal posa de manifest la pèrdua efectiva de control sobre les dades per part del responsable i, conseqüentment, la possibilitat de què aquest vulneri la normativa de protecció de dades.

Com bé assenyala el Consell comarcal en el seu escrit, és possible que la contractació d'aquests serveis "en el núvol" pugui comportar la realització d'una transferència internacional de dades personals (article 5.1.s) RLOPD) si la seva transmissió té lloc fora del territori de l'Espai Econòmic Europeu (EEE), ja sigui perquè aquesta transmissió constitueix una cessió o comunicació de dades (article 3.i) LOPD), ja sigui perquè té per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en el territori espanyol (article 12 LOPD).

D'acord amb la informació facilitada pel Consell Comarcal, la contractació dels serveis *Google Apps for Business* en aquest cas es duria a terme, tal i com s'ha indicat a l'inici d'aquest dictamen, amb Google Ireland Limited.

Segons les condicions del servei *Google Apps for Business* de Google Ireland Limited (www.google.com/apps/intl/es/terms/premier_terms_ie.html), Google Ireland Limited és una societat constituïda de conformitat amb les lleis d'Irlanda i amb seu ubicada a Dublín. Per tant, d'inici, la transmissió de les dades personals des del Consell comarcal a Google Ireland Limited no tindria consideració de transferència

internacional de dades, en trobar-se ubicada aquesta societat dins de l'EEE, de tal manera que no seria aplicable el règim previst en aquest sentit a la LOPD i al RLOPD.

Ara bé, si es continua examinant aquestes condicions es pot comprovar que es preveu també la transmissió de la informació a les "empresas del grupo" (punt 6 relatiu a la informació confidencial), tot i que sense concretar quines són aquestes empreses i on es troben ubicades físicament.

Si s'examinen les altres condicions del servei de *Google Apps for Business* (www.google.com/apps/intl/es/terms/premier_terms.html) a què ens remet Google des d'aquestes primeres condicions, es pot comprovar com la companyia preveu que, com a part del subministrament dels serveis contractats, pot emmagatzemar, transferir i processar "datos de cliente" (definits com "cualquier dato, incluido el correo electrónico, proporcionado, generado, transmitido o mostrado a través de los servicios por el cliente o por los usuarios finales") en els Estats Units o en qualsevol altre país en què Google o els seus agents disposin d'instal·lacions (punt 1.1 relatiu a les instal·lacions i a les transferències de dades), novament sense concretar quins serien aquests països.

Si s'observa el que disposa el ja citat llistat de preguntes i respostes sobre seguretat i privacitat (http://support.google.com/a/bin/answer.py?hl=es&answer=60762), es pot comprovar que Google reitera la previsió d'emmagatzemar les dades del client en la xarxa de centres de dades de Google, els quals es troben repartits per diferents zones geogràfiques "cuyas ubicaciones se mantienen en secreto por motivos de seguridad".

D'acord amb aquestes previsions, per tant, caldrà tenir en compte que, en la mesura que la informació personal s'emmagatzemi en servidors ubicats en els Estats Units, així com en altres zones geogràfiques o tercers països, la transmissió de les dades per part del Consell comarcal a Google sí tindrà consideració de transferència internacional de dades (article 5.1.s) RLOPD).

Per a que aquesta transferència internacional de dades pugui considerar-se conforme amb la normativa de protecció de dades caldrà, a banda de donar compliment al que estableix la LOPD, obtenir l'autorització del Director de l'Agència Espanyola de Protecció de Dades (articles 33 LOPD i 137 a 144 RLOPD), tret que, entre d'altres excepcions, les dades es transfereixin a països que ofereixin un nivell adequat de protecció.

Entre aquests països (article 67 RLOPD), s'inclouen les entitats d'Estats Units adherides als principis de Port Segur (Safe Harbor), d'acord amb la Decisió 2000/520/CE de la Comissió de 26 de Juliol de 2000. Entre elles, hi trobem l'empresa Google, per la qual cosa s'entén que les dades facilitades seran tractades amb determinades garanties i condicions de seguretat.

D'acord amb aquests preceptes, doncs, la transferència internacional de dades des del Consell Comarcal a Google, quan la informació s'emmagatzemi únicament en servidors ubicats en els Estats Units, podria realitzar-se sense necessitat d'autorització del Director de l'Agència, sempre és clar que es complís amb la resta de requeriments de la LOPD, això és, disposar d'un contracte d'encarregat amb els termes de l'article 12.2 de la LOPD, sent necessari que, a més a més, es notifiqui aquesta transferència internacional de dades al Registre General de Protecció de Dades per tal de procedir a la seva inscripció.

En aquest punt, convé tenir presents altres elements addicionals, com ara el fet que, en aquell país i per aplicació de la *USA Patriot Act* (*Public Law* 107-56-Oct. 26, 2001), l'FBI (*Federal Bureau of Investigation*) té capacitat per exigir als prestadors de serveis, inclosos aquells que ofereixen serveis de "computació en el núvol", la divulgació de tot tipus d'informacions, relatives als ciutadans nord-americans però també als estrangers,

ubicades o no en territori nord-americà, en virtut d'una Carta de Seguretat Nacional, sense necessitat de control judicial previ i sense la obligació d'informar als afectats.

Així mateix, cal tenir en compte que, sovint, l'aplicació d'aquests principis de Port Segur poden ser insuficients en un entorn com és el de la "computació en el núvol", en què els fluxos d'informació poden referir-se no als Estats Units sinó a altres zones geogràfiques o tercers països. De fet, aquest és el cas de l'empresa Google que, com hem vist abans, també preveu la transmissió de les dades a servidors ubicats en qualsevol altre país en què ell o els seus agents disposin d'instal·lacions, així com a diferents zones geogràfiques, sense esclarir però les seves ubicacions físiques "por motivos de seguridad".

En aquests casos, perquè la transferència internacional de dades es consideri conforme amb la normativa de protecció de dades, cal assegurar que aquestes altres zones geogràfiques en què s'ubiquen els servidors també estan adherides als principis de Port Segur, tenint en compte, en aquest sentit, que l'adhesió es troba limitada a les entitats que estiguin establertes en els Estats Units i que reben dades personals procedents de la Unió Europea (article 1 de la Decisió de la Comissió Europea de 26 de juliol de 2000 sobre l'adequació de la protecció conferida pels principis de Port Segur per a la protecció de la vida privada i les corresponents preguntes més freqüents, publicades pel Departament de Comerç dels Estats Units d'Amèrica), o bé que aquests tercers països en què s'ubiquen els servidors ofereixen un nivell de protecció equivalent.

En cas contrari, i de no donar-se cap altra de les excepcions previstes a la LOPD, caldria, a banda de complir amb la resta d'extrems de la LOPD, comptar amb l'autorització del Director de l'Agència Espanyola de Protecció de Dades.

VI

Encara en relació amb els fluxos d'informació que poden tenir lloc, cal fer una referència específica a la previsió de Google, en les seves condicions del servei *Google Apps for Business* de Google Ireland Limited, de transmetre la informació tractada a les "empresas del grupo" (punt 6 relatiu a la *"Información confidencial"*). Aquest tipus de transmissions de dades, tot i produir-se entre societats integrades en un mateix grup empresarial, s'han de considerar com una comunicació de dades (article 3.i) LOPD). Per tant caldria que concorri algun dels supòsits habilitants que preveu l'article 11 de la LOPD o bé que, si es tracta d'una comunicació per tal que una tercera empresa presti un servei per compte del responsable, s'estableixi el corresponent contracte de subencàrrec del tractament.

En qualsevol cas, i en la mesura que es duguin a terme fora de l'espai econòmic europeu constitueixen també transferències internacionals de dades. En aquest sentit, cal fer avinent que, per tal de considerar-les conformes amb la normativa de protecció de dades, caldrà comptar amb l'autorització prèvia del Director de l'Agència Espanyola de Protecció de Dades.

Aquesta autorització pot ser atorgada si, de conformitat amb allò establert a l'article 70.4 del RLOPD, el grup empresarial ha adoptat normes o regles internes en què constin les necessàries garanties de respecte per a la protecció de la vida privada i el dret fonamental a la protecció de dades dels afectats i si es garanteix, així mateix, el compliment dels principis i l'exercici dels drets que reconeix la LOPD i el RLOPD.

És necessari que aquestes regles corporatives, conegudes com *Binding Corporate Rules* (BCR), siguin vinculants per a totes les empreses del grup (article 137 RLOPD) i que s'hagi avaluat la conveniència de la seva adopció d'acord amb les previsions dels documents de treball elaborats en aquest sentit pel Grup de Treball de l'Article 29 de la

Directiva Europea 95/46/CE (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm).

Correspon a l'Agència Espanyola de Protecció de Dades decidir sobre l'adequació d'aquestes comunicacions a la normativa de protecció de dades.

D'altra banda, també convé fer una referència específica a la previsió continguda en aquestes condicions pel que fa a la participació d'empreses subcontractades en la prestació dels serveis *Google Apps for Business* (punt 13.3 relatiu a la *"Subcontractación"*).

En concret, s'estableix que *"cualquier parte puede subcontratar sus obligaciones bajo el Acuerdo, en su totalidad o en parte, sin el previo consentimiento por escrito de la otra parte, con la condición de que la parte subcontratante esté completamente sujeta a todas las obligaciones subcontratadas y acepte toda la responsabilidad existente entre las partes en relación con las acciones o la falta de acción de sus subcontratantes como si dichas acciones o falta de acción fueran propias".*

Aquesta previsió, tal i com està redactada, no donaria compliment a les previsions establertes en aquest sentit en la Disposició addicional vint-i-sisena del TRLCSP. Com s'ha apuntat en l'apartat II d'aquest dictamen, l'encarregat del tractament no pot subcontractar amb un tercer la realització de cap tractament que li ha encomanat el responsable del tractament de forma unilateral. Per contra, només és possible fer la subcontractació quan concorrin els requisits següents:

a) Que aquest tractament s'hagi especificat en el contracte signat per l'entitat contractant i el contractista.

b) Que el tractament de dades de caràcter personal s'ajusti a les instruccions del responsable del tractament.

c) Que el contractista encarregat del tractament i el tercer formalitzin el contracte en els termes previstos en l'article 12.2 de la Llei Orgànica 15/1999, de 13 de desembre.

Així mateix, d'acord amb allò establert al Dictamen 5/2012, d'1 de juliol, sobre el *Cloud Computing,* del Grup de Treball de l'Article 29 de la Directiva Europea 95/46/CE, en cas que existeixi un o varis subcontractistes caldria especificar el nom de cadascú en aquest contracte. Així mateix, el proveïdor dels serveis de "computació en el núvol" hauria de signar un contracte específic amb cada subcontractista en què es fixin totes les obligacions que el client (el responsable) ha imposat al proveïdor i que aquests també hauran de complir (apartats 3.3.2 i 3.4.2.7).

Només garantint el compliment d'aquestes condicions es podria admetre, des de la vessant de la protecció de dades, la participació d'empreses subcontractes en la prestació del servei *Google Apps for Business* a contractar pel Consell comarcal.

VII

Arribats a aquest punt és necessari fer referència a les mesures de seguretat que cal implementar per tal de garantir no només la confidencialitat, sinó també la integritat i la disponibilitat de la informació que sigui objecte de tractament amb la finalitat de garantir, en definitiva, el dret fonamental a la protecció de dades personals.

La normativa espanyola de protecció de dades personals imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9 LOPD).

Aquestes mesures de seguretat venen regulades en el Títol VIII del RLOPD, que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar, i tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors.

El conjunt d'aquestes mesures de seguretat comprèn:

a) Un document de seguretat que reculli les mesures de seguretat, tant tècniques com organitzatives, definides pel responsable del fitxer o tractament.
b) Registre d'incidències.
c) Control d'accés.
d) Gestió de suports i documents.
e) Mesures d'identificació i d'autenticació dels usuaris.
f) Còpies de seguretat i recuperació de les dades.
g) Responsable de seguretat.
h) Auditories de seguretat.
i) Control d'accés físic.
j) Registre d'accessos.
k) Mecanismes de xifratge, en cas de transmissió de les dades a través de xarxes públiques o xarxes sense fil de comunicacions electròniques.

En el cas d'un tractament de dades de tercers per compte del responsable, cal recordar que en el contracte d'encarregat han de quedar fixades quines d'aquestes mesures de seguretat en concret s'adoptaran (article 12.2 LOPD). En particular, quan l'encarregat del tractament presta els seus serveis en un entorn de "computació en el núvol", caldria acordar i detallar en aquest contracte d'encarregat la manera en què es donarà compliment a l'obligació de realitzar, si escau, auditories per verificar el compliment de les mesures de seguretat implementades en els sistemes d'informació, instal·lacions de tractament i emmagatzematge de dades (article 96 RLOPD). Així mateix, cal recordar que s'exigeix al responsable del tractament o fitxer (client) vetllar perquè l'encarregat del tractament compleixi les garanties per al compliment del que disposa el RLOPD en aquest sentit (article 20.2 RLOPD).

Ara bé, la complexitat del funcionament de la prestació de serveis de "computació en el núvol" fa que no sempre resulti fàcil definir o establir quines són aquestes mesures de seguretat que s'implementaran. Per exemple, és molt probable que en aquest àmbit es tractin alhora dades que requereixen un nivell de protecció diferenciat (bàsic, mitjà o alt) però que el proveïdor d'aquests serveis, per tal d'establir una oferta clara per a tots els seus clients, acabi aplicant unes mesures de seguretat homogènies. A més, probablement aquestes mesures estaran articulades d'acord amb estàndards diferents dels previstos en el RLOPD (com ara, les normes ISO).

Si s'examinen les condicions del servei *Google Apps for Business* de *Google Ireland Limited* (www.google.com/apps/intl/es/terms/premier_terms_ie.html) es pot comprovar que, en relació amb aquest extrem, s'estableix que:

> *1.5. Protección de datos. En el Apartado 1.4. y 1.5. del presente Acuerdo, los términos "datos personales", "procesar", "control de los datos" y "procesar los datos" reciben el significado que se estipula en la Directiva de la Unión Europea. A propósito de este Acuerdo y con respecto a los datos personales de los Usuarios finales, por el presente, las partes acuerdan que el Cliente será el encargado de realizar el control de los datos y Google el encargado de procesarlos. Google se compromete a aplicar las medidas técnicas y organizativas que correspondan para proteger estos datos personales ante la destrucción o pérdida accidental, modificación, revelación o acceso no autorizado, ya sea de forma accidental o ilegal."*

No obstant això, pel que fa a quines són aquestes mesures tècniques i organitzatives que en concret s'adoptaran no s'hi conté cap referència, sinó que cal acudir al citat llistat de preguntes i respostes sobre seguretat i privacitat en relació amb els serveis de *Google Apps* (http://support.google.com/a/bin/answer.py?hl=es&answer=60762).

En aquest llistat s'estableix que disposen d'un certificat de seguretat SAS 70 tipus II, de tal manera que un auditor independent extern ha comprovat que *Google Apps* aplica els següents controls i protocols:

> *"**Seguridad lógica:** los controles proporcionan una garantía razonable de que el acceso lógico a los sistemas de producción y a los datos de Google Apps está restringido a las personas autorizadas.*
> ***Privacidad:** los controles proporcionan una garantía razonable de que Google ha implementado políticas y procedimientos en torno a la privacidad de los datos de los clientes de Google Apps.*
> ***Seguridad física de los centros de datos:** los controles proporcionan una garantía razonable de que los centros de datos donde se aloje la información de Google Apps y las oficinas corporativas están protegidos.*
> ***Gestión de incidentes y disponibilidad:** los controles proporcionan una garantía razonable de que los sistemas de Google Apps son redundantes y de que los incidentes se notifican, se responden y se graban correctamente.*
> ***Gestión de cambios:** los controles proporcionan una garantía razonable de que el desarrollo de Google Apps y las modificaciones que se aplican a este servicio se someten a pruebas y a revisiones de código independientes antes de su lanzamiento.*
> ***Organización y administración:** los controles proporcionan una garantía razonable de que la administración ofrece la infraestructura y los mecanismos necesarios para realizar el seguimiento de las iniciativas de la empresa que afectan a Google Apps y para comunicarlas."*

Tot seguit, en aquest mateix llistat s'assegura, entre d'altres aspectes, que:

- L'accés al centres de processament de dades es limita a aquells treballadors de Google que gaudeixen de la corresponent autorització.
- Tots els comptes d'usuari estan protegits mitjançant un cadenat virtual que garanteix que un usuari no pot veure les dades d'un altre.
- En cas de detectar-se un error de seguretat en una aplicació o en un component de la infraestructura, avaluen el risc i actuen en conseqüència.
- Les dades es dupliquen varis cops en els servidors actius en clúster de Google perquè, en cas d'error en una màquina concreta, es pugui accedir mitjançant un altre sistema.
- Tots els servidors ofereixen la possibilitat d'accedir a les dades mitjançant procediments d'encriptació.
- Compten amb eines de bloqueig de l'*spam*, així com de detecció de virus.
- Ofereix la connectivitat mitjançant el protocol SSL (*Secure Sockets Layer*), el qual permet establir comunicacions segures en Internet.
- Aplica a tots els seus sistemes d'informació la Llei federal dels Estats Units de protecció de la informació de 2002 o FISMA (*Federal Information Security Management Act*).

Si bé, en la mesura que l'empresa Google afirma adoptar normes tècniques reconegudes per assegurar les dades del seus clients, cal valorar aquestes previsions de manera positiva, cal fer avinent que la normativa espanyola vigent en aquesta matèria és clara en establir la necessitat de donar compliment a les previsions establertes en el RLOPD, per la qual cosa és possible que les mesures adoptades per Google en aquest sentit, tot i ser adequades, resultin insuficients.

Així mateix, el responsable haurà de tenir present que, més enllà del compliment de les previsions del RLOPD, també haurà de donar compliment a allò disposat en el

Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

VIII

Finalment, es considera convenient fer unes consideracions addicionals en relació, encara, amb les condicions establertes pel servei *Google Apps for Business.*

En l'apartat *"Definiciones"* del *"Acuerdo de Google Apps for Business de Google Ireland Limited"* (www.google.com/apps/intl/es/terms/premier_terms_ie.html) –previsió també contemplada en el "*Acuerdo de Google Apps for Business (online)"* (www.google.com/apps/intl/es/terms/premier_terms.html)-, s'estableix que *"información confidencial hace referencia a la información divulgada por una parte a la otra parte bajo el Acuerdo, que está marcada como confidencial o que, a partir de su naturaleza, de su contenido o de las circunstancias en las que se divulga, puede suponerse razonablemente que es confidencial".*

Cal fer avinent, en aquest sentit, que l'objecte de protecció del dret fonamental a la protecció de dades personals (article 18.4 CE) no es redueix només a aquelles dades que puguin marcar-se com a "confidencials", sinó que engloba qualsevol tipus de dades personals, fins i tot aquelles que, pel fet de ser públiques, puguin ser conegudes per qualsevol persona. És a dir, les dades emparades per aquest dret són totes aquelles que identifiquin o permetin identificar una persona física *"pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo* (STC 292/2000, de 30 de novembre, FJ 6).

Per tant, totes aquelles dades personals que el Consell Comarcal faciliti a Google Ireland Limited per a la prestació del seu servei de *Google Apps for Business* estan sotmeses al deure de secret (art. 10 LOPD) i tenen aquest caràcter de "confidencial".

D'altra banda, convé assenyalar la previsió establerta en l'apartat *"Declaraciones, garantías y renuncia de responsabilidades"* del "*Acuerdo de Google Apps for Business (online)" (*www.google.com/apps/intl/es/terms/premier_terms.html). En la primera part d'aquest apartat s'estableix que *"en la medida en que la ley lo permita, a menos que quede expresado de otro modo en este documento, ninguna de las partes ofrece ninguna otra garantía de ningún tipo, implícita ni explícita, obligatoria ni de otra clase incluidas, sin limitarse a ello, las garantías de comerciabilidad, adecuación para un fin particular y no infracción".*

Per tant, a l'hora de contractar els serveis de *Google Apps for Business*, cal tenir en compte que, pel que fa al tractament de dades personals, Google només es compromet a complir aquelles previsions que s'hagin fixat en l'acord subscrit i en els termes que s'hagin indicat, unes previsions que, com s'ha fet esment al llarg d'aquest dictamen, podrien resultar no suficients des de la vessant del dret a la protecció de dades personals.

Així mateix, no és sobrer assenyalar què succeiria en cas de desacord o conflicte sobre alguna de les previsions establertes en el contracte de prestació del servei *Google Apps for Business.*

D'acord amb l'apartat *"Otras disposiciones"* de *"Acuerdo de Google Apps for Business de Google Ireland Limited"* (www.google.com/apps/intl/es/terms/premier_terms_ie.html), qualsevol desacord (contractual o no) que se susciti en relació amb l'acord subscrit es regirà pel dret anglès. Ara bé, segons el "*Acuerdo de Google Apps for Business (online)" (*www.google.com/apps/intl/es/terms/premier_terms.html), el dret aplicable en aquests casos serà el de Califòrnia.

Cal tenir en compte, per tant, que en cas d'existir un desacord entre el client (Consell Comarcal) i Google sobre els termes i o les condicions de l'acord subscrit per a la prestació d'aquest servei, la normativa aplicable en cap cas seria l'espanyola. Tot això sens perjudici que els ciutadans espanyols les dades dels quals siguin tractades pel Consell Comarcal tenen dret a què aquest organisme, i també els que intervinguin per compte seu, tractin les seves dades personals d'acord amb el que estableixen la LOPD i el RLOPD.

IX

Tenint en compte les consideracions fetes fins ara pel que fa als riscos que "la computació en el núvol" pot comportar per a la seguretat i integritat de la informació personal i, en concret, els que es poden derivar d'un tractament en un "núvol" públic (com és el cas dels serveis *Google Apps for Business)*, i atès el volum de dades personals, fins i tot de caràcter més sensible, que les administracions públiques empren per dur a terme les seves funcions, cal fer avinent que, des de la vessant del dret a la protecció de dades de caràcter personal, els models de "computació en el núvol" privat i/o comunitari podrien resultar una opció més adequada, atès que ofereixen un major grau de control sobre el tractament de les dades realitzat pel proveïdor d'aquests serveis (l'encarregat).

Si bé l'opció d'utilitzar un "núvol" públic podria resultar més satisfactòria *a priori* pel responsable del tractament, en la mesura que es tracta de serveis més flexibles i rentables, la seva contractació s'ha d'efectuar, en qualsevol cas, garantint el control de la informació per part de l'administració responsable, analitzant els riscos que en cada cas es puguin derivar i assegurant que es reuneixen tots els requisits legalment establerts.

En qualsevol cas, seguint les recomanacions fetes pel Grup de Treball de l'Article 29 de la Directiva Europea 95/46/CE en el seu Dictamen 5/2012, d'1 de juliol, sobre el *Cloud Computing,* es recomana al Consell Comarcal que, com a bona pràctica, informi als titulars de les dades sobre les circumstàncies en què seran tractades les seves dades personals, sobre la identitat del proveïdor dels serveis de "computació en el núvol" i, si escau, dels subcontractistes, així com del lloc en què s'emmagatzemaran i tractaran les seves dades (apartat 3.4.1.1).

D'acord amb les consideracions fetes en aquest dictamen en relació amb la consulta plantejada, es fan les següents,

Conclusions

La contractació dels serveis *Google Apps for Business* per part del Consell Comarcal requereix la realització d'un anàlisi previ dels riscos que per a la seguretat i integritat de la informació personal pot comportar el seu tractament en entorns que operen en el "núvol".

En la mesura que Google Ireland Limited efectuï un tractament de dades per compte del Consell Comarcal, la contractació dels seus serveis *Google Apps for Business* requereix, d'entrada, la signatura d'un contracte d'encarregat del tractament amb els termes establerts a l'article 12 de la LOPD.

No obstant això, ateses les condicions a què se sotmet el servei *Google Apps for Business,* el Consell Comarcal ha de tenir present que l'existència d'aquest contracte d'encarregat per si sol no pressuposa que el tractament de les dades per Google

Ireland Limited es dugui a terme sempre amb totes les garanties exigides per la normativa espanyola de protecció de dades de caràcter personal.

Sens perjudici que el Consell Comarcal, com a responsable del tractament o fitxer, pugui decidir lliurement amb qui contractar la prestació d'aquests serveis, des de la vessant de la protecció de dades personals, resulten més adequats altres models de "computació en el núvol", com ara, els de tipus privat o comunitaris.

Barcelona, 4 de juliol de 2012