Dictamen sobre una consulta formulada per una organització en relació amb la contractació dels sistemes de correu al núvol de *Google Apps* i de *Microsoft Office 365*.

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una organització en què es demana el parer de l'Autoritat sobre si la contractació dels sistemes de correu en el núvol de *Google Apps* o de *Microsoft Office 365* vulneraria la normativa de protecció de dades personals.

Analitzada la petició, vista la normativa vigent aplicable, l'informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat i l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

L'organització sol·licita, en el seu escrit de consulta, el parer d'aquesta Autoritat sobre si la contractació dels sistemes de correu electrònic en el núvol mitjançant *Google Apps* o *Microsoft Office 365* podria vulnerar la normativa de protecció de dades personals, tenint en compte que les empreses proveïdores d'aquests serveis estan subscrites a l'acord "U.S.-E.U. Safe Harbor" i el fet que no es presten a negociar contractes d'encarregat del tractament.

Per tal de donar resposta a aquesta qüestió, es considera necessari analitzar quins són els riscos que, per a la seguretat i la integritat de la informació, pot comportar l'ús d'aquests serveis. En aquest sentit, i per tal de facilitar la comprensió del present dictamen, s'ha optat per dur a terme aquesta anàlisi de manera diferenciada, tal com s'indica a continuació:

- Els fluxos d'informació i l'adhesió de les empreses proveïdores dels serveis *Google Apps* i *Microsoft Office 365* als principis de l'acord "U.S.-E.U. Safe Harbor".
- El principi de qualitat de les dades en la prestació dels serveis *Google Apps for Business* i *Microsoft Office 365*.
- Les mesures de seguretat adoptades per les empreses proveïdores d'aquests serveis.
- La seguretat proporcionada específicament per les aplicacions d'accés al seu servei de correu electrònic.

Abans d'efectuar aquesta anàlisi però, es fan algunes consideracions prèvies pel que fa a la naturalesa d'aquests serveis, la necessitat d'establir un contracte d'encarregat del tractament amb les empreses proveïdores d'aquests serveis, i sobre les conseqüències derivades de l'existència d'una transferència internacional de dades.

Així mateix, es considera necessari fer referència, en el darrer apartat d'aquest dictamen, als mecanismes establerts per a la resolució de possibles conflictes, atès que, des del punt de vista de la protecció de dades personals, es tracta d'un aspecte també rellevant en la prestació d'aquests serveis.

III

Els serveis *Google Apps* i *Microsoft Office 365*.

D'acord amb la informació disponible a la pàgina web de l'empresa Google, *Google Apps* és *"un paquete de productividad basado en la nube que te ayuda a ti y a tu equipo a conectaros y a trabajar desde cualquier lugar y dispositivo"* que s'ofereix a diversos col·lectius: empreses (*Google Apps for Business*), centres educatius (*Google Apps for Education*) i organitzacions governamentals (*Google Apps for Government*).

Google Apps for Business comprèn l'ús de diverses eines de comunicació i col·laboració senzilles i eficaces en línia (com ara, *Gmail, Google Calendar, Google Drive,* etc.) 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.

D'acord amb la informació disponible a la pàgina web de l'empresa Microsoft, *Microsoft Office 365* és *"una solución de comunicación y colaboración en la nube"* que s'ofereix també, mitjançant una sèrie de "plans", a diversos col·lectius: empreses, organitzacions governamentals, institucions educatives, organitzacions sense ànim de lucre, o bé a nivell personal.

Aquest producte per a empreses incorpora també un gran nombre d'eines de comunicació i col·laboració senzilles i eficaces en línia (com ara, *Office Professional Plus* –Excel, Word, PowerPoint i Outlook-, *Exchange Online* –correu electrònic empresarial amb calendaris d'ús compartit, correu de veu i missatgeria unificada-, etc.).

Així doncs, el servei de correu electrònic a què es fa referència en l'escrit de consulta forma part del conjunt d'eines que les empreses Google i Microsoft posen a disposició dels seus clients-usuaris a través de la contractació, respectivament, dels seus productes *Google Apps for Business* i *Microsoft Office 365*.

Per tant, amb independència que en el cas examinat es pretengui emprar únicament el servei de correu electrònic –així sembla desprendre's de les manifestacions efectuades en l'escrit de consulta-, s'entén que l'objecte de la contractació comprèn la totalitat d'eines o d'aplicacions incloses en *Google Apps for Business* i *Microsoft Office 365*.

Tal com ha posat de manifest aquesta Autoritat en dictàmens anteriors (CNS 24/2012 sobre la contractació, precisament, dels serveis *Google Apps for Business* i CNS 57/2013 sobre els riscos derivats de l'ús dels serveis de *cloud storage*, ambdós disponibles al web de l'Autoritat www.apd.cat), la contractació d'aquests serveis TIC tipus *cloud computing* o "computació 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 el responsable del fitxer o tractament com 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".*

En l'àmbit de la "computació en el núvol", s'entén que els clients-usuaris d'aquests serveis 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 atès que, en la mesura que decideixen dur a terme la seva contractació, són els qui decideixen la finalitat, el contingut i l'ús del tractament d'aquestes dades.

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, per tant, la posició jurídica de l'empresa o entitat que contracta *Google Apps for Business* o *Microsoft Office 365* és la de responsable del fitxer o tractament, mentre que les empreses proveïdores d'aquests serveis –Google i Microsoft - adoptarien la postura d'encarregats del tractament.

Sent així, la transmissió d'informació personal des de l'entitat de què es tracti a les empreses Google o Microsoft, que inclourà no només les dades dels seus treballadors sinó probablement també, atès l'àmbit en què duen a terme les seves funcions, dades de ciutadans (fins i tot, podria ser el cas de dades de caràcter sensible (article 7 LOPD)), no tindria 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 fos possible caldrà que se celebri un contracte d'encarregat del tractament (article 12.2 LOPD), 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.

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 els seus articles 20, 21 i 22.

Per tant, per tal de donar compliment a la normativa de protecció de dades personals en la contractació dels serveis oferts mitjançant *Google Apps for Business* o *Microsoft Office 365* (com ara el correu electrònic), com se sol·licita en l'escrit de consulta, és necessari, d'entrada, subscriure un **contracte d'encarregat del tractament** amb el contingut mínim determinat en aquests preceptes.

Ara bé, tal i com posa de manifest l'entitat consultant i així ho ha afirmat aquesta Autoritat en els citats dictàmens CNS 24/2012 i CNS 57/2013, 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, atesa la pèrdua constatada del poder de disposició i de control sobre les dades personals –nucli essencial del dret fonamental a la protecció de dades (STC 292/2000, de 30 de novembre)- que experimenta el responsable en el món de la "computació en el núvol", sovint fruït de la impossibilitat de negociar amb les empreses proveïdores d'aquests tipus de serveis el contingut de l'esmentat contracte d'encarregat.

Per aquest motiu, i atès que correspon al 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 (article 20.2 RLOPD), és necessari que l'entitat faci una anàlisi prèvia de l'impacte de la contractació dels serveis *Google Apps for Business* i *Microsoft Office 365* en la privacitat, amb especial atenció als **riscos per a la seguretat i la integritat de la informació**, així com que esculli un proveïdor que 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/files/2012/wp196_en.pdf).

Cal dir que, en relació amb l'anàlisi d'aquests riscos, en l'escrit de consulta es fa menció, com s'ha avançat, al fet que les empreses proveïdores d'aquests serveis estan adherides als principis de l'acord "U.S.-E.U. Safe Harbor". Aquest aspecte s'analitza de manera diferenciada en els apartats següents d'aquest dictamen, prenent com a referència les respectives condicions d'ús dels serveis *Google Apps for Business* (http://www.google.com/apps/intl/es/terms/premier_terms.html) i *Microsoft Office 365* (http://windows.microsoft.com/es-es/windows/microsoft-services-agreement) vigents en el moment en què s'ha plantejat la consulta. Cal fer però unes consideracions prèvies al respecte:

Les condicions d'ús dels serveis *Google Apps for Business* examinades per aquesta Autoritat en el Dictamen CNS 24/2012 a què s'ha fet referència només són d'aplicació a les contractacions d'aquests serveis efectuades amb anterioritat al 6 de desembre de 2012, data en què Google va deixar d'oferir-los de manera gratuïta. Atès el temps transcorregut des de l'emissió del citat dictamen, així com el fet que aquestes condicions han patit variacions, es considera pertinent analitzar-les novament.

Les condicions d'ús dels serveis *Google Apps for Business* i *Microsoft Office 365* examinades contenen diversos enllaços amb remissions a altres aspectes que també s'han de tenir en compte a l'hora de contractar els serveis, algunes d'especial transcendència per a la protecció de dades personals, com ara, la política de privacitat emprada o les mesures de seguretat aplicades.

Per exemple, Microsoft ofereix als seus clients que contractin els serveis *Microsoft Office 365* una sèrie de garanties contractuals addicionals mitjançant la signatura dels *"acuerdos de procesamiento de datos (DPA)"*. Ara bé, per tal de conèixer aquesta possibilitat, cal consultar la informació establerta en aquest sentit al "Centro de confianza de Microsoft Office 365" (http://office.microsoft.com/ca-es/business/centro-de-confianza-office-365-seguridad-informatica-FX103030390.aspx).

Segons manifestacions de Microsoft, el DPA aborda la privacitat, seguretat i tractament de les dades del client i li permet donar compliment a les regulacions locals. Apuntar, en aquest sentit, que, atès que per tal d'accedir a aquest document és necessari disposar de les credencials d'inici de sessió d'administrador d'Office 365, no s'ha pogut examinar la seva adequació a la normativa espanyola de protecció de dades.

Tal com admeten les mateixes companyies, qualssevol d'aquestes condicions i, especialment, les relatives a la privacitat poden ser modificades en qualsevol moment sense necessitat de notificar-ho prèviament als seus clients-usuaris, tret que es consideri, a criteri de la mateixa companyia, que la revisió pot afectar de manera significativa els seus drets.

Un exemple d'aquesta modificació unilateral el trobem en la companyia Microsoft. En el transcurs de l'elaboració del present dictamen Microsoft ha anunciat una actualització del contracte de serveis i de la política de privacitat. Les dites actualitzacions està previst que entrin en vigor el proper 31 de juliol de 2014.

Aquests fets posen de manifest la dificultat existent en aquest àmbit per determinar quines són les condicions exactes de la prestació d'aquests serveis i a les que se sotmetrà, en concret, l'entitat, com a responsable del tractament, amb la seva contractació. És a dir, dificulten l'anàlisi prèvia dels riscos per a la seguretat i la integritat de la informació derivats, en aquest cas, dels serveis *Google Apps for Business* i *Microsoft Office 365*, a què es fa referència a continuació.

IV

Els fluxos d'informació i l'adhesió de les empreses proveïdores d'aquests serveis als principis de l'acord "U.S.-E.U. Safe Harbor".

Tenint en compte el funcionament propi d'aquests serveis que operen en el núvol, basat en un emmagatzematge de la informació en diversos servidors en centres de processament de dades, un risc que pot amenaçar la seguretat de les dades personals i que l'entitat com a responsable ha de tenir en compte abans de dur a terme la contractació dels serveis *Google Apps for Business* o *Microsoft Office 365* és el de la deslocalització de les dades. 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 que aquest vulneri la normativa de protecció de dades.

És possible que la contractació d'aquests serveis 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).

Veiem, a continuació, què es preveu al respecte per als serveis *Google Apps for Business* i *Microsoft Office 365:*

- D'acord amb les condicions d'ús del servei *Google Apps for Business* (http://www.google.com/apps/intl/es/terms/premier_terms.html), la contractació d'aquest servei pel client-usuari (l'entitat) es duria a terme amb l'empresa Google Inc., el domicili social de la qual està ubicat a Califòrnia, als Estats Units. Tot i no fer-hi referència, no es pot descartar, atès els supòsits examinats en els dictàmens CNS 24/2012 i CNS 57/2013, que la contractació tingués lloc amb una de les seves filials, en concret, amb Google Ireland Limited.

Sent així, es podria pensar que la transmissió de les dades personals per l'entitat a Google 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 s'examina la seva política de privacitat (http://www.google.com/intl/es/policies/privacy/) es pot comprovar que l'empresa Google preveu tractar les dades personals en els seus servidors que estan ubicats en diferents països del món i reconeix, alhora, que aquest tractament pot fer-se en un servidor que no estigui ubicat en el país de residència del client (apartat "*Cómo utilizamos los datos recogidos*").

D'acord amb la informació facilitada a la pàgina web http://www.google.com/about/datacenters/inside/locations/index.html, Google disposa de centres de processament de dades en 14 localitzacions repartides en tres continents diferents: Amèrica, Àsia i Europa.

- Pel que fa als serveis *Microsoft Office 365*, d'acord amb les seves condicions d'ús (http://windows.microsoft.com/es-es/windows/microsoft-services-agreement), la contractació pel client-usuari (l'entitat) es duria a terme amb la companyia Microsoft Corporation o, segons on resideixi el client, amb una de les seves filials. En aquest sentit, s'assenyala que, si el lloc de residència es troba a Europa –com succeiria en aquest cas-, la relació contractual s'estableix amb Microsoft Luxembourg S.à.r.l. (apartat 12 "*Entidad contratante de Microsoft*"). Aquest aspecte no ha sofert modificacions en les condicions d'ús que entraran en vigor el proper 31 de juliol de 2014.

Per tant, també es podria pensar que la transmissió de les dades personals per l'entitat a Microsoft 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 s'examina la seva política de privacitat (http://www.microsoft.com/online/legal/v2/?docid=22&langid=es%2Des) es pot comprovar com la companyia preveu emmagatzemar i tractar la informació personal recopilada en els Estats Units o en un altre país en què Microsoft o les seves filials, societats del grup o proveïdors de serveis disposin d'instal·lacions (apartat *"Ubicación de los datos"*), sense concretar quines són aquestes empreses i on es troben ubicades físicament.

Per esclarir aquest aspecte, cal acudir a l'apartat *"Dónde estan mis datos"* del *"Centro de Confianza de Microsoft Office 365*" (http://www.microsoft.com/online/legal/v2/?docid=25&langid=es%2Des), pàgina web a què remet la política de privacitat de *Microsoft Office 365*. D'acord amb aquest apartat, Microsoft preveu emmagatzemar i tractar les dades en servidors ubicats, per a clients de la Unió Europea, a Irlanda i als Països Baixos, així com també als Estats Units, entre d'altres possibles zones geogràfiques que insisteix no poder revelar.

Ateses aquestes previsions, cal 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 pel client-usuari (l'entitat) a les empreses Google o Microsoft –que, atès l'àmbit en què du a terme les seves funcions, probablement inclourà dades de caràcter sensible (article 7 LOPD), en concret, dades relatives a la salut (article 5.1.g) RLOPD)- 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 previstes a l'article 34 LOPD i l'article 70 RLOPD, 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 l'acord "U.S.-E.U. Safe Harbor",** d'acord amb la Decisió 2000/520/CE de la Comissió de 26 de Juliol de 2000. Entre elles hi trobem, tal i com s'assenyala en l'escrit de consulta, les empreses Google i Microsoft, 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 client-usuari (l'entitat) a Google o Microsoft, 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.

Ara bé, dit això, cal tenir en compte que, tal com ha reiterat aquesta Autoritat en dictàmens anteriors (CNS 24/2012 i CNS 57/2013), sovint l'aplicació d'aquests principis de l'acord Safe Harbor pot ser insuficient 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.

En aquests casos, cal tenir en compte que l'adhesió a l'acord Safe Harbor 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).

En aquest sentit, cal fer avinent que, si bé les empreses proveïdores examinades informen, per mitjà de la seves polítiques de privacitat, de la seva adhesió als principis de l'acord Safe Harbor, el dit acord no abasta la resta de zones geogràfiques en què podrien ubicar-se els seus servidors (o els de tercers).

Així mateix, 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), la NSA (*National Security Agency*) 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.

De fet, diverses revelacions d'espionatge a gran escala sorgides en els darrers mesos (com ara, entre d'altres, el funcionament dels programes PRISMA, *Evil Olive, Shell Trumpet* o *Fairview*) han evidenciat pràctiques de recopilació massiva i indiscriminada de dades per part dels Estats Units, justificades per raons de seguretat, que han comportat –i comporten- la vulneració de drets fonamentals dels ciutadans, com ara, el dret a la intimitat i el dret a la protecció de dades personals.

Cal tenir present que, a conseqüència d'aquests fets, les autoritats europees han sol·licitat, entre d'altres aspectes, una revisió dels principis de l'acord Safe Harbor a què es fa referència en aquest dictamen, per tal d'augmentar la transparència i el control de les empreses que hi estan adherides i, sobretot, per tal de limitar al màxim les excepcions que permeten a les autoritats nord-americanes accedir a les dades personals per motius de seguretat.

Un exemple en aquest sentit el trobem en la Comissió Europea que ha elaborat els documents *"El funcionament dels principis de Port Segur des de la perspectiva dels ciutadans i les empreses de la UE"* (disponible al web http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0847:FIN:EN:PDF) i *"El restabliment de la confiança en les transferències de dades entre la UE i els Estats Units"* (també disponible al web http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:EN:PDF).

La Comissió ha constatat que, en la mesura que els programes de supervisió nord-americans afectin dades emmagatzemades en el núvol a les quals resulti d'aplicació la legislació europea sobre protecció de dades, facilitar-les a les autoritats dels Estats Units, sense complir els requisits previstos en aquesta legislació, suposarà la infracció de la dita legislació –així com de la nacional aplicable-, fins i tot, per a aquells que siguin encarregats del tractament. Considera, en aquest sentit, que les excepcions previstes en

el marc dels principis de Safe Harbor no permeten extreure'n una conclusió diferent (la Comissió assenyala expressament la preocupació existent entorn a empreses com Google i Microsoft, entre d'altres, atès l'elevat nombre d'usuaris de què disposen).

Cal destacar, fruït d'aquesta situació, la decisió adoptada pel govern nord-americà amb la voluntat de reformar, tal com s'ha exigit, els mètodes de recopilació d'informació per part de la NSA, amb la finalitat de garantir un millor control judicial i reduir els riscos d'un ús inapropiat d'aquesta informació (www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf).

Tot i així, el Parlament Europeu, en una recent resolució, ha instat la Comissió Europea i els vint-i-vuit països de la Unió Europea a què suspenguin l'acord Safe Harbor, atès que considera demostrat que les empreses que hi estan adherides incompleixen l'obligació de protegir la privacitat de les dades que, en virtut d'aquest acord, poden transferir des de la Unió Europea als Estats Units.

Aquests fets evidencien que, com s'ha dit, l'adhesió de les empreses Google i Microsoft als principis de l'acord Safe Harbor podria resultar insuficient en l'àmbit examinat. Ara bé, a data d'avui i en la mesura en què aquest acord continua vigent, la dita adhesió pressuposa un tractament de les dades personals amb certes garanties i condicions de seguretat.

En aquest punt, cal fer esment a l'actuació duta a terme per l'empresa Microsoft.

Aquesta empresa, conscient que part dels seus clients necessiten majors garanties que les proporcionades per l'adhesió a l'acord Safe Harbor, es compromet a signar amb ells les clàusules contractuals tipus establertes per la Comissió Europea en la seva Decisió 2010/87/UE de 5 de febrer de 2010 (apartat "*cumplimiento normativo*" del "*Centro de Seguridad de Microsoft Office 365*").

D'acord amb la normativa de protecció de dades, en aquells supòsits en què sigui necessària l'autorització del Director de la Agència Espanyola de Protecció de Dades per a les transmissions de dades fora del territori de l'EEE, la dita autorització pot ser atorgada si el responsable del fitxer o tractament aporta un contracte escrit, subscrit entre l'exportador i l'importador, en què constin les necessàries garanties de respecte per la protecció de la vida privada dels afectats i els seus drets i llibertats fonamentals i es garanteix l'exercici dels seus drets respectius (articles 33 LOPD i 70.2 RLOPD).

En aquest sentit, cal assenyalar que el darrer 9 de maig de 2014, el Director de l'Agència, per mitjà de la Resolució TI/00032/2014 (disponible al web de l'Agència www.agpd.es), ha considerat **adequades les garanties establertes en els models de contracte per a la transferència internacional de dades amb destinació a Microsoft Corporation**, establerta als Estats Units, amb motiu de la prestació dels serveis *Microsoft Online Services* (entre ells, *Office 365*) i actuant com encarregat del tractament.

Així doncs, d'acord amb aquesta Resolució, caldrà considerar autoritzades les transferències internacionals de dades amb destinació als Estats Units que es realitzin a l'empara de les dites clàusules, sempre que, tal com s'estableix en ella, es doni compliment a les condicions següents:

> *"1. La finalidad de la transferencia será la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) por parte de MICROSOFT CORPORATION, actuando como encargado del tratamiento. Los datos se transfieren en las condiciones y con todas las garantías reseñadas en los Fundamentos de Derecho anteriores.*
> *2. La autorización sólo podrá entenderse concedida en caso de que el contrato firmado entre los responsables exportadores de los datos y MICROSOFT CORPORATION incorpore la totalidad de los documentos que se han aportado para*

la adopción de la presente resolución para cada uno de los servicios a los que la misma se refiere.
3. El exportador de datos deberá notificar al RGPD los ficheros cuyos datos vayan a ser objeto de transferencia internacional con carácter previo, con indicación de su denominación y código de inscripción en el RGPD, indicando que se producirá la transferencia internacional de los datos al amparo de la presente resolución.
4. El alcance de la transferencia internacional de datos que se lleve a cabo deberá resultar ajustado a la estructura del fichero, categorías de datos y finalidades del tratamiento establecidas en la inscripción del correspondiente fichero.
5. El exportador de datos deberá poner a disposición de la AEPD, cuando le fueran requeridos, los contratos de prestación de servicios que haya suscrito con MICROSOFT IRELAND OPERATIONS LIMITED (MIOL) y MICROSOFT CORPORATION.
6. La autorización de transferencia internacional podrá denegarse o suspenderse cuando concurra alguna de las circunstancias recogidas en el artículo 70.3 del RLOPD; es decir:
a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en las cláusulas contractuales aportadas.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados."

Per tant, als efectes que interessen en el present cas, cal tenir present que la contractació del servei *Microsoft Office 365* per l'entitat de què es tracti resultarà, en aquest sentit, conforme amb la normativa espanyola de protecció de dades personals, sempre que es compleixin les condicions a què es fa referència en l'esmentada Resolució TI/00032/2014 del Director de l'Agència Espanyola de Protecció de Dades.

Convé destacar la importància de comptar amb aquesta autorització, atès que, com s'ha dit, no es pot descartar que en el present cas l'entitat contractant del servei transmeti a Microsoft informació personal de caràcter sensible (article 7 LOPD), fet que l'obliga, com a responsable, a extremar les precaucions per tal de garantir que la seva comunicació s'efectuï sempre amb ple respecte a la normativa de protecció de dades.

V

Relacionat amb l'apartat anterior relatiu als fluxos d'informació, es considera convenient fer, a continuació, una referència específica a les previsions incloses en les polítiques de privacitat dels serveis examinats relatives a la transmissió de la informació tractada a **empreses o societats del grup**:

- En el cas de *Google Apps for Business,* això es preveu en l'apartat *"Qué datos personales compartimos. Tratamiento externo*" de la política de privacitat.

- En el cas de *Microsoft Office 365*, això es pot deduir de les previsions establertes a l'apartat *"Compartir su información"* de la seva declaració de privacitat.

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 les transmissions de dades s'efectuïn des d'un país de l'EEE a una societat del mateix grup empresarial ubicada fora de l'EEE constitueixen també transferències internacionals de dades, tal com hem exposat. Caldrà, per tant, comptar amb l'autorització prèvia del Director de l'Agència Espanyola de Protecció de Dades, llevat que es doni alguna de les excepcions previstes als articles 34 LOPD i 70 RLOPD.

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, en aquest mateix apartat, una referència específica a les previsions contingudes en aquestes polítiques de privacitat pel que fa a la participació **d'empreses subcontractades** en la prestació dels serveis examinats:

- En el cas de *Google Apps for Business* s'estableix que *"proporcionamos información personal a nuestros afiliados o a otras personas o empresas de confianza para que lleven a cabo su procesamiento por parte de Google, siguiendo nuestras instrucciones y de conformidad con nuestra Política de privacidad, y adoptando otras medidas de seguridad y confidencialidad adecuadas."*

- En el cas de *Microsoft Office 365* s'estableix que "*en ocasiones, se contrata a otras compañías para prestar servicios (como el soporte técnico al cliente) en nuestro nombre. A tal efecto, podríamos proporcionar a estas compañías acceso a su información cuando sea necesario para cumplir su contrato. Estas compañías están obligadas a mantener la confidencialidad de su información y tienen prohibido utilizarla para ningún fin que no sea aquél por el que Microsoft las ha contratado."*

Cal tenir en compte que, de conformitat amb la normativa de protecció de dades, 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 (article 21 RLOPD). 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 LOPD.

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, els proveïdors dels serveis examinats haurien 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 del Dictamen).

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 serveis *Google Apps for Business* o *Microsoft Office 365* a contractar per l'entitat.

VI

El principi de qualitat de les dades en la prestació dels serveis *Google Apps for Business* i *Microsoft Office 365*.

Qualsevol tractament de dades personals 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).

En l'àmbit de la computació en el núvol aquest principi resulta igualment d'aplicació, per la qual cosa és necessari establir amb claredat la **finalitat** o finalitats concretes per a les quals seran tractades les dades personals per part de les empreses proveïdores 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).

D'acord amb la LOPD, aquesta finalitat del tractament de les dades ha d'establir-se de manera expressa en el contracte d'encarregat del tractament (article 12.2). Ara bé, en els casos com l'examinat, el més habitual és que la dita finalitat estigui establerta en les condicions d'ús del servei ofert per l'empresa que n'és proveïdora.

Per tant, l'entitat, abans de dur a terme la contractació dels serveis *Google Apps for Business* o *Microsoft Office 365*, ha d'examinar amb cautela dites condicions d'ús, per tal de tenir la seguretat que la seva acceptació no implica autoritzar a l'empresa proveïdora per a que tracti les dades personals (dades que, recordem, poden ser especialment protegides) amb finalitats diferents a aquella que va justificar la contractació del servei.

Doncs bé, si s'examinen, en aquest sentit, les previsions establertes en les condicions d'ús dels serveis *Google Apps for Business* o *Microsoft Office 365* es pot comprovar que es tracta d'unes condicions generals o estàndards que les companyies fixen de manera unilateral i que no deixen marge d'opció a l'usuari-client (l'entitat).

A més, contenen escasses previsions pel que fa a la **finalitat concreta** del tractament de les dades, limitant-se a establir una remissió a les respectives polítiques de privacitat, les quals, recordem, poden ser modificades en qualsevol moment (apartats *"Modificacions"* i *"Cambios en la presente declaración de privacidad"*, respectivament).

A banda d'aquest fet, cal assenyalar, pel que fa a *Google Apps for Business,* que es tracta d'una política de privacitat dissenyada per al conjunt de serveis prestats per Google i no així específicament per als serveis *Google Apps for Business*, de tal manera que les

previsions contemplades en ella podrien no encaixar amb el funcionament previst per a aquest tipus de servei.

A més, s'empra una terminologia imprecisa, expressions genèriques (tals com, "podran" o "és possible", entre d'altres), així com expressions ambigües (com ara, "millorar l'experiència de l'usuari") que donen lloc a una política de privacitat indeterminada i poc clara.

Tot això origina una evident incertesa sobre les condicions exactes en què les dades personals serien tractades per l'encarregat (Google) i, alhora, posa en evidència que el responsable (l'entitat) 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.

Dit això, si s'examinen, en concret, aquestes polítiques de privacitat a què ens remeten les condicions de servei pot comprovar-se que Google i Microsoft poden accedir a dades personals de què pugui disposar el client-usuari (l'entitat), ja sigui perquè les facilita directament, ja sigui perquè és Google o Microsoft qui les obté quan el client utilitza els seus serveis (dades del client, dades de l'administrador, dades del dispositiu emprat, dades de registre, dades sobre la ubicació física, *cookies* o identificadors anònims, etc.). La finalitat per a la qual es recullen aquestes dades sol coincidir en els proveïdors examinats: proporcionar i millorar el servei prestat.

Tot i que pugui ser raonable que el client (l'entitat) hagi d'acceptar necessàriament un cert nivell de tractament de les dades perquè això pot ser necessari, des d'un punt de vista tècnic, per a la pròpia prestació del servei, escau assenyalar que això no implica que resulti adequada la prestació d'un consentiment general, en el sentit d'una acceptació incondicionada, per utilitzar les dades del client (o de tercers) per a finalitats que no resultin estrictament necessàries per a la prestació de dit servei.

Es fa aquesta consideració en relació, en concret, amb el servei prestat per Google, atès que la finalitat del tractament de les dades al·legada per aquesta companyia (la prestació i millora del servei prestat) no és l'única finalitat pretesa.

Per exemple, en l'apartat "*Cómo utilizamos los datos recogidos"* de la seva política de privacitat, s'estableix que *"también utilizamos estos datos para ofrecerte contenido personalizado como, por ejemplo, resultados de búsqueda y anuncios más relevantes"* i concreta, més endavant, que només no preveu associar cookies o identificadors anònims quan es tracti de dades especialment protegides. Així mateix, afirma que pot *"combinar la información personal de un servicio con otro tipo de información, incluida información personal, de otros servicios de Google, por ejemplo, para que resulte más sencillo compartir información con las personas que conoces (...)."*

Però, a més, si es revisa les indicacions donades al "centre d'ajuda de Google Apps" pot comprovar-se que Google també estableix que *"nuestros sistemas exploran e indexan correos electrónicos y algunos otros datos de usuario para diversos fines. Esta exploración está completamente automatizada y no se puede desactivar. Por ejemplo, la exploración nos permite detectar spam y software malicioso, ordenar el correo electrónico para algunas funciones (p. ej., Prioritarios) y ofrecer con rapidez potentes resultados de búsqueda cuando los usuarios buscan información en sus cuentas. La exploración e indexación que nuestros sistemas llevan a cabo también nos permiten mostrar publicidad contextualmente relevante, incluso en Gmail. Si se inhabilitan los anuncios en tu dominio, no utilizaremos tus datos para mostrar publicidad a tus usuarios. En los dominios que utilizan la edición estándar de Google Apps, no se puede inhabilitar los anuncios."*

Pel que fa a les previsions de rebre anuncis personalitzats, escau assenyalar que s'ofereix tant la possibilitat de consultar i editar la informació relacionada amb les preferències d'anuncis, com l'opció d'inhabilitar la recepció d'aquests anuncis (apartat *"Transparencia y elección"* de la política de privacitat). Tot i valorar positivament aquests mecanismes,

escau assenyalar que la inhabilitació no implica deixar de rebre aquests anuncis, sinó rebre'ls de manera "*menos relevante".*

En relació, en concret, amb la previsió de combinar la informació personal, escau assenyalar que no determina en cap moment per a quins "altres usos" es combinarà la informació personal d'un servei amb la d'un altre. Es desconeix, així mateix, si això implica combinar la informació personal tramesa mitjançant el correu electrònic amb la d'altres serveis de què pogués disposar l'entitat.

Microsoft, per la seva part, ofereix informació més detallada sobre la finalitat del tractament de la informació recopilada tant en la seva política de privacitat com en el "Centro de confianza de Microsoft Office 365".

Així, assegura que les dades del client només s'empraran per a la prestació del servei, tret que l'usuari indiqui un altre ús. En aquest sentit, concreta que la prestació del servei pot incloure transaccions diàries, la resolució de problemes, la millora de les característiques del servei o dels requisits de manteniment (inclosa la detecció d'amenaces, tals com malware o spam) o la personalització del servei. Així mateix, i a diferència de Google, assegura no examinar els correus electrònics o els documents que s'hi adjunten amb fins publicitaris, previsió que s'inclou també en les condicions del servei actualitzades.

A la vista d'aquestes consideracions, cal tenir en compte, a l'hora de contractar els serveis examinats -especialment, el relatiu a *Google Apps for Business*-, que les actuacions previstes **poden excedir la finalitat principal** per la qual l'entitat li encarregaria el tractament de les dades. Destinar la informació personal a finalitats diferents de la que justificà la seva obtenció, així com combinar la informació personal obtinguda a través dels diversos serveis o productes que ofereixen per emprar-la amb múltiples finalitats que no es determinen amb claredat, comportaria una vulneració del principi de qualitat, en la seva vessant de finalitat (article 4.2 LOPD).

Encara relacionat amb el **principi de qualitat** de les dades esmentat, cal fer avinent que, en el cas d'un tractament de dades per compte del responsable, és recomanable que en el contracte d'encarregat s'estableixin previsions concretes sobre el **retorn o la destrucció** de les dades un cop complerta la prestació contractual (articles 12.3 LOPD i 22 RLOPD).

En relació amb aquest aspecte, cal dir que les condicions d'ús examinades són, segons el cas, poc precises o confuses al respecte:

- Google estableix que, en cas de rescissió del servei, *"proporcionarà al cliente acceso a los datos del cliente, así como capacidad de exportarlos, durante un periodo de tiempo comercialment raonable; tras un periodo de tiempo comercialmente razonable, Google eliminará los Datos del cliente mediante la supresión de redireccionamientos que hagan referencia a estos en los servidores activos de Google y sobrescribiéndolos conforme transcurra el tiempo; cada una de las partes aplicará de inmediato todos los esfuerzos comercialmente razonables para devolver o destruir cualquier otra Información confidencial de la otra parte, si así se solicita"* (apartat *"Rescisión"*), sense esclarir però quin és aquest període "comercialment raonable" previst.

- En el cas de Microsoft, existeix una disparitat de previsions al respecte en funció de si atenem les condicions d'ús del servei o bé allò establert al "Centro de confianza de Microsoft Office 365".

D'acord amb les condicions d'ús del servei vigents, en cas de cancel·lació del servei, Microsoft podrà *"eliminar su contenido de forma permanente de nuestros servidores, sin que exista ninguna obligación de que se lo devolvamos a usted"* (apartat *"Cancelación de Servicios"*), previsió que no pot considerar-se en cap cas adequada.

En les condicions d'ús actualitzades s'estableix una previsió de caire similar: "*si sus Servicios se cancelan, eliminaremos la información o el contenido (tal y como se define anteriormente) asociados con su cuenta Microsoft, o los desvincularemos de otra manera de usted y de su cuenta Microsoft, a menos que la legislación nos obligue a conservarlos, y no estamos obligados a devolverle el contenido"*.

Ara bé, a l'apartat *"Son sus datos"* del "Centro de confianza de Microsoft Office 365" s'estableix que *"tras la expiración o finalización de su contrato o suscripción de Office 365, Microsoft le proporcionará, de manera predeterminada, acceso limitado adicional para 90 días para exportar sus datos".*

Dit això, cal fer avinent que en dites condicions tampoc es fa cap referència al període de temps de **conservació** de la informació personal recollida, més enllà de la previsió genèrica, en les respectives polítiques de privacitat, d'estar obligats a conservar-la per motius legals o legítims relacionats amb l'activitat que desenvolupen.

En relació amb aquestes previsions, cal fer avinent que emmagatzemar i conservar dades personals per períodes de temps indeterminats o injustificats més enllà de les exigències que es deriven de les finalitats preteses en el moment de la recollida, com així sembla desprendre's, comportaria una vulneració del principi de qualitat (article 4.5 LOPD).

D'altra banda, en relació amb el principi d'exactitud, 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"* (apartat "*Cómo utilizamos los datos recogidos"*).

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).

VII

Les mesures de seguretat adoptades per les empreses proveïdores dels serveis *Google Apps for Business* i *Microsoft Office 365.*

Un dels eixos fonamentals de la normativa de protecció de dades és el compliment de 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 (articles 79 i següents).

En el cas d'un tractament de dades de tercers per compte del responsable, com l'examinat, cal recordar que en el contracte d'encarregat han de quedar fixades quines de les mesures de seguretat del RLOPD en concret s'adoptaran (article 12.2 LOPD).

Ara bé, és cert que la complexitat del funcionament de la prestació de serveis que operen 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.

En aquest sentit, escau apuntar que, en atenció a les funcions que duen a terme les entitats que es plantegen dur a terme la contractació de *Google Apps for Business* o *Microsoft Office 365*, és probable, com s'ha apuntat anteriorment, que algunes de les informacions personals trameses a Google o Microsoft siguin dades especialment protegides, és a dir, dades que la normativa protegeix de forma reforçada, com ara, dades personals relacionades amb la salut (articles 7.3 LOPD i 5.1.g) RLOPD). El tractament d'informació personal d'aquesta naturalesa comporta, d'acord amb l'article 81.3.a) del RLOPD, implementar, a més de les mesures de seguretat de nivell bàsic i mitjà, les mesures de nivell alt (articles 89 a 104 RLOPD).

Així mateix, és probable que aquestes mesures estiguin articulades d'acord amb estàndards diferents dels previstos en el RLOPD, com ara, en normes internacionals o en certificacions en matèria de seguretat informàtica.

Veiem, a continuació, quines previsions en matèria de seguretat contenen les condicions de servei i les polítiques de privacitat dels serveis examinats:

- En relació amb *Google Apps for Business*, les seves condicions de servei es limiten a establir que *"Google ha implementado como mínimo los sistemas y procedimientos estándar del sector para garantizar la seguridad y confidencialidad de los Datos del cliente, protegerlos contra amenazas o riesgos previstos para la seguridad o integridad de dicha información, y evitar accesos no autorizados e impedir su uso"* (apartat *"Servicios"*).

Per obtenir més informació al respecte, cal atendre a l'apartat *"Seguridad de los datos"* de la seva política de privacitat, d'acord amb el qual:

- Fan còpies de seguretat.
- Fan "esforços" per evitar l'accés no autoritzat a les dades.
- Xifren la transmissió de la informació mitjançant SSL.
- Tenen implantats mecanismes de verificació de l'accés en dues passes.
- Tenen implantades mesures de seguretat físiques per impedir l'accés als seus sistemes.
- Limiten l'accés d'empleats i de tercers que puguin tractar les dades per compte de Google, indicant que aquestes persones estan subjectes a estrictes obligacions de confidencialitat.

Si bé en aquest apartat de la política de privacitat podem trobar informació relacionada amb la seguretat, cal dir que la major part d'aquesta informació es tracta de declaracions d'intencions i de consells o orientacions per als usuaris. No hi ha una concreció sobre quins són els sistemes de xifrat utilitzats, ni on s'empren, ni expliciten si les infraestructures són pròpies o de tercers, ni tampoc informen sobre quines mesures de seguretat apliquen en cada cas o sobre si estan subjectes a certificacions de seguretat específiques. I és que el fet que es tracti d'una política de privacitat pensada en realitat per a tots els serveis oferts per Google no permet conèixer quines són les mesures tècniques i organitzatives que s'adoptaran, en particular, en els serveis *Google Apps for Business* per protegir la informació tractada.

Aquesta informació només es pot conèixer 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 els serveis de *Google Apps* (http://support.google.com/a/bin/answer.py?hl=es&answer=60762). D'acord amb aquest llistat, Google:

- Limita l'accés al centres de processament de dades a aquells treballadors que gaudeixen de la corresponent autorització.
- Protegeix tots els comptes d'usuari 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, avalua el risc i actua en conseqüència.
- Duplica les dades varis cops en els servidors actius en clúster 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.
- Compta amb eines de bloqueig de l'spam, així com de detecció de virus.
- Ofereix la connectivitat mitjançant el protocol SSL (*Secure Sockets Layer*) i TLS (*Transport Layer Security*), el qual permet establir comunicacions segures en Internet.
- Amb la contractació dels serveis de Google Apps, l'organització contractant pot designar un o diversos usuaris administradors de domini. Els administradors de domini poden gestionar els serveis de Google Apps de l'organització.
- 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).
- Disposa dels certificats de seguretat SSAE16 e ISAE 3402 tipus II, i SAS 70 tipus II, de tal manera que un auditor independent extern ha comprovat que Google Apps for Business 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 registran 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."*
- Disposa de la certificació ISO 27001, de tal manera que una entitat de certificació externa, independent i acreditada hauria auditat el seu Sistema de Gestió de Seguretat de la Informació (SGSI), determinant la seva conformitat amb l'estàndard ISO/IEC/27001, el seu grau d'implementació real i la seva eficàcia.

• Pel que fa a *Microsoft Office 365*, cal dir que en la seva política d'ús, si més no en relació amb els serveis *"Office.com, Microsoft Office 365 Hogar Premium, Microsoft Office 365 Universitarios y otros servicios de la marca Microsoft Office vinculados a este Contrato por medio de un Contrato complementario ("Servicios de Office"), Bing y MSN",* es recorda al client-usuari, i de manera reiterada, que ha de fer còpies de seguretat de la informació (apartats *"Contenido", "Cancelación de los Servicios" i "Interrupciones de los*

Servicios y respaldos"). Aquest aspecte no ha sofert modificacions en les condicions d'ús que entraran en vigor el proper 31 de juliol de 2014.

Per tant, el client (l'entitat) ha de tenir present que el mateix proveïdor reconeix no poder garantir la integritat i la conservació de les dades en la prestació d'aquests serveis, tal i com exigeix la normativa de protecció de dades personals (articles 94 i 102 RLOPD). Això, sens perjudici de les previsions que, en aquest sentit, s'hagin pogut establir en el *"acuerdo de procesamiento de datos"* (DPA), document al qual, recordem, aquesta Autoritat no ha tingut accés.

No s'explicita cap altra informació en relació amb les mesures de seguretat implantades per Microsoft en els seus serveis, més enllà de dir que s'esforcen en mantenir el serveis en funcionament -per tant, només una breu referència a la disponibilitat, òbviament del tot insuficient-, i de remetre's a la política de privacitat aplicable per obtenir més informació al respecte.

Si s'acudeix a la citada política de privacitat de *Microsoft Office 365*, aquesta remet al "*Centro de confiança de Office 365*", segons el qual:

- La seguretat està basada en l'aplicació de diferents capes de seguretat: física i lògica de les dades. Entre les mesures de seguretat aplicades a les diferents capes de seguretat, hi ha les d'evitar l'accés físic no autoritzat a les instal·lacions on resideixen els servidors que tracten les dades dels diferents serveis de *Microsoft Office 365*, evitar l'accés lògic no autoritzat als servidors i restringir i controlar l'accés a les dades dels usuaris per part del personal tècnic de Microsoft.
- Totes les dades emmagatzemades en els servidors de *Microsoft Office 365* estan xifrades usant el programari BitLocker (que utilitza l'algoritme de xifratge AES 128 o AES 256). Les dades en trànsit es xifren mitjançant SSL/TLS.
- Els usuaris poden fer servir tècniques de xifratge de documents o missatges de correu com RMS (Rights Management Service), S/MIME i Office 365 Message Encryption.
- Amb la contractació dels serveis de *Microsoft Office 365*, l'organització contractant pot designar un o diversos usuaris administradors que poden definir, entre d'altres aspectes, si l'usuari ha d'accedir amb una autenticació de diversos factors o des de quins tipus de dispositius pot accedir un determinat usuari.
- S'ha sotmès a auditories realitzades per tercers i pot proporcionar informes de tipus I i II de SSAE16.
- Disposa de la certificació ISO 27001.
- Compleix amb els requeriments de compliment i gestió del risc definits per la Cloud Security Alliance (CSA).
- Aplica a tots els seus sistemes d'informació la FISMA (Llei federal dels Estats Units de protecció de la informació), la FERPA (Llei de drets educacionals i privadesa de la família), així com la HIPAA BAA (llei aplicable a entitats d'atenció sanitària i que regeix l'ús, la confidencialitat i la protecció de la informació de salut protegida).

Si bé, en la mesura que, de la informació proporcionada, Google i Microsoft afirmen adoptar normes i mesures tècniques reconegudes per assegurar les dades dels seus clients-usuaris, es podrien valorar totes aquestes previsions examinades de manera positiva, no es pot obviar que aquests mateixos proveïdors també afirmen no poder fer-se responsables de la pèrdua d'informació ni poder garantir al 100% la seguretat de la informació emmagatzemada en els seus servidors.

Cal tenir present 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 tant, cal tenir en compte que és possible que les mesures adoptades per Google i Microsoft en relació amb el seus serveis *Google Apps for Business* i *Microsoft Office 365*, respectivament, tot i ser adequades, resultin insuficients.

Per aquest motiu, en el citat dictamen CNS 57/2013 es va concloure que, davant la mancança a data d'avui de cap certificació per a proveïdors de serveis en el núvol capaç de verificar, de manera específica, el compliment estricte de les mesures de seguretat previstes al RLOPD, als efectes de garantir el compliment de la normativa vigent en matèria de protecció de dades, és necessari que qualsevol certificació o estàndard internacional en matèria de seguretat de què puguin disposar aquests proveïdors (com ara, en aquest cas, els certificats de seguretat SSAE16, SAS 70 tipus II, FISMA o ISO 27001) s'acompanyi de l'**auditoria** prevista al RLOPD.

Recordar que és responsabilitat de l'entitat (com a responsable del tractament) vetllar perquè els proveïdors dels serveis examinats (com a encarregats del tractament) garanteixin la implementació de les mesures previstes al RLOPD (article 20.2 RLOPD).

VIII

La seguretat proporcionada específicament per les aplicacions d'accés al servei de correu electrònic de *Google Apps for Business* i *Microsoft Office 365.*

Un cop examinats els aspectes de seguretat global de *Google Apps for Business* i *Microsoft Office 365* convé analitzar, atesos els termes en què s'efectua la consulta, la seguretat implementada en les aplicacions que es poden fer servir per accedir, en concret, al seu servei de correu electrònic.

Aquest accés es pot produir de tres maneres: mitjançant el navegador "web", mitjançant el que s'anomena "aplicació d'escriptori" o "clients de correu" i mitjançant una aplicació per a dispositius "mòbils" (APPS).

- Accés mitjançant el navegador "web":

L'accés al correu electrònic tant de *Google Apps for Business* (conegut com Gmail) com de *Microsoft Office 365* a través de la corresponent aplicació "web" es fa mitjançant un canal segur basat en "https". Per tant, en ambdós casos, la informació serà tramesa de manera xifrada entre el servidor i el navegador web.

El codi d'usuari que s'empra per accedir-hi en ambdós casos és una adreça de correu electrònic. Això que podria implicar un risc moderat, en el cas de Google i Microsoft, en què han unificat els accessos als seus serveis, es converteix en un risc molt alt, atès que el coneixement de la dita adreça de correu electrònic permetria que un tercer pogués realitzar diversos intents d'accés, sobre la base que ja es coneix l'usuari, i, en cas d'èxit, aconseguir accedir també a tots els serveis prestats per Google o Microsoft que utilitzen el seu sistema unificat de credencials.

Tot i que, en ambdós casos, s'estableixen uns requisits mínims per a la configuració de la contrasenya d'accés (obliga a emprar una contrasenya amb certa robustesa, que no es podrà reutilitzar), aquests podrien ser insuficients, atès que l'intent reiterat de contrasenyes errònies no provoca en cap dels dos casos el bloqueig del compte (per al cas de Google, només a partir del quinzè intent es demana un codi tipus "captcha" per evitar intents d'accés automatitzats; en el cas de Microsoft, això succeeix a partir del desè intent).

Com aspecte positiu cal destacar que, en ambdós casos, la casella de memorització automàtica de les credencials no apareix marcada per defecte. El cas contrari comportaria un risc alt per a la seguretat de la informació, especialment en ordinadors compartits o en ordinadors d'ús públic, atès que si l'usuari s'oblida de sortir de la sessió, un tercer que posteriorment empri aquests ordinadors i accedeixi a l'adreça https://mail.google.com o https://outlook.office365.com podrà accedir al compte de correu electrònic, fins i tot si s'hagués tancat el navegador o l'ordinador de què es tracti.

Ambdues aplicacions "web" permeten activar el que anomenen *"verificación en dos pasos",* de manera que ja sigui per accedir al compte, o per accedir des d'un dispositiu mòbil al compte, es demanarà a l'usuari, a banda de les seves credencials i de la seva contrasenya, un codi numèric de 6 dígits de caràcter temporal. Aspecte que cal valorar positivament.

Finalment, cal tenir present que, un cop s'accedeix al compte, la sessió a Google o a Microsoft no caduca o, com a mínim, no caduca en un termini raonable.

- Accés mitjançant el que s'anomena "aplicació d'escriptori" o "clients de correu":

L'accés al compte de correu de *Google Apps for Business* (Gmail) o de *Microsoft Office 365* es pot configurar amb qualsevol client de correu que suporti els protocols SMTP i POP3 o IMAP, per a Google, i Exchange, SMTP i POP3 o IMAP, per Microsoft, com ara, per exemple, Microsoft Outlook o Thunderbird.

En cas que s'activi la verificació en dos passos s'ha d'establir, en ambdós casos, una contrasenya específica per a cadascuna de les aplicacions d'escriptori o clients de correu que es vol utilitzar per accedir al compte de correu electrònic.

Així doncs, la disponibilitat i la integritat de la informació no sembla que estigui subjecta a uns riscos específics pel fet d'utilitzar "aplicacions d'escriptori", més enllà dels que es derivin pel fet que la persona usuària, en algun moment, deixi d'emprar l'ordinador sense adoptar mecanismes de control d'accés escaients, com ara, tancar la sessió del correu electrònic o bloquejar l'ordinador.

- Accés mitjançant una aplicació per a dispositius "mòbils" (APPS):

L'accés al servei de correu electrònic de *Google Apps for Business* (Gmail) des de telèfons mòbils amb sistema operatiu Android es pot fer utilitzant les aplicacions natives que porten preinstal·lades. En el cas d'emprar telèfons mòbils Iphone, l'accés es pot fer utilitzant Google Sync des de l'aplicació de correu nativa del telèfon mòbil o bé utilitzant l'aplicació Gmail per a iOS. En telèfons mòbils amb sistema operatiu Windows Phone, s'ha de fer utilitzant Google Sync des de l'aplicació de correu nativa.

L'accés al servei de correu electrònic de *Microsoft Office 365* des de telèfons amb sistema operatiu Android o Windows Phone es pot fer utilitzant les aplicacions natives que porta preinstal·lades. En el cas del model Iphone, l'accés es pot fer utilitzant l'aplicació de correu nativa del telèfon mòbil o bé utilitzant l'aplicació OWA for iPhone.

Un risc per a la integritat de la informació podria derivar-se de la no adopció, per part de la persona usuària, d'un sistema de bloqueig d'accés al dispositiu mòbil. En aquest cas, el compte de correu electrònic i la informació que s'hi pugui contenir podrien quedar exposats a tercers si algú accedeix de manera no autoritzada (per exemple, en cas de pèrdua del dispositiu).

Vistes aquestes previsions, es pot concloure que els riscos de l'ús del servei de correu electrònic de *Google Apps for Business* o de *Microsoft Office 365* estarien relacionats amb les diferents aplicacions i plataformes que permeten el seu accés, atès que, amb diferents nivells, presenten certes vulnerabilitats que podrien donar lloc a l'afectació de la informació que es tracta en els respectius serveis de correu electrònic, especialment en relació amb la seva confidencialitat, com a conseqüència d'accessos no autoritzats.

Per tal d'evitar aquest risc, especialment pel que fa a les dades sensibles a què es pugui tenir accés, es fan als usuaris (l'entitat) les recomanacions següents:

- Emprar contrasenyes segures pels comptes d'usuari (combinar números, lletres, símbols, majúscules i minúscules, i establir una longitud mínima de 8 caràcters).
- Emprar la verificació en dues passes que ofereixen tots els proveïdors.
- En el cas d'emprar l'aplicació d'accés mitjançant el "web", no activar l'opció de recordar les credencials, atès que l'accés a l'ordinador podria quedar disponible per a d'altres usuaris, i tancar la sessió un cop s'abandoni el lloc de treball, atès que les sessions obertes no caduquen per inactivitat i, per tant, un altre usuari podria accedir a la informació o, fins i tot, modificar paràmetres del perfil del compte, inclosos els aspectes de seguretat.
- En el cas d'emprar l'aplicació d'escriptori o "clients de correu", protegir l'accés a l'ordinador mitjançant un usuari (local o de xarxa) i una contrasenya, o amb un mecanisme equivalent, i configurar l'ordinador perquè es bloquegi passat un temps d'inactivitat.
- En el cas d'emprar les aplicacions de dispositius mòbils, protegir sempre l'accés al dispositiu.
- En cas d'accedir al servei mitjançant una xarxa sense fils, verificar la confiança de la xarxa en qüestió.

IX

Altres aspectes rellevants en la prestació d'aquests serveis: resolució de conflictes.

Arribats a aquest punt, no és sobrer assenyalar què succeiria en cas de **desacord o conflicte** sobre alguna de les previsions establertes en el contracte dels serveis examinats:

• D'acord amb l'apartat *"Otras disposicions"* de les condicions de servei aplicables a *Google Apps for Business*, qualsevol desacord (contractual o no) que se susciti en relació amb l'acord subscrit es regirà pel dret de l'Estat de Califòrnia, sotmetent-se empresa i client (l'entitat) a la jurisdicció exclusiva dels tribunals federals o estatals del comtat de Santa Clara (Califòrnia, Estats Units).

• Microsoft preveu, en l'apartat *"Entidad contratante de Microsoft"* de les condicions del servei que, en cas que el client resideixi o tingui la seva seu social a Espanya, el dret espanyol regirà la interpretació de l'acord subscrit, si bé qualsevol altre conflicte (protecció del consumidor, competència deslleial o responsabilitat extracontractual, per exemple) es resoldrà de conformitat amb les lleis del país a què Microsoft dirigeixi els seus serveis.

En les condicions d'ús actualitzades, aquesta previsió ha estat modificada, de tal manera que, a partir del 31 de juliol de 2014, tota reclamació sorgida en relació amb els serveis de pagament prestats per Microsoft es resoldran de conformitat amb les lleis del país a què Microsoft dirigeixi els seus serveis.

Cal tenir en compte, per tant, que en cas d'existir un desacord entre el client (l'entitat) i Google sobre els termes i/o les condicions de l'acord subscrit per a la prestació dels serveis, la normativa aplicable, a criteri d'aquest proveïdor, no seria l'espanyola. Aquesta previsió no pot considerar-se adequada.

Cal recordar que els ciutadans espanyols, les dades dels quals siguin tractades per l'entitat, tenen dret a que aquest, i també els que intervinguin per compte seu, tractin les seves dades personals d'acord amb el que estableixen la LOPD i el RLOPD.

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

Conclusions

Per tal de donar compliment a la normativa de protecció de dades personals en la contractació dels serveis oferts mitjançant *Google Apps for Business* o *Microsoft Office 365* és necessari, a banda de subscriure un contracte d'encarregat del tractament, realitzar una anàlisi prèvia dels riscos per a la seguretat i la integritat de la informació (que, en aquest cas, pot ser especialment protegida) que es puguin derivar de l'ús d'aquests serveis.

L'adhesió de Google i Microsoft als principis de l'acord "U.S.-E.U. Safe Harbor" pressuposa, a data d'avui, que les dades personals trameses per l'entitat consultant seran tractades amb determinades garanties i condicions de seguretat, tot i que podria resultar insuficient, atès que els fluxos d'informació poden referir-se a zones geogràfiques o tercers països que no ofereixen un nivell adequat de protecció. En aquest sentit, l'Agència Espanyola de Protecció de Dades, per mitjà de la Resolució TI/00032/2014, ha considerat adequades les garanties establertes en els models de contracte per a la transferència internacional de dades amb destinació a Microsoft Corporation amb motiu de la prestació dels serveis *Microsoft Online Services* (entre ells, *Office 365*) i actuant com encarregat del tractament, en els termes previstos en la dita Resolució.

Les actuacions previstes en les condicions d'ús dels serveis examinats, especialment de *Google Apps for Business*, poden excedir la finalitat principal per la qual l'entitat li encarregaria el tractament de les dades i, per tant, poden comportar una vulneració del principi de qualitat, en la seva vessant de finalitat (article 4.2 LOPD).

Les mesures de seguretat global implementades en els serveis *Google Apps for Business* i *Microsoft Office 365,* tot i ser adequades, podrien resultar insuficients. Per aquest motiu, qualsevol certificació o estàndard internacional en matèria de seguretat de què puguin disposar els dits proveïdors hauria d'anar acompanyada de la auditoria prevista a la normativa de protecció de dades.

L'ús del servei de correu electrònic de *Google Apps for Business* o de *Microsoft Office 365* no presenta riscos addicionals per a la seguretat de la informació, sempre que s'adoptin les recomanacions establertes en aquest dictamen.

Barcelona, 17 de juliol de 2014