CNS-57/2013

Informe en relació amb la consulta d'un col·legi d'advocats en relació amb els riscos que comporta l'ús de "Google Drive", "Microsoft Skydrive" i "Dropbox" en l'àmbit professional de les relacions entre advocat i client.

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un col·legi d'advocats, en què es demana el parer de l'Autoritat en relació amb els riscos que suposa l'ús de "Google Drive", "Microsoft Skydrive" i "Dropbox" en l'àmbit professional de les relacions entre advocat i client.

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

El col·legi d'advocats sol·licita, en el seu escrit de consulta, el parer d'aquesta Autoritat en relació amb els riscos que comporta l'ús de les aplicacions "Google Drive", "Microsoft Skydrive" i "Dropbox" per a l'advocat en el cas que aquest decideixi emmagatzemar-hi documentació relativa als seus clients.

En concret, planteja si la certificació ISO/IEC/27001:2013, juntament amb el contracte d'encàrrec del tractament, i la inclusió, de les empreses proveïdores d'aquests serveis, a l'acord "U.S.-E.U. Safe Harbor" podria considerar-se garantia suficient per complir amb la normativa de protecció de dades personals.

Així mateix, sol·licita a aquesta Autoritat que especifiqui les certificacions que en aquest sentit hauria d'adquirir un prestador de serveis de computació en el núvol per complir estrictament amb la normativa.

Per tal de donar resposta a totes aquestes qüestions, s'ha optat per dur a terme l'anàlisi dels riscos derivats de l'ús dels serveis "Google Drive", "Microsoft Skydrive" i "Dropbox" de manera diferenciada, tal com s'indica a continuació:

- 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".
- Les mesures de seguretat i la certificació ISO/IEC/27001:2013 de les empreses proveïdores d'aquests serveis.
- La seguretat proporcionada específicament pels serveis "Google Drive", "Microsoft Skydrive" i "Dropbox".

Abans d'efectuar aquesta anàlisi però, es faran 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, tot i no ser objecte de consulta, es considera necessari fer referència, en els darrers apartats d'aquest informe, a d'altres aspectes que, des del punt de vista de la protecció de dades personals, són també rellevants en la prestació d'aquests serveis: el principi de qualitat de les dades, les responsabilitats assumides per les empreses proveïdores d'aquests serveis i els mecanismes establerts per a la resolució de possibles conflictes.

III

Els serveis de *"cloud storage".*

D'acord amb la informació disponible en les pàgines web de les respectives companyies, "Google Drive" (www.drive.google.com), "Microsoft Skydrive" -actualment, "Microsoft Onedrive"- (https://onedrive.live.com) i "Dropbox" (www.dropbox.com) són serveis d'emmagatzematge d'informació que operen en el núvol.

Convé apuntar que, si bé l'escrit de consulta menciona "Google Drive", "Microsoft Skydrive" i "Dropbox" com "aplicacions", s'entén que es vol fer referència als "serveis" que utilitzen diferents "aplicacions" que s'executen en diferents plataformes, per tal de posar les prestacions d'aquests serveis a l'abast de qualsevol usuari.

Aquest aclariment es considera necessari, atès que l'anàlisi dels riscos per a la seguretat de la informació derivats de l'ús d'aquests serveis -que es durà a terme en un altre apartat del present informe- pot comprendre, tant els aspectes de seguretat global de cadascun dels serveis citats, com els aspectes de seguretat de les aplicacions emprades per accedir a les prestacions i les funcionalitats que aquests serveis ofereixen.

En relació, precisament, amb aquestes prestacions i funcionalitats, equivalents en els tres serveis de *"cloud storage"* examinats, escau destacar-ne les següents:

- Faciliten als usuaris un espai per emmagatzemar informació (fitxers) en format digital, que és accessible des d'Internet mitjançant un compte d'usuari.
- Permeten emmagatzemar els fitxers en diferents formats: tractaments de textos, fulls de càlculs, imatges, vídeo, àudio, etc. Per tant, incorporen les funciones de càrrega i descàrrega dels fitxers, així com de sincronització dels fitxers entre l'emmagatzematge local (en el dispositiu) i l'emmagatzematge remot (en el servidor).
- Permeten accedir a l'espai on s'emmagatzemen els fitxers des de qualsevol dispositiu amb accés a la xarxa (Internet). Com a requisit caldrà que en el dispositiu d'accés es pugui executar un navegador web o una aplicació d'escriptori (proveïda pel mateix prestador del servei o bé per un tercer), o bé una aplicació tipus APP (fonamentalment per a sistemes Android o iOS que, generalment, pot ser proveïda tant pel mateix prestador del servei com per un tercer).
- Incorporen, entre les seves funcionalitats bàsiques, la de compartir amb tercers els fitxers emmagatzemats en l'esmentat espai que, per defecte, és d'accés exclusiu de l'usuari (qui l'ha contractat). Per tant, per compartir els fitxers amb tercers caldrà que l'usuari autoritzi prèviament aquest accés al seu espai d'emmagatzematge.

Fetes aquestes consideracions inicials, cal fer avinent que, tal com es va posar de manifest en el Dictamen CNS 24/2012 emès per aquesta Autoritat en relació amb la contractació del servei *Google Apps for Business* (disponible al web de l'Autoritat www.apd.cat), la contractació d'aquests serveis TIC tipus *"cloud computing"* o "computació en el núvol" –en el present cas, serveis de *"cloud storage"*- 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-usuaris 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.

Per la seva part, l'article 3.g) de la LOPD defineix, com a encarregat del tractament, "*la persona física o a, 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'advocat que contracta serveis de *"cloud storage"* és la de responsable del fitxer o tractament, mentre que les empreses proveïdores d'aquests serveis –Google, Microsoft i Dropbox- adoptarien la postura d'encarregats del tractament.

Sent així, la transmissió d'informació personal (fitxers) per l'advocat a les empreses Google, Microsoft i Dropbox, per tal d'emmagatzemar-la en els seus servidors, que inclourà dades dels seus clients però probablement també dades del propi advocat o, fins i tot, dades de terceres persones, 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 sigui possible cal que, tal i com es manifesta en l'escrit de consulta, se celebri un contracte d'encarregat del tractament (article 12 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.
d) El retorn o la destrucció de les dades, un cop complerta la prestació contractual.

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, d'entrada, cal tenir present que la contractació per part d'un advocat de la prestació de serveis *"cloud storage"* requereix l'existència d'un **contracte d'encarregat del tractament** amb el contingut mínim determinat en aquests preceptes.

També s'ha de tenir en compte, tal i com es va posar de manifest en el citat Dictamen CNS 24/2012, 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, 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".

Per aquest motiu, i atès que correspon a l'advocat, 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 (article 20.2 RLOPD), aquest està obligat, de manera inexcusable, a fer una anàlisi prèvia de l'impacte de la contractació d'aquests serveis de *"cloud storage"* 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/files/2012/wp196_en.pdf).

Cal dir que, en relació amb l'anàlisi d'aquests riscos, en l'escrit de consulta es planteja, com s'ha avançat, si el fet que les empreses proveïdores d'aquests serveis estiguin adherides als principis de l'acord "U.S.-E.U. Safe Harbor", així com que comptin amb la certificació ISO/IEC/27001:2013, podria considerar-se garantia suficient del compliment de la normativa de protecció de dades.

Aquests aspectes s'analitzen de manera diferenciada en els apartats següents d'aquest informe, prenent com a referència les respectives condicions d'ús dels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox" vigents en el moment en què s'ha plantejat la consulta. Cal fer però unes consideracions prèvies al respecte:

Atesos els termes en què es formula la consulta, les condicions d'ús examinades són les previstes per les respectives companyies amb caràcter general. És a dir, no s'han examinat les condicions de servei de "Google Drive" per a usuaris d'un compte de *"Google Apps"* (www.google.com/apps/intl/en/terms/standard_terms.html), ni les de "Microsoft Onedrive" per a comptes gestionats per un tercer (www.domains.live.com/Addendums/en-us/CB.htm), ni les de "Dropbox" per a empreses (www.dropbox.com/privacy#business_agreement), sens perjudici que les observacions fetes en aquest informe puguin resultar igualment aplicables en aquests supòsits.

Sovint, aquestes condicions d'ús 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 emprada o les mesures de seguretat aplicades.

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 el servei "Dropbox". En el transcurs de l'elaboració del present informe l'empresa Dropbox ha anunciat una actualització de la política de privacitat, així com de les condicions d'ús generals i de les condicions previstes per a les empreses del seu servei "Dropbox". Les dites actualitzacions està previst que entrin en vigor el 24 de març 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, el responsable del tractament (l'advocat) 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, de l'ús dels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox", 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 de *"cloud storage",* 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 el responsable del tractament o fitxer (l'advocat) 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 que aquest vulneri la normativa de protecció de dades.

És possible que la contractació d'aquests serveis de *"cloud storage"* 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 "Microsoft Onedrive", "Google Drive" i "Dropbox":

- D'acord amb les condicions generals del servei "Microsoft Onedrive" (http://windows.microsoft.com/es-es/windows-live/microsoft-services-agreement), la contractació d'aquest servei pel client-usuari (l'advocat) es durà 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*").

Per tant, d'inici, es podria pensar que la transmissió de les dades personals per l'advocat 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 (www.microsoft.com/privacystatement/es-es/core/default.aspx) 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 "*Otra información de privacidad importante. Dónde se guarda y procesa la información*"), sense concretar però quines són aquestes empreses i on es troben ubicades físicament.

- Pel que fa a la contractació del servei "Google Drive", d'acord amb les seves condicions de servei (www.google.com/policies/terms), aquesta es duria a terme amb l'empresa Google Inc., el domicili social de la qual està ubicat a Califòrnia, als Estats Units, si bé també seria possible fer-ho amb una de les seves filials. En aquest cas, i a diferència de Microsoft, no s'assenyala quines podrien ser aquestes empreses filials.

En aquest sentit, escau assenyalar que, en el supòsit que la contractació tingués lloc amb Google Ireland Limited (el més probable), la transmissió de les dades personals per l'advocat 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, de la mateixa manera que en el cas de Microsoft, si s'examina la política de privacitat de Google (www.google.com/intl/es/policies/privacy/) es pot comprovar que la companyia afirma 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*"), sense concretar però quins serien aquests països.

- Pel que fa a la contractació del servei "Dropbox" sembla ser que, pel que es desprèn de les condicions del servei (www.dropbox.com/privacy#terms), aquesta es duria a terme amb una empresa ubicada a Califòrnia, als Estats Units.

En aquest cas, si s'examina la política de privacitat vigent en el moment d'efectuar la consulta (www.dropbox.com/privacy#privacy), es pot comprovar, a més, com la companyia preveu que tercers (proveïdors de servei, socis empresarials i altres persones externes de confiança) puguin tenir accés a la informació personal tractada (apartat "3. *Intercambio y divulgación de información*"), sense concretar, més enllà dels serveis d'emmagatzematge de l'empresa Amazon emprats, quins són aquests tercers i on es troben ubicats físicament.

Cal assenyalar que en la versió actualitzada de la política de privacitat (https://www.dropbox.com/privacy2014) s'omet la referència a l'empresa Amazon, si bé es manté que tercers puguin tenir accés a la informació del client, establint, en aquest sentit, que el dit accés serà exclusivament per realitzar tasques en nom de Dropbox (apartat *"Con quién"*). A això cal afegir que l'empresa admet poder emmagatzemar, processar i transmetre la informació a qualsevol lloc del món, incloses ubicacions fora del país del client (apartat *"Dónde"*).

Ateses totes aquestes previsions, 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 pel client-usuari (l'advocat) als prestadors de serveis *"cloud storage"* assenyalats -Microsoft, Google o Dropbox- 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 Microsoft, Google i Dropbox (fins i tot, si fos el cas, Amazon) 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 a Microsoft, Google o Dropbox, 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, 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. De fet, aquest és el cas de les empreses analitzades que, com hem vist abans, també preveuen la transmissió de les dades a servidors ubicats en qualsevol altre país en què l'empresa o els seus agents disposin d'instal·lacions, així com a diferents zones geogràfiques, sense esclarir però les seves ubicacions físiques.

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 tres empreses proveïdores d'aquests serveis de *"cloud storage"* informen, per mitjà de la seves polítiques de privacitat, de la seva adhesió als principis de l'acord Safe Harbor, no informen d'aquest mateix extrem pel que fa a la resta de zones geogràfiques en què podrien ubicar-se els seus servidors (o els de tercers).

Únicament "Dropbox" especifica -si bé tal previsió s'omet en la política de privacitat actualitzada- que empra l'espai d'emmagatzematge ofert per l'empresa Amazon (apartats *"tus cosas y tu privacidad"*). Ara bé, cal recórrer a la política de privacitat de dita companyia per conèixer que aquesta empresa també es troba adherida als principis de l'acord Safe Harbor (http://aws.amazon.com/es/privacy/) i, tot i així, no es podria descartar que Amazon disposés també de servidors ubicats en tercers països amb un nivell de protecció no equivalent.

En cas de no poder garantir, per tant, la dita adhesió als principis de l'acord Safe Harbor o que les zones o països en què tenen ubicats els seus servidors ofereixen un nivell de protecció equivalent, i de no donar-se cap altra de les excepcions previstes a la LOPD –com ara, el supòsit previst a l'article 34.g) 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.

En aquest punt, i atesos els termes en què es formula la consulta, 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", tals com el *"cloud storage",* 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 han sol·licitat, entre d'altres aspectes, una revisió dels principis de l'acord Safe Harbor a què es fa referència en aquest informe, 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).

D'aquests documents destaca, en concret, la constatació per part de la Comissió del fet que, en la mesura que els programes de supervisió nord-americans afectin a dades emmagatzemades en el núvol a les quals resulti d'aplicació la legislació europea sobre protecció de dades personals, facilitar a les autoritats dels Estats Units, sense complir els requisits previstos en aquesta legislació, l'accés a les dades allà allotjades, fins i tot, per a aquells que tinguin la condició d'encarregats del tractament, suposarà la infracció de la legislació europea de protecció de dades –així com de la nacional aplicable-, sense que les excepcions previstes en el marc dels principis de Safe Harbor permetin 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).

Cab 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 Microsoft, Google i Dropbox 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. Tot i així, cal tenir present que aquesta adhesió de les empreses proveïdores del serveis *"cloud storage"* a l'acord Safe Harbor no eximeix el

responsable del tractament del compliment de la resta de previsions establertes en la normativa espanyola 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 a les condicions del servei, relatives a la transmissió de la informació tractada a **empreses o societats del grup**:

- En el cas de "Microsoft Onedrive", això es preveu en els apartats *"Cómo utilizamos su información personal"* i "*Otra información de privacidad importante"* de la seva declaració de privacitat.

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

- En el cas de "Dropbox", es preveu en els apartats *"Tus cosas y tu privacidad"* de les condicions de servei i "*Proveedores de Servicios, socios empresariales y otros*" de la seva política de privacitat, ambdues en les seves versions no actualitzades en data 24 de març de 2014.

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'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 condicions pel que fa a la participació **d'empreses subcontractades** en la prestació dels serveis de *"cloud storage":*

- En el cas de "Microsoft Onedrive" s'estableix que *"podemos compartirla con empresas a las que hemos contratado para ofrecer servicios en nuestro nombre. Cuando compartimos información con estas empresas para que nos ofrezcan sus*

servicios, no les está permitido utilizarla para ningún otro fin y deben mantener su confidencialidad".

- En el cas de "Google Drive" s'estableix que *"proporcionaremos tus datos personales a nuestras filiales o a organizaciones y otros terceros de confianza para que lleven a cabo su tratamiento por cuenta de Google siguiendo nuestras instrucciones, de conformidad con nuestra Política de privacidad y adoptando cuantas medidas sean oportunas para garantizar la confidencialidad y seguridad de dichos datos*".

- Pel que fa a "Dropbox" s'estableix que *"a fecha de entrada en vigor de esta política, utilizamos los servicios de almacenamiento S3 de Amazon para almacenar parte de tu información (por ejemplo, tus Archivos)*". Aquesta previsió, com s'ha indicat, ha estat eliminada en la versió actualitzada de data 24 de març de 2014.

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, el proveïdor dels serveis de *"cloud storage"* 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 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 *"cloud storage"* a contractar per l'advocat.

VI

Les mesures de seguretat i la certificació ISO/IEC/27001:2013 de les empreses proveïdores dels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox".

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.

D'entrada, i abans d'analitzar la seguretat proporcionada específicament per "Google Drive", "Microsoft Onedrive" i "Dropbox" –que es farà en un apartat diferenciat-, cal destacar que les companyies proveïdores d'aquests serveis de *"cloud storage"* expliciten en les seves condicions de servei i de privacitat que ni són responsables de la pèrdua d'informació ni poden garantir al 100% la seguretat de la informació emmagatzemada en els seus servidors (o, en el seu cas, en els de tercers):

- Pel que fa a "Microsoft Onedrive" s'estableix que *"no podemos garantizar que los Servicios sean ininterrumpidos, puntuales, seguros ni que estén libres de errores"* (apartat "*Microsoft no otorga ninguna garantía adicional*" de les condicions de servei).

- En relació amb "Google Drive" s'estableix que *"(...) ni Google ni sus proveedores o distribuidores serán responsables por la pérdida de (...) datos (....)"* (apartat *"Responsabilidad por nuestros Servicios"* de les condicions de servei).

- En relació amb "Dropbox" s'estableix que *"en ningún caso serán responsables Dropbox, sus afiliados, directivos, empleados, agentes, proveedores ni licenciatarios de ningún daño indirecto, especial, incidental, punitivo, ejemplar o consecuente (incluida la pérdida de uso, datos, negocios o beneficiarios"* (apartat *"Limitación de responsabilidad"* de les condicions de servei, i, en sentit similar, en les noves condicions). Així mateix, reconeix que *"ningún método de transmisión ni de almacenamiento electrónico es seguro al 100%"* (apartat *"Seguridad"* de la política de privacitat, tot i que aquest apartat ha estat eliminat de la versió actualitzada en data 24 de març de 2014).

Previsions d'aquest tipus, que, cal assenyalar, són formulades unilateralment per les empreses que ofereixen els serveis, no poden considerar-se com una eximent de les obligacions que, en funció de la informació tractada, poguessin resultar exigibles en base al que disposa l'article 9 de la LOPD.

D'acord amb aquest precepte correspon al responsable del tractament i, si s'escau, a l'encarregat del tractament 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.

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 de *"cloud storage"* 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, per la pròpia naturalesa de la relació entre advocats i clients, és possible que algunes de les informacions personals que s'emmagatzemin a "Google Drive", a "Microsoft Onedrive" o a "Dropbox" (o, en el seu cas, en els servidors de tercers) siguin dades especialment protegides, és a dir, dades que la normativa protegeix de forma reforçada (article 7 LOPD), com ara, les dades de salut o les dades relatives a la comissió d'infraccions penals o administratives, entre d'altres.

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.

Per exemple, l'estàndard ISO/IEC/27001 "Sistemes de Gestió de la Seguretat de la Informació" de la *International Standards Organization*; la certificació SAS 70 *"Statement on Auditing Standards No. 70";* la certificació Systrust y Webtrust del *American Institute of Certified Public Accountants* (AICPA); la certificació del *Federal Information Security Management Act* (FISMA): NIST SP 800-37 *"Guide for the Security Certification and Accreditation of Federal Information Systems"*, entre d'altres.

A l'escrit de consulta es planteja si el fet de comptar amb **la certificació ISO/IEC/27001:2013** pot considerar-se garantia suficient per complir amb la normativa de protecció de dades.

Convé puntualitzar que aquesta versió de l'estàndard va ser publicada a l'octubre de 2013. Tot i incorporar algunes modificacions respecte de la seva versió anterior, ISO/IEC/27001:2005, als efectes que interessen en la present consulta, es poden considerar equivalents, de tal manera que ens referim de manera genèrica a l'estàndard ISO/IEC/27001.

El fet que les empreses Microsoft, Google i Dropbox disposessin de la certificació ISO/IEC/27001 suposaria 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 i, en cas positiu, hauria emès el corresponent certificat.

Els pilars bàsics d'aquest estàndard ISO/IEC/27001 comprenen:

- L'establiment d'una política, un abast i uns objectius per a la seguretat de la informació.
- L'elaboració d'una anàlisi de riscos proporcionat a la naturalesa i la valoració dels actius i dels riscos a què aquests actius estan exposats.
- La selecció dels controls adequats, de conformitat amb els objectius que es pretenen obtenir amb aquests controls, justificant la seva elecció (recollits a l'Annex A de la norma).
- La millora continua.

Tenint en compte els apartats d'aquest estàndard i, específicament, els controls per a la seguretat de la informació establerts en el seu Annex A (en la darrera versió han passat de 133 a 114), podria admetre's que, en la mesura que aquests controls podrien en certa manera concordar amb diferents preceptes del RLOPD relatius a les mesures de seguretat (articles 89 a 104), l'aplicació de la ISO/IEC/27001 per una empresa proveïdora de serveis *"cloud storage"* li facilitaria el compliment de la normativa de protecció de dades en aquest sentit.

És a dir, disposar d'una certificació ISO/IEC/27001 vigent podria considerar-se un bon indici de que els sistemes d'informació dels proveïdors de serveis *"cloud storage"* examinats estan convenientment gestionats des de la perspectiva de la seguretat de la informació.

Ara bé, dit això, escau puntualitzar que:

- El nucli de l'estàndard ISO/IEC/27001 és que els riscos per al sistema d'informació de l'empresa en qüestió s'analitzin i es gestionin, que la seguretat es planifiqui, s'implementi, es revisi, es corregeixi i es millori. És a dir, l'objectiu d'aquest estàndard és que l'empresa sigui capaç de prioritzar i seleccionar els controls d'acord amb les seves possibilitats i les seves necessitats (o riscos) de seguretat.

- Tot i que les mesures de seguretat susceptibles de ser implantades en un sistema certificat segons l'estàndard ISO/IEC/27001 puguin concordar amb diferents preceptes

del RLOPD, en realitat no hi ha una relació directa entre aquestes mesures i les previstes en el RLOPD.

És a dir, disposar de la certificació ISO/IEC/27001 no es garantia de l'existència, a tall d'exemple, d'un document de seguretat amb els continguts mínims previstos a la legislació espanyola de protecció de dades, d'una política de còpies de seguretat que compleixi els requisits del RLOPD, d'un registre d'accés a les dades o d'un registre d'incidències que compleixi amb tots els requisits previstos en la normativa vigent.

A més, escau assenyalar la dificultat existent en poder determinar si efectivament els proveïdors d'aquests serveis de *"cloud storage"* disposen de la certificació ISO/IEC/27001. Ni les condicions de servei, ni les polítiques de privacitat o, en el seu cas, de seguretat contenen referències específiques a aquesta certificació.

Veiem, doncs, què s'estableix en relació amb aquest aspecte:

- L'empresa Microsoft explicita en la pàgina web (www.microsoft.com/online/legal/v2/es-es/MOS_PTC_Security_Audit.htm) que els seus productes "Office 365" i "Microsoft Dynamics CRM Online", així com els respectius centres de dades i d'infraestructures físiques, han obtingut la certificació ISO/IEC/27001, però es desconeix si el servei "Microsoft Onedrive" també podria disposar d'aquesta certificació.

- Pel que fa a l'empresa Google, aquesta hauria obtingut tal certificació per als sistemes, les aplicacions, els experts, les tecnologies, els processos i els centres de dades de "Google Analytics" i de Google "Analytics Premium" (https://support.google.com/analytics/answer/3407084?hl=ca&ref_topic=2919631), desconeixent-se però si també l'hauria obtingut pel servei de "Google Drive".

- Només l'empresa Dropbox explicita, si bé en l'apartat "centre d'ajuda" de la seva pàgina web (www.dropbox.com/help/238/es_ES), que, entre d'altres certificacions, l'empresa Amazon compta amb la certificació ISO/IEC/27001, de la qual, recordem, "Dropbox" fa servir les infraestructures de processament de la informació (http://aws.amazon.com/es/about-aws/whats-new/2010/11/18/aws-achieves-iso-27001-certification/). Per tant, cal tenir present que les aplicacions que ofereix Dropbox no han estat certificades segons l'estàndard ISO/IEC/27001, sinó els serveis del seu proveïdor Amazon. A això cal afegir que la referència a Amazon ha estat omesa en l'actualització de les condicions de servei.

Així doncs, a la vista d'aquestes consideracions, cal dir, en relació amb la qüestió concreta plantejada a l'escrit de consulta, que disposar de la certificació ISO/IEC/27001 -o qualsevol altra certificació o estàndard internacional en matèria de seguretat- podria no equivaldre a donar compliment a les previsions del RLOPD en matèria de seguretat.

Per tal que la dita certificació pugui ser considerada garantia suficient, aquesta hauria d'anar acompanyada de la auditoria prevista al RLOPD, atès que la finalitat d'aquesta mesura és, precisament, pronunciar-se de manera directa sobre si les mesures de seguretat implementades són conformes amb la legislació espanyola de protecció de dades.

Aquesta consideració pot fer-se extensible pel que fa a la qüestió plantejada en l'escrit de consulta relativa a les certificacions que hauria d'adquirir un prestador d'aquests tipus de serveis. No existeix cap certificació per a proveïdors en el núvol que verifiqui, de manera específica, el compliment estricte de les mesures de seguretat previstes al RLOPD. Qualsevol certificació en aquest àmbit, com en el cas de la ISO/IEC/27001, hauria d'anar acompanyada de l'informe d'auditoria a què s'ha fet referència.

En aquest punt, convé recordar que és responsabilitat de l'advocat (com a responsable del tractament) vetllar perquè els proveïdors dels serveis de *"cloud storage"* (com a encarregats del tractament) garanteixin la implementació de les mesures previstes al RLOPD (article 20.2 RLOPD).

VII

La seguretat proporcionada específicament pels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox".

Tal i com s'ha avançat a l'apartat III d'aquest informe, l'anàlisi dels riscos per a la seguretat de la informació en la prestació dels serveis de *"cloud storage"* examinats pot comprendre:

A. Els aspectes de seguretat global de cadascun dels serveis citats: allò establert a les respectives polítiques de servei, de privacitat i altres documents.

B. Els aspectes de seguretat de les aplicacions emprades per accedir a les prestacions i funcionalitats d'aquests serveis:

- Accés mitjançant el navegador "web".
- Accés mitjançant el que s'anomena "aplicació d'escriptori".
- Accés mitjançant una aplicació per a dispositius "mòbils".

Cal puntualitzar, en aquest punt, que en cas d'accés als serveis mitjançant aplicacions d'escriptori i aplicacions per a dispositius mòbils és possible emprar aplicacions proveïdes per tercers, és a dir, no necessàriament proveïdes per "Google Drive", "Microsoft Onedrive" i "Dropbox". Aquest ús d'aplicacions de tercers –per raons òbvies, no s'examina aquest aspecte- afegeix riscos addicionals en funció de la identitat del seu proveïdor. Per tant, fer només l'advertiment que el seu ús limitarà les possibles responsabilitats de Google, Microsoft o Dropbox en relació amb la gestió dels fitxers emmagatzemats per l'usuari (l'advocat).

A. Aspectes de seguretat global.

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

- Pel que fa al servei "Dropbox", l'única referència que es fa a la seguretat del servei en les seves condicions d'ús –referència que s'omet en l'actualització de 24 de març de 2014- és la que tracta aspectes relacionats amb la seguretat del compte d'usuari (apartat *"Seguridad de la cuenta"*). Dita referència es limita a determinar que l'usuari:

- Ha de custodiar la contrasenya d'accés al servei.
- Està obligat a comunicar immediatament a "Dropbox" l'ús no autoritzat del seu compte.
- I que és responsabilitat seva utilitzar una connexió xifrada al accedir al serveis de "Dropbox", tot i que aquesta previsió es contradiu parcialment amb la informació que "Dropbox" proporciona en relació amb les mesures de seguretat implantades en el seu servei, atès que, entre les mesures de seguretat que aporta el proveïdor, es preveu precisament la de xifrar el canal de comunicació.

Si acudim a la seva política de privacitat, es pot comprovar que "Dropbox" afirma, en el seu apartat *"Seguridad"*:

- Emprar el xifratge en la transmissió d'informació. Ara bé, cal dir que només es refereix a quan es tracta d'informació recollida mitjançant formularis (habitualment

quan l'usuari es dona d'alta en el servei) i, concretament, es refereix a l'ús de SSL16 quan es tracta d'informació relativa a mitjans de pagament, una qüestió que en tot cas creiem que no forma part del nucli de la consulta adreçada a aquesta Autoritat.
- Utilitzar els estàndards generalment acceptats per protegir la informació, sense concretar però de quins estàndards es tracta i, en tot cas, advertint que no poden garantir la seguretat al 100%.

Cal assenyalar que dita informació sobre la seguretat emprada per "Dropbox" es redueix de forma considerable en la versió actualitzada de la seva política de privacitat, en què, un cop dit que disposen d'una organització orientada a protegir la informació, recorden que tenen implantades mesures de seguretat tals com *"la autenticación en dos pasos, el cifrado de archivos en pausa y las alertas al vincular dispositivos y aplicaciones a tu cuenta."*

Malgrat aquesta reducció de la informació relativa a la seguretat, cal apuntar que "Dropbox" compta amb un apartat específic, anomenat "Resumen de Seguridad", a la seva pàgina web (www.dropbox.com/privacy#security), en què es conté informació addicional en aquest sentit i que, pel que es desprèn d'allò disposat al seu web, es manté vigent tot i les actualitzacions dutes a terme en les condicions d'ús i la política de privacitat.

D'acord amb el citat "Resumen de Seguridad", els arxius un cop han estat tramesos pel client són xifrats –és a dir, es mantenen xifrats mentre estan emmagatzemats-, esclarint, en aquest sentit, que ells gestionen les claus d'aquest xifratge. Per tant, en qualsevol moment "Dropbox" podria desxifrar la informació o, si aquestes claus queden compromeses, els arxius podrien ser desxifrats per tercers no autoritzats, que òbviament també haurien de tenir accés als fitxers.

Ara bé, també informa de la possibilitat que l'usuari, per tal de gestionar les seves pròpies claus de xifratge, pugui afegir una capa de xifratge abans de transmetre'ls, aspecte que cal valorar positivament, malgrat que això pugui comportar alguna pèrdua de funcionalitat o que, en cas de pèrdua de la clau per desxifrar, "Dropbox" no podria recuperar la informació xifrada per l'usuari en origen.

Així mateix, atès que empra Amazon S3 per emmagatzemar les dades (o, com a mínim, així s'afirma fins l'entrada en vigor de l'actualització de la política de privacitat), manté que dita companyia empra mesures de seguretat físiques de grau militar, tot i que cal recórrer a la seva pàgina web per obtenir més informació al respecte.

Pel que respecta a la transmissió de la informació entre les diferents aplicacions i els servidors, aquesta també es realitza de manera xifrada, utilitzant un canal segur, xifrat mitjançant SSL de 256 bits.

Pel que fa a la conservació de les dades, manté que tant ell com Amazon realitzen còpies de seguretat de totes les dades en múltiples ubicacions, per tal d'evitar la pèrdua d'informació.

Pel que fa al control d'accessos, assegura que el seu personal només té accés a les metadades dels arxius dipositats pels motius assenyalats en la seva política de privacitat, si bé es preveuen algunes excepcions (per exemple, per requeriments legals). També afirma emprar mesures de seguretat físiques i electròniques per evitar accessos no autoritzats, tot i que no en dóna detalls.

- En relació amb el servei "Google Drive", cal atendre a l'apartat *"Seguridad de los datos"* de la seva política de privacitat (www.google.com/policies/privacy/), 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 i altres apartats de la política de privacitat podem trobar molta 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 el servei “Google Drive” per protegir la informació que s’emmagatzema.

Si s’acudeix al “centre d’ajuda” de “Google Drive” només obtindrem recomanacions sobre com guardar la informació de manera segura -tals com, assegurar-se del que el compte sigui segur; sortir del compte en cas d’emprar un ordinador compartit; no instal·lar “Google Drive” en ordinadors públics; o escollir una configuració per compartir els arxius adequada per preservar la informació personal (privat, qualsevol usuari que rebi l’enllaç o públic en la web)-, així com una remissió a la política de privacitat i a un seguit d’eines pensades per protegir la privacitat (per exemple, la verificació en dos passos), però que no serveixen als efectes de conèixer detalls de com protegeix Google els seus sistemes d’informació.

El motiu d’aquestes recomanacions és, en bona part, que “Google Drive” està enllaçat amb “Gmail” –servei de correu electrònic de Google-, fet que pot comprometre fàcilment els arxius dipositats pel client (l’advocat) si aquest, per exemple, deixa oberta la finestra del navegador o si no protegeix el seu compte amb una contrasenya robusta.

Cal recordar que Google, a partir de l’any 2012, va començar a unificar les polítiques de privacitat i les condiciones d’ús de serveis tant importants com el correu electrònic, les xarxes socials i, també, el servei d’emmagatzematge, per tal de facilitar l’accés dels usuaris a tots aquests serveis mitjançant un compte únic. Això suposa evidents riscos des de la perspectiva de la seguretat, atès que si, com s’ha dit, no es protegeixen convenientment les credencials d’accés, aconseguint l’accés a un dels serveis seria possible accedir a la resta.

- Pel que fa a “Microsoft Onedrive”, cal dir que en la seva política d’ús només es recorda a l’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”).* Per tant, el client (l’advocat) ha de tenir present que, en aquest cas concret, el mateix proveïdor del servei de *“cloud storage”* reconeix no poder garantir la integritat i la conservació de les dades, tal i com exigeix la normativa de protecció de dades personals (articles 94 i 102 RLOPD).

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.

Si s'acudeix a l'apartat *"Protección de la Seguridad de la información personal"* de la seva política de privacitat (www.microsoft.com/privacystatement/es-es/core/default.aspx#), Microsoft afirma que:

- Es comprometen a protegir la seguretat de la informació personal dels usuaris.
- Apliquen mesures de seguretat per evitar l'accés, ús o divulgació no autoritzada, així com mesures per evitar l'accés físic als sistemes d'informació.
- Utilitzen el protocol SSL per al cas de transmissió d'informació "altament confidencial" (com a tal consideren el números de targetes de crèdit o les contrasenyes).
- Informen que, en tot cas, la responsabilitat de mantenir les credencials d'accés de manera confidencial correspon a l'usuari.

De la mateixa manera que Google, Microsoft incorpora, en aquest mateix apartat, un seguit de recomanacions de seguretat per al client-usuari consistents en no compartir la contrasenya del compte i en tancar la sessió abans de sortir del lloc web o del servei emprat, atès que el seu servei de "Microsoft Onedrive" també està enllaçat amb el seu servei de correu electrònic, "Outlook".

Així doncs, cal dir que la informació sobre la seguretat que aplica Microsoft és molt breu i insuficient per determinar quins mecanismes concrets apliquen a la protecció de la informació i dels seus sistemes.

Si bé, en la mesura que, de la informació proporcionada, Google, Microsoft i Dropbox afirmen adoptar normes i mesures tècniques reconegudes per assegurar les dades dels seus clients, 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 Drive", "Microsoft Onedrive" i "Dropbox" en aquest sentit, tot i ser adequades, resultin insuficients.

Dit això, es fan als usuaris (l'advocat) les recomanacions següents:

- Revisar la configuració per defecte del nivell de privacitat del servei pel que fa a la compartició de fitxers entre usuaris, per tal d'evitar publicar, sense coneixement, informació sense que estigui protegida per algun sistema de control d'accés.
- Realitzar còpies de seguretat periòdiques de la informació emmagatzemada.

B. Aspectes de seguretat de les aplicacions d'accés al servei

Fer avinent, d'entrada, que les consideracions que es fan, a continuació, en relació amb l'anàlisi dels **riscos de caràcter general** de les aplicacions que permeten l'accés als fitxers o arxius emmagatzemats en els serveis de *"cloud storage"* poden fer-se extensibles a tots els serveis analitzats en aquest informe:

- Accés mitjançant el navegador "web": aquesta aplicació s'empra per realitzar l'accés puntual a fitxers emmagatzemats en el servei.

El risc més rellevant en aquest tipus d'aplicació està relacionat amb la protecció de la confidencialitat, atès que el fet d'utilitzar navegadors per accedir a la informació pot implicar l'emmagatzematge automàtic, d'una banda, de les credencials d'accés a la

informació -d'especial rellevància quan es tracta de dispositius d'ús compartit- i, d'altra banda, dels arxius que es descarreguin mitjançant aquest tipus d'aplicació (habitualment tenen predeterminada una carpeta del sistema), circumstància que obliga a gestionar-los, ja sigui per desplaçar-los a d'altres ubicacions o bé per suprimir-los, segons el cas. En ambdós casos, l'accés per part de tercers al dispositiu o ordinador podria suposar l'accés total o parcial als fitxers emmagatzemats al servei.

La disponibilitat i la integritat de la informació emmagatzemada no estan subjectes a uns riscos específics pel fet d'utilitzar aplicacions web, més enllà de la possibilitat que un tercer pogués accedir als fitxers emmagatzemats al servidor i els modifiqués o esborrés malintencionadament (per exemple, aprofitant les credencials guardades de manera automàtica pel navegador).

- Accés mitjançant el que s'anomena "aplicació d'escriptori": la seva funció és mantenir una còpia en l'ordinador que està vinculat al compte del servei de manera sincronitzada amb els fitxers que s'emmagatzemen al servidor.

Els riscos relacionats amb el seu ús afecten a la confidencialitat de la informació, atès que una vegada vinculat l'ordinador, l'aplicació d'escriptori no demana cap tipus d'autenticació, per tant, qualsevol persona que tingués accés físic a l'ordinador (si no s'han establert prèviament mecanismes de control d'accés: bloqueig o credencials d'usuari per iniciar sessió) podria accedir també a tots els fitxers.

Així mateix, la integritat de la informació es podria veure afectada per un potencial accés no autoritzat que impliqués la modificació malintencionada d'algun dels fitxers que, a posteriori, seria sincronitzat en el servidor.

- Accés mitjançant una aplicació per a dispositius "mòbils" (APPS): la seva principal funció és sincronitzar els fitxers del servidor amb un dispositiu de tipus mòbil. En general, només si ho decideix l'usuari els fitxers s'emmagatzemen en el dispositiu.

Un risc per a la integritat de la informació podria derivar-se de la no adopció, per part de l'usuari, d'un sistema de bloqueig d'accés al dispositiu mòbil. En aquest cas, els fitxers ubicats al servidor podrien quedar exposats a tercers si algú accedeix de manera no autoritzada (per exemple, en cas de pèrdua del dispositiu).

A més, la pròpia arquitectura d'aquestes aplicacions pot comportar un risc en sí mateixa. En línies generals, el programari maliciós que es pugui descarregar en aquests dispositius podria arribar a interactuar amb les APPS dels serveis d'emmagatzematge i, per tant, amb els fitxers emmagatzemats.

Dit això, a continuació, es fan algunes consideracions en relació amb l'anàlisi dels **riscos derivats de la implementació concreta** que cada proveïdor de servei de "*cloud storage"* ha fet en les aplicacions que proporcionen l'accés als seus usuaris.

En aquest sentit, escau assenyalar que els serveis "Google Drive" i "Microsoft Onedrive" contenen previsions molt similars:

- Accés mitjançant el navegador "web":

L'accés a "Google Drive" o "Microsoft Onedrive" 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.

Ara bé, el codi d'usuari que s'empra per accedir-hi, tant a "Google Drive" com a "Microsoft Onedrive", és una adreça de correu electrònic. Això que podria implicar un risc moderat, en el cas de Google i Microsoft, en què, com s'ha vist, s'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 a, segons el cas, "Google Drive" o "Microsoft Onedrive" i, en cas d'èxit, aconseguir accedir també a tots els serveis prestats per Google o Microsoft amb un compte d'accés únic.

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, per al cas de "Google Drive", l'intent reiterat de contrasenyes errònies no provoca el bloqueig del compte (només a partir del quinzè intent es demana un codi tipus "captcha" per evitar intents d'accés automatitzats) i, per al cas de "Microsoft Onedrive", si bé l'intent reiterat de contrasenyes errònies sí bloqueja el compte, només cal reinicialitzar la contrasenya.

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. A més, "Microsoft Onedrive" també permet iniciar la sessió amb un codi d'ús únic quan ho desitgi l'usuari.

Finalment, cal tenir present que, un cop s'accedeix al compte, la sessió a "Google Drive" o "Microsoft Onedrive" no caduca o, com a mínim, no caduca en un termini raonable. Per tant, cal tenir en compte els riscos que es poden derivar d'aquest fet per a la informació emmagatzemada, tal i com s'ha fet referència en apartats anteriors.

- Accés mitjançant el que s'anomena "aplicació d'escriptori":

Cal tenir present que, un cop vinculat l'ordinador en què està instal·lada aquesta aplicació amb, segons el cas, el compte de "Google Drive" o el compte de "Microsoft Onedrive", no s'ha establert cap mecanisme addicional de control d'accés. Per tant, s'emprarà només el control d'accés previst a l'ordinador (usuari i contrasenya). Això comporta que, un cop iniciada la sessió a l'ordinador, es podrà accedir a la seva carpeta local, que contindrà el fitxers sincronitzats.

Atès que, com s'ha vist, ni Google ni Microsoft faciliten informació sobre si els fitxers emmagatzemats als servidors es mantenen xifrats, l'usuari ha de tenir present que, per tal que els documents es transmetin xifrats des del seu ordinador a "Google Drive" o a "Microsoft Onedrive" i per tal que s'emmagatzemin també xifrats en els respectius servidors, caldria aplicar sistemes propis de xifratge, de manera que ni aquests proveïdors ni tercers podrien tenir accés al seu contingut, tret que disposessin de la clau per desxifrar-los.

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

Mentre que la dita aplicació en el cas de "Microsoft Onedrive" no incorpora cap opció especial de seguretat, cal dir que l'aplicació de "Google Drive" permet xifrar els fitxers que s'emmagatzemen al dispositiu mòbil, aspecte que cal valorar positivament.

Pel que fa als permisos que requereixen les respectives APPS per oferir els serveis, cal fer avinent que, el relatiu, en concret, a l'accés al registre de trucades sol·licitat per "Google Drive", resultaria desproporcionat en relació amb les seves funcionalitats d'emmagatzematge d'arxius.

Mencció a part cal fer del servei "Dropbox". Alguns dels riscos detectats per a la seguretat de la informació coincideixen amb els ja analitzats pel que fa als serveis "Google Drive" i "Microsoft Onedrive", per la qual cosa es fan extensibles les

consideracions fetes en aquest sentit en els paràgrafs anteriors. Ara bé, es preveuen altres aspectes respecte els quals cal fer algunes consideracions:

- Accés mitjançant el navegador "web":

En el cas concret de "Dropbox" (això no succeeix amb "Google Drive" ni amb "Microsoft Onedrive") la casella de memorització automàtica de les credencials apareix marcada per defecte. Aquest fet comporta 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://www.dropbox.com/ podrà accedir a tots els fitxers emmagatzemats al servidor, inclús encara que s'hagués tancat el navegador o l'ordinador de què es tracti.

Així mateix, "Dropbox" no obliga a fer servir contrasenyes robustes. A més, no hi ha límits d'ús pel cas de reiniciar una contrasenya ja emprada anteriorment, és a dir, permet que es puguin reutilitzar.

Poder emprar contrasenyes no robustes, juntament amb el fet que els intents reiterats d'accés amb contrasenyes incorrectes només produeix el bloqueig del compte durant uns minuts, implica un risc moderat d'accés no autoritzat a la informació emmagatzemada.

- Accés mitjançant el que s'anomena "aplicació d'escriptori":

"Dropbox", a diferència de "Google Drive" i "Microsoft Onedrive", sí manté els fitxers emmagatzemats als servidors de manera xifrada. Ara bé, com s'ha apuntat, les claus de desxifrat estan en poder de la companyia. Per tant, caldria incorporar sistemes de xifratge propis, per tal que els documents es transmetin xifrats des de l'ordinador a "Dropbox" i per tal que s'emmagatzemin també xifrats en el servidor (aquests fitxers estaran xifrats dues vegades). Així, ni Dropbox ni un tercer podrien accedir al contingut dels fitxers, tret que disposin de la clau per desxifrar-los.

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

"Dropbox" incorpora, com a opció especial de seguretat, la possibilitat d'afegir un codi numèric de 4 dígits que se sol·licita cada vegada que l'usuari vol accedir a l'APP instal·lada al seu dispositiu mòbil.

Pel que fa als permisos que requereix l'APP per ser instal·lada, l'accés als contactes sense restriccions podria ser massa permissiu, si bé s'entén que podria estar justificat en la funcionalitat que ofereix de compartir fitxers amb tercers.

Vistes aquestes previsions, es pot concloure que els riscos de l'ús dels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox", com es planteja a l'escrit de consulta, estarien relacionats, no només amb les particularitats del servei en si mateix, sinó també amb les diferents aplicacions i plataformes que permeten l'accés i la gestió dels arxius emmagatzemats pels clients (l'advocat), atès que presenten certes vulnerabilitats que podrien donar lloc a l'afectació de la informació emmagatzemada, especialment en relació amb la seva confidencialitat, com a conseqüència d'accessos no autoritzats.

Per tal d'evitar aquests i altres possibles riscos, es fan als usuaris (advocats) les recomanacions següents:

- Examinar amb cautela quina informació es vol emmagatzemar en aquests serveis de *"cloud storage",* així com quina d'aquesta informació podria ser compartida.

No seria recomanable emmagatzemar-hi ni compartir informació confidencial o especialment protegida sense adoptar amb caràcter previ cap mesura addicional de seguretat, tal com, per exemple, l'ús d'eines que permeten el seu xifratge abans de ser emmagatzemada (TrueCrypt, Boxcryptor, etc.).

- 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 optar per l'opció de recordar les credencials i tancar la sessió un cop s'abandoni el lloc de treball.
- En el cas d'emprar l'aplicació d'escriptori, protegir l'accés a l'ordinador mitjançant un usuari (local o de xarxa) i una contrasenya, o amb un mecanisme equivalent, i xifrar els documents abans d'enviar-los als serveis d'emmagatzematge.
- En el cas d'emprar les aplicacions de dispositius mòbils, protegir sempre l'accés al dispositiu i, si ho permet l'aplicació, protegir també l'accés a l'APP concreta (per exemple, cas de "Dropbox").
  Així mateix, abstenir-se, en la mesura del possible, d'emmagatzemar els documents en el propi dispositiu mòbil i, si l'aplicació ho permet, activar el xifrat dels documents descarregats (per exemple, cas de "Google Drive").
- Controlar, en tot moment, quins dispositius es troben vinculats al compte del servei (és a dir, amb quins dispositius se sincronitza la informació emmagatzemada) i verificar periòdicament si cal desvincular-ne algun.
- Tot i que, a priori, es poden utilitzar aplicacions de tercers per accedir als serveis d'emmagatzematge examinats, seria bo utilitzar només les aplicacions proporcionades pels mateixos proveïdors dels serveis o, en tot cas, verificar que l'aplicació proveïda per altres tercers és confiable.
- En cas d'accedir al servei mitjançant una xarxa sense fils, verificar la confiança de la xarxa en qüestió.

VIII

Altres aspectes rellevants en la prestació d'aquests serveis: el principi de qualitat de les dades.

En aquest punt, i un cop analitzades l'adhesió als principis de l'acord de Safe Harbor i l'obtenció de la certificació ISO/IEC/27001 pels prestadors dels serveis *"cloud storage"* expressament manifestades en l'escrit de consulta com a possibles mecanismes que garanteixin el compliment de la normativa de protecció de dades personals, escau fer avinent l'existència d'altres aspectes que l'advocat, com a responsable, també ha de tenir en compte abans de dur a terme la contractació d'aquests serveis.

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).

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 12.4 LOPD).

En l'àmbit del *"cloud storage"* aquests principis resulten 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 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 previsions establertes en les condicions d'ús dels serveis de "*cloud storage"* examinats es pot comprovar, d'entrada, que es tracta d'unes condicions generals o estàndards que les companyies fixen de manera unilateral i que no deixen marge d'opció al client (l'advocat):

- En el cas concret de "Google Drive", per tal de conèixer què comporta l'acceptació d'aquestes condicions generals pel client, cal acudir al seu "centre d'ajuda", si bé en cap moment s'hi fa referència a aquest extrem en les seves condicions de servei.

En aquest "centre d'ajuda" s'especifica breument que *"como se indica en nuestras Condiciones de servicio, mantienes la propiedad de los derechos de propiedad intelectual que posees con respecto a ese contenido. En pocas palabras, lo que te pertenece, tuyo es."*

Per tant, *a priori*, podria pensar-se que, com a conseqüència de tal previsió, Google no podrà disposar de la informació emmagatzemada per l'advocat ni fer-ne ús per a una finalitat que no estigui expressament autoritzada per aquest com a responsable del seu tractament, tal i com exigeix l'article 12.2 de la LOPD.

No obstant això, si tornem a les condicions de servei, es pot comprovar que aquestes preveuen, a més a més, que *"al subir contenido o al enviarlo por otros medios a nuestros Servicios, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros Servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros Servicios (...)"* (apartat *"Tu contenido en nuestros Servicios"*).

Atesa, doncs, la disparitat de previsions, no queda suficientment clar què farà Google amb el contingut emmagatzemat pel client (l'advocat) mitjançant el servei "Google Drive", contingut que, recordem, contindrà dades personals tant de l'advocat com dels seus clients o, fins i tot, de tercers. Tenint en compte que la contractació del servei "Google Drive" implica l'acceptació de les condicions de servei generals, no pot descartar-se, malgrat que en el "centre d'ajuda" citat no s'hi faci referència, que la resta del clausurat d'aquestes condicions siguin aplicades igualment per Google i que, per tant, s'empri la informació dipositada amb qualsevol altra finalitat.

- En termes similars es manifesta "Microsoft Onedrive". Pel que es desprèn de les seves condicions de servei, Microsoft diferencia el contingut que el client (l'advocat) "col·loca" en els seus serveis (apartat *"Contenido"*) de la informació personal que recopila (apartat *"Privacidad"*). Això podria fer pensar erròniament que en el "contingut" no hi consten dades personals, però, en atenció a la definició que d'aquest se'n fa per Microsoft *("El contenido incluye todo aquello que cargue, o almacene, o transmita mediante los servicios, como datos, documentos, fotografías, vídeos, música, mensajes de correo electrónico o mensajes instantáneos"*), això no seria així. És important tenir en compte aquest aspecte perquè Microsoft preveu expressament que *"cuando usted*

carga su contenido en los servicios, acepta que su contenido se podrá modificar, adaptar, guardar, reproducir, distribuir y mostrar en la medida necesaria para protegerle a usted y para proporcionarle, proteger y mejorar los productos y servicios de Microsoft".

- Per la seva part, "Dropbox" sembla més clar en afirmar que "*sigues conservando la propiedad absoluta sobre tus cosas. No pretendemos asumir ningún derecho de propiedad sobre ellas. Estas Condiciones no nos otorgan ningún derecho sobre tus cosas ni tu propiedad intelectual, excepto los derechos limitados necesarios para ejecutar los Servicios (...)"* (apartat *"Tus cosas y tu privacidad"*). Malgrat que aquesta previsió desapareix en la política de privacitat actualitzada en data 24 de març de 2014, cal dir que trobem una previsió en termes similars en les condicions d'ús, també actualitzades (apartat "*Tu contenido y tus permisos*").

Per tant, cal tenir present que clàusules d'aquest tipus impliquen que qualsevol informació personal que el client (l'advocat) decideixi emmagatzemar en els servidors, especialment de les companyies Google i Microsoft, podrà ser emprada per aquestes empreses per a qualsevol ús sense requerir el consentiment, aspecte particularment problemàtic pel que fa a continguts d'arxius privats o confidencials. Per tant, com ja s'ha fet esment en aquest informe, convé examinar minuciosament quina informació personal es vol emmagatzemar-hi.

Dit això, pel que fa a la **finalitat concreta** del tractament de les dades, tant "Google Drive" com "Microsoft Onedrive" i "Dropbox" contenen escasses previsions al respecte en les seves condicions d'ús i remeten, en aquest sentit, a les respectives polítiques de privacitat.

Per tant, l'advocat que contracta aquests serveis ha de tenir present que accepta que Google, Microsoft o Dropbox, segons el cas, tracti la informació personal dipositada de conformitat amb la política de privacitat que estableix la mateixa companyia, una política de privacitat que, recordem, pot ser modificada en qualsevol moment (apartats *"Acerca de estas condiciones", "Otra información de privacidad importante"* i *"Cambios en nuestra Política de privacidad"*, respectivament).

A banda d'aquest fet, cal assenyalar que, tret de "Dropbox", es tracta d'unes polítiques de privacitat dissenyades per al conjunt de serveis prestats per Google i Microsoft i no així específicament per als serveis "Google Drive" i "Microsoft Skydrive", de tal manera que les previsions contemplades en elles podrien no encaixar amb el funcionament previst per a aquests tipus de serveis.

A més, sovint empren 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, Microsoft o Dropbox) i, alhora, posa en evidència que el responsable (l'advocat) 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 Drive", "Microsoft Onedrive" i "Dropbox" poden accedir a dades personals de què pugui disposar el client (l'advocat), ja sigui perquè les facilita directament (dades personals de l'advocat i la informació personal dels seus clients que l'advocat decideix emmagatzemar-hi), ja sigui perquè és Google, Microsoft o Dropbox qui les obté quan el client (l'advocat) utilitza els seus serveis (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 tres proveïdors examinats: proporcionar i millorar el servei prestat.

Tot i que pugui ser raonable que el client (advocat) 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 (de *"cloud storage"* en aquest cas), 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 (a aquest aspecte ja s'ha fet referència en aquest informe en l'apartat anterior relatiu a la seguretat de les aplicacions d'accés als serveis).

Es fa aquesta consideració perquè la finalitat del tractament de les dades al·legada (la prestació i millora del servei prestat) no és l'única finalitat pretesa pels prestadors de serveis de "*cloud storage"* examinats en el present cas, tal i com s'explica a continuació:

- Per exemple, en el cas de "Google Drive" s'estableix, en l'apartat "*Cómo utilizamos los datos recogidos",* 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 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.(...)."*

- De la mateixa manera, "Microsoft Onedrive" preveu, en l'apartat *"Cómo utilizamos su información personal",* que *"la información captada a través de uno de los servicios de Microsoft puede combinarse con la información captada a través de otros servicios de Microsoft para ofrecerle una experiencia más coherente y personalizada en sus interacciones con nosotros (...), también podemos utilizar la información para comunicarnos con usted (...)"* i que "*(...) la información que captamos puede utilizarse para ayudar a mejorar los anuncios que ve haciéndolos más relevantes para usted."*

- En el cas concret de "Dropbox", cal assenyalar que, si bé en la política de privacitat vigent fins el 24 de març de 2014 s'explica amb força detall la finalitat per la qual es recullen les dades personals (*"proporcionar y mejorar nuestro Servicio; administrar tu uso del Servicio; entender mejor tus necesidades e intereses; personalizar y mejorar tu experiencia; proporcionar u ofrecer actualizaciones de software y anuncios de productos")*, a més de donar informació sobre les dades de geolocalització i sobre l'ús de Google Analytics, en la nova versió d'aquesta política de privacitat tal explicació s'omet, de tal manera que la nova redacció no permet conèixer amb claredat quin ús farà "Dropbox" de les dades personals que recopila. Tan sols estableix que podrien compartir la informació però que no la vendran a tercers amb fins publicitaris ni de cap altre tipus (apartat *"Con quién"*). Òbviament, resulta més ajustat a la normativa de protecció de dades les previsions de la política de privacitat anteriors a la seva actualització.

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 (apartats *"Transparencia y elección"* per a "Google Drive" i *"Visualización de anuncios"* per a "Microsoft Skydrive" i *"Cómo utilizamos la información personal"* per "Dropbox", si bé aquest apartat s'omet en la nova política de privacitat de "Dropbox"). 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 les previsions de Google i de Microsoft de combinar la informació personal, escau assenyalar que cap d'elles 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 emmagatzemada a "Google Drive" o a "Microsoft Onedrive" amb la d'altres serveis de què pugui disposar l'advocat. En qualsevol cas, cal fer avinent que això comportaria un ús de les dades personals que excedeix àmpliament les expectatives que el client podria esperar de la utilització d'un servei de *"cloud storage"*.

A la vista d'aquestes consideracions, cal tenir en compte, a l'hora de contractar aquests serveis, que les actuacions previstes per Google, Microsoft i Dropbox (especialment, per Google i Microsoft) poden excedir la finalitat principal per la qual l'advocat els 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, 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), però les condicions d'ús examinades són poc precises al respecte:

- Google únicament estableix que, en cas d'interrupció del servei i sempre que sigui possible, *"(...) te informaremos con suficiente antelación y te permitiremos extraer la información del Servicio."* (apartat "*Cómo modificar y cancelar nuestros Servicios*"), sense aportar més informació ni esclarir què succeeix en cas de deixar d'emprar el seu servei, en aquest cas, de "Google Drive".

- Per la seva part Microsoft disposa que, en cas de cancel·lació del servei, *"podremos 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.

- Pel que fa a Dropbox, les noves condicions d'ús varien les previsions fins ara establertes en aquest sentit. Abans s'establia que, en cas de suspensió o finalització del servei, *"intentaremos comunicártelo por adelantado y ayudarte a recuperar tus datos, aunque pueden darse casos (como infracciones reiteradas o flagrantes de estas Condiciones, una orden judicial o riesgo para otros usuarios) en los que tendríamos que aplicar una suspensión immediata"* (apartat *"Finalización de los Servicios*"). A partir del 24 de març de 2014 només s'estableix que, si bé el client és lliure de deixar d'emprar els serveis en qualsevol moment, Dropbox es reserva *"el derecho a suspender o dar por terminados los servicios en cualquier momento a nuestra discreción y sin previo aviso"*. S'afegeix que els comptes gratuïts inactius durant dotze mesos consecutius poden ser cancel·lats i eliminats.

Així mateix, 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 (apartat "*Cómo acceder a tus datos personales y actualizarlos*" en el cas Google; apartat *"Otra información de privacidad importante"* en el cas de Microfost; o apartat *"Conservación de datos"* en el cas de Dropbox).

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, en la seva vessant d'exactitud (article 4.5 LOPD).

D'altra banda, si bé encara relacionat amb aquest 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).

IX

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

Dit això, es considera convenient fer unes consideracions addicionals en relació amb altres previsions de les condicions d'ús establertes per aquests proveïdors de serveis de *"cloud storage".*

Cal tenir en compte, a l'hora de contractar aquests serveis, que, pel que fa al tractament de dades personals, tant Google com Microsoft i Dropbox només es **comprometen** a complir aquelles previsions que s'hagin fixat en els respectius acords subscrits amb el client (l'advocat) i en els termes que s'hagin indicat (no ofereixen cap garantia addicional ni condició explícita ni implícita de cap classe). Previsions que, com s'ha fet esment al llarg d'aquest informe, 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 d'aquests serveis de *"cloud storage":*

- D'acord amb l'apartat *"Acerca de estas condiciones"* de les condicions de servei aplicables a "Google Drive", 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'advocat) a la jurisdicció exclusiva dels tribunals federals o estatals del comtat de Santa Clara (Califòrnia, Estats Units).

- El mateix succeeix en el cas de "Dropbox", si bé amb alguna puntualització. Fins el 24 de març de 2014, Dropbox preveia, en l'apartat *"Condiciones legales generales"* de les seves condicions de servei, que tota reclamació originada o relacionada amb l'acord subscrit havia de resoldre's exclusivament en els tribunals federals o estatals del comtat de San Francisco (Califòrnia, Estats Units). A partir de l'entrada en vigor de l'actualització de les condicions, s'imposa l'arbitratge com a sistema per resoldre les disputes que puguin sorgir, si bé es dóna l'opció de renunciar a aquesta submissió arbitral. Ara bé, en aquells casos en què es consideri no aplicable l'arbitratge, les reclamacions continuaran havent-se de resoldre en els tribunals federals o estatals de San Francisco (apartat "*Resolución de disputas"*).

- Únicament Microsoft preveu, en l'apartat *"Entidad contratante de Microsoft"* de les condicions del servei "Microsoft Skydrive", 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 en què Microsoft dirigeixi els seus serveis.

Cal tenir en compte, per tant, que en cas d'existir un desacord entre el client (l'advocat) i Google o Dropbox sobre els termes i/o les condicions de l'acord subscrit per a la prestació dels serveis "Google Drive" o "Dropbox", respectivament, la normativa aplicable, a criteri d'aquestes empreses, 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'advocat, 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 informe en relació amb la consulta plantejada, es fan les següents,

Conclusions

L'adhesió de Google, Microsoft o Dropbox als principis de l'acord "U.S.-E.U. Safe Harbor" pressuposa, a data d'avui, que les dades personals emmagatzemades per l'advocat en els seus serveis "Google Drive", "Microsoft Onedrive" i "Dropbox", respectivament, seran tractades amb determinades garanties i condicions de seguretat, tot i que podria resultar insuficient, en els termes exposats en aquest informe.

Així mateix, disposar de la certificació ISO/IEC/27001, o de qualsevol altra certificació o estàndard internacional en matèria de seguretat, no és garantia suficient del compliment de les mesures de seguretat del RLOPD. A data d'avui, no existeix cap certificació per a proveïdors en el núvol que verifiqui, de manera específica, el compliment estricte de les dites mesures. La certificació ISO/IEC/27001, o qualsevol altra, hauria d'anar acompanyada de la auditoria prevista a la normativa de protecció de dades.

Els riscos que suposa l'ús dels serveis "Google Drive", "Microsoft Onedrive" i "Dropbox" per a l'advocat que decideix emmagatzemar-hi documentació relativa als seus clients estarien relacionats, tant amb el funcionament propi d'aquests serveis, com amb les diferents aplicacions i plataformes que permeten l'accés i la gestió dels arxius emmagatzemats, atès que presenten certes vulnerabilitats que podrien donar lloc a l'afectació de la informació emmagatzemada, especialment en relació amb la seva confidencialitat, com a conseqüència d'accessos no autoritzats, en els termes exposats en aquest informe.

Barcelona, 28 de març de 2014