Dictamen en relació amb la consulta plantejada per un Col·legi professional, sobre si les aplicacions de missatgeria instantània Whatsapp, Telegram i Nepcom compleixen amb la Resolució 280/XI del Parlament de Catalunya

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit provinent d'un Col·legi professional en què es fa referència al Dictamen CNS 55/2016, en relació amb una consulta formulada per un Grup del Parlament de Catalunya sobre l'adaptació dels sistemes de missatgeria exprés als requisits que es deriven de la Resolució 280/XI del Parlament de Catalunya, sobre l'ús de serveis de comunicació pel Govern (BOPC 220, de 27 de setembre de 2016).

Com indica la consulta, el Dictamen 55/2016, fa una anàlisi general de diverses qüestions i d'indicadors que poden ser especialment rellevants, des de la perspectiva de la protecció de dades, de cara a ser tinguts en compte per les administracions públiques, en relació amb la utilització de sistemes de missatgeria instantània (en endavant, SMI).

La consulta desitja conèixer si concretament les aplicacions de missatgeria instantània Whatsapp, Telegram i Nepcom, que segons la consulta són utilitzades per algunes administracions públiques catalanes, complirien amb la Resolució 280/XI, del Parlament de Catalunya (en endavant, la Resolució 280/XI).

Analitzada la petició, vista la normativa aplicable i l'informe de l'auditor de Sistemes d'Informació i el 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 Dictamen CNS 55/2016, citat, fa una anàlisi general de diverses qüestions i d'indicadors que poden ser especialment rellevants, des de la perspectiva de la protecció de dades, de cara a ser tinguts en compte per les administracions públiques, en relació amb la utilització de sistemes de missatgeria instantània (SMI), a la llum de les indicacions que la Resolució 280/XI adreça al Govern.

S'ha de dir que moltes de les qüestions que cal analitzar en aquest dictamen obeeixen precisament a l'anàlisi que ja es va fer, de manera general en aquell dictamen, per la qual cosa, en el plantejament general de l'anàlisi que ara es demana, ens remetem al que ja vam exposar en aquell dictamen.

Segons la Resolució 280/XI, del Parlament de Catalunya, sobre l'ús de serveis de comunicacions pel Govern (BOPC 220, de 27 de setembre de 2016):

"El Parlament de Catalunya insta el Govern a:

a) Utilitzar mitjans de comunicació que ofereixin garanties de seguretat i privacitat quan es tractin dades sensibles o confidencials.

b) Utilitzar preferiblement els mitjans i els serveis de comunicació que siguin econòmicament més assequibles, d'acord amb llur nivell de seguretat i de privacitat.
c) Assegurar-se que els prestadors de serveis de comunicació assumiran i compliran llurs deures de col·laboració si són requerits per òrgans de l'Administració i la justícia.
d)** Fomentar l'ús dels **sistemes de missatgeria exprés** que utilitzen els organismes públics dependents de la Generalitat, les administracions públiques, els cossos i forces de seguretat, etc. Les **característiques d'aquests sistemes han d'ésser:

1a. Que tinguin una política de privacitat d'acord amb la legislació vigent en matèria de protecció de dades.

2a. Que tinguin els servidors en el territori de la Unió Europea.

3a. Que llurs centres de càlcul (data centers) compleixin certs estàndards de seguretat, com la norma ISO 27001.

4a. Que practiquin la transparència incorporant informació sobre els accessos per part dels cossos policials i sobre els contractes d'encàrrec del tractament amb els prestadors.

e) Incorporar les noves mesures que estableix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, del 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades, d'acord amb els terminis establerts."

D'entrada, cal reiterar les consideracions de tipus general fetes en el Fonament Jurídic V del Dictamen CNS 55/2016, en relació amb les previsions dels apartats a), b) i c) de la Resolució 280/XI, aplicables a qualsevol sistema de comunicació que puguin emprar les administracions públiques en llurs comunicacions amb els ciutadans. Això, sens perjudici de les concrecions que es puguin fer més endavant en relació amb els sistemes de missatgeria instantània (SMI), a què es refereix específicament la consulta.

Pel que fa a la gratuïtat dels serveis oferts, tant **Whatsapp** com **Telegram** ofereixen gratuïtament el respectiu servei de missatgeria. Pel que fa a **Nepcom**, segons la informació del seu web, s'ofereixen dues modalitats: la llicència "Nepcom Lite", que és la llicència que s'ofereix a l'usuari per defecte a l'instal·lar l'aplicació, també gratuïta, i que permet un ús limitat de l'aplicació, i la llicència "Nepcom", de pagament, que ofereix una utilització més completa del servei. Per tant, la gratuïtat del servei, al menys parcialment, és comuna als tres SMI. En qualsevol cas, pel que fa a la gratuïtat dels serveis (ap. b) de la Resolució 280/XI), ens remetem a consideracions fetes en aquell dictamen i, en especial les implicacions que això pot tenir respecte el model de negoci de l'entitat que ofereix aquest servei de missatgeria.

Pel que fa a la incorporació de les noves mesures que estableix el Reglament general de protecció de dades (UE) 2016/679 (en endavant, RGPD), a que fa esment l'apartat e) de la Resolució, si bé fins a la plena aplicació de l'RGPD (25 de maig de 2018), segueix vigent el règim previst a l'LOPD i a l'RLOPD, a partir de la data esmentada resulta obvi que caldrà donar compliment al conjunt de les obligacions que imposa el nou marc normatiu de protecció de dades personals, no ja com una opció sinó com una obligació.

III

La consulta fa referència a tres sistemes de missatgeria instantània (Whatsapp, Telegram i Nepcom) que, segons s'afirma en la consulta, serien *"utilitzades per algunes AAPP catalanes"*.

Podem entendre per missatgeria instantània la forma de comunicació en temps real entre dues o més persones, basada principalment en text, que s'envia a través de dispositius connectats a una xarxa com ara Internet. Això, sens perjudici que alguns d'aquests sistemes, permetin adjuntar missatges de text, i arxius d'imatges, vídeo i àudio, és a dir, altres continguts a banda del propi missatge de text. Així mateix, aquests SMI permeten a més d'utilitzar la missatgeria bàsica, els usuaris d'alguns d'aquests sistemes poden fer videoconferències, crear grups més o menys nombrosos, "xats", i compartir-hi informació, arxius o contactes.

La consulta no especifica si la consulta relativa al grau de compliment de la Resolució 280/XI, per tres SMI en particular, podria tenir relació amb el context de les comunicacions que poden produir-se entre advocats i clients (àmbit professional d'actuació propi de l'entitat que formula la consulta), o si es refereix, com sembla dels propis termes de la consulta, en general, a les administracions públiques catalanes.

Fem avinent que aquesta Autoritat ha analitzat en diverses ocasions (Dictàmens CNS 24/2013, CNS 57/2013, i CNS 36/2014), la utilització de diverses tecnologies i sistemes de comunicació, entre d'altres, determinats sistemes de missatgeria instantània, en l'àmbit professional específic de les relacions entre advocat i client.

Com ha posat de manifest l'Autoritat, quan una administració pública o, per extensió, qualsevol altre responsable (art. 3.d) LOPD i art. 4.7 RGPD), vol emprar un SMI per a les seves comunicacions amb tercers (ciutadans, clients...), haurà de tenir en compte, d'entrada, quina finalitat, quines dades es tractaran, quin tipus de comunicació vol establir, en relació amb quin servei o prestació, a qui va adreçada la comunicació, etc.

Des de la perspectiva de la protecció de dades no té les mateixes implicacions utilitzar un SMI per a donar, rebre o fer consultes sobre una informació general o "innòcua" des del punt de vista de la protecció de dades (informació sobre l'estat del trànsit o sobre determinats serveis municipals...), que l'ús que es realitza per comunicar un possible fet delictiu, un accident (comunicacions a cossos policials, a serveis sanitaris, ambulàncies, serveis a persones dependents que requereixen atenció domiciliària, etc), o quan es tracti de comunicacions relacionades amb persones menors d'edat o col·lectius vulnerables, els quals poden ser, per diversos motius, objecte d'especial protecció i atenció per part de les administracions públiques. Moltes comunicacions amb les administracions o entitats diverses, no comporten un tractament d'informació especialment protegida o sensible.

En d'altres casos, la transmissió de dades de salut a serveis assistencials, o entre una víctima d'una agressió i els cossos de seguretat, etc, suposaria transmetre informació que la normativa protegeix especialment (Considerant 75 i article 9 RGPD). Ens remetem, en aquest sentit, a les consideracions fetes en el FJ VIII del Dictamen 55/2016, pel que fa a les particularitats que, des de la perspectiva de la protecció de dades personals, pugui presentar la utilització dels dits sistemes en l'àmbit professional propi de l'entitat que formula la consulta.

Aquest és un factor a tenir en compte a l'hora de considerar si els SMI objecte de consulta poden ser més o menys adequats a les exigències de la Resolució 280/XI.

Cal tenir en compte que les solucions que ofereixen les empreses prestadores de SMI poden ser de diferents tipus, així:

En primer lloc, pot tractar-se d'una solució comercial de tipus públic (l'aplicació és descarregada per l'usuari i s'instal·la de manera lliure, i es poden començar a utilitzar les seves funcions sense més requisits que disposar del dispositiu, l'aplicació i la

connexió a la xarxa); en segon lloc, pot tractar-se d'una solució comercial que tingui l'opció d'ús corporatiu, i que s'implanta de tal manera que només podria servir per intercanviar missatges entre persones autoritzades per l'organització; finalment, pot tractar-se d'una solució corporativa pròpia, feta *ad hoc* per a una determinada empresa o organització, sens perjudici que pugui estar basada en solucions comercials (com les que han dut a terme, per exemple, algunes universitats per a ús intern).

Per la informació disponible, les tres apps objecte de consulta (Whatsapp, Telegram i Nepcom) s'inclourien en el primer grup (solucions comercials d'ús públic), si bé pel que fa a Nepcom, en el seu web s'explica que és una aplicació de missatgeria instantània *"que pretén facilitar la comunicació entre professionals",* de manera que sembla més adreçada a col·lectius professionals, com a canal de comunicació de tipus corporatiu.

Les administracions públiques poden utilitzar canals de comunicació unidireccionals per oferir informació als ciutadans, o poden permetre establir una comunicació bidireccional, de manera que l'usuari o afectat no només rep informació d'interès, sinó que comunica les pròpies dades a l'administració. Així, per exemple, si es vol facilitar una informació general sobre serveis al conjunt dels ciutadans (xarxes de transport públic, informació sobre tramitació de serveis...) podria ser adient utilitzar un SMI que sigui àmpliament conegut i utilitzat per la ciutadania, com podria ser Whatsapp o Telegram. En canvi, si el número d'usuaris del SMI es preveu més limitat (el personal al servei d'un ens o administració, per exemple), una solució corporativa feta *ad hoc* per a determinat col·lectiu, podria ser més adient.

El major o menor grau de sensibilitat de la informació personal que en cada cas es tracti pot fer aconsellable o no un determinat SMI, a la llum de les previsions de la Resolució 280/XI i la normativa de protecció de dades, però els termes generals en què es fa la consulta no permeten analitzar supòsits concrets.

Als efectes de les previsions de la Resolució 280/XI, no es pot establir una categorització o recomanació general a favor d'un dels SMI objecte de consulta, ja que en funció del dit context (tipus de comunicació, persones a qui s'adreça, servei o prestació a la que es vol donar compliment amb la utilització del SMI, major o menor "sensibilitat" de la informació que presumiblement es comunicarà, etc...), la seva utilització podria resultar adequada, des de la perspectiva de la normativa de protecció de dades.

Per tant, no correspon en aquest dictamen validar, recomanar o, pel contrari, desaconsellar amb caràcter general la utilització o no per part de qualsevol de les administracions públiques o altres ens sotmesos a l'àmbit de competència d'aquesta Autoritat (art. 3 Llei 32/2010), d'un determinat instrument de comunicació (SMI), per al conjunt de les seves comunicacions amb els ciutadans que, insistim, poden ser de naturalesa molt diversa

IV

Dit això, en el context de la Resolució 280/XI, es poden fer les següents consideracions de tipus general.

Segons informació disponible als web respectius **Nepcom** seria una solució oferta per una empresa amb un establiment principal a la Unió Europea, mentre que en el cas de **Whatsapp** i Telegram sembla desprendre's que el seu establiment principal estaria fora de la Unió Europea. Pel que fa a **Telegram**, en l'apartat de FAQ *("Dónde se establece Telegram?*"), s'indica *que "El equipo de desarrollo de Telegram tiene su*

base en Dubai". A banda d'això, i d'algunes referències a anteriors ubicacions de l'equip de Telegram (San Petersburgo, Berlín, Londres o Singapur), en el web no es troba informació específica sobre la seu de Telegram a efectes de resolució de conflictes, ni a la jurisdicció o el marc normatiu que l'empresa considera aplicable, en cas de conflicte o reclamació dels seus usuaris.

Sigui com sigui, d'acord amb l'article 3 de l'RGPD en els tres supòsits seria d'aplicació el RGPD. Així, pel que fa a les empreses amb un establiment principal fora de la Unió, cal tenir en compte que d'acord amb l'article 3.2 de l'RGPD, aquesta norma serà d'aplicació també a les empreses que ofereixin aquests serveis a ciutadans residents a la Unió Europea, encara que no estiguin establertes dins la Unió Europea:

> *"2.El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*
> *a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o*
> *(...)."*

Com ha fet avinent aquesta Autoritat (FJ IV del Dictamen 55/2016), les empreses titulars dels SMI (com ara Whatsapp, Telegram o Nepcom) decideixen quin tractament fan de les dades dels usuaris que s'instal·len la corresponent aplicació per utilitzar el servei, i estableixen les condicions d'ús corresponents. Aquestes empreses, com es desprèn de la informació que difonen en els seus respectius llocs web (Whatsapp.com; Telegram.com; Nepcom.es), són responsables del tractament de dades personals dels usuaris, als efectes de la normativa de protecció de dades (art. 4.7 RGPD i art. 3.d) de l'LOPD).

En la mesura que l'ús de SMI comporti un tractament d'informació personal, aquest tractament ha de sotmetre's als principis i garanties de la protecció de dades, és a dir, el RGPD, que va entrar en vigor el 25 de maig de 2016, i que serà aplicable a partir del 25 de maig de 2018 (art. 99 RGPD). Això, sens perjudici que, fins a la data indicada, s'haurà de tenir en compte la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), així com el Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de l'LOPD (RLOPD).

De fet, ja abans de l'entrada en vigor de l'RGPD les autoritats de control europees en matèria de protecció de dades ja han hagut de requerir alguna d'aquestes empreses pel que fa al compliment de la normativa europea de protecció de dades. Serveixin com exemple les actuacions dutes a terme en els darrers anys per diferents autoritats europees de protecció de dades en relació amb el tractament de dades d'usuaris a la UE per part de Whatsapp, a les que s'ha fet esment en ocasions anteriors (ens remetem al Dictamen CNS 24/2013), com ara els informes i investigacions de diverses Autoritats de protecció de dades (Autoritat de Protecció de Dades d'Holanda i Autoritat federal de Canadà, de gener de 2013). També cal recordar la intervenció del Grup de Treball de l'Article 29, a través de diversos escrits adreçats a Facebook i Whatsapp (27 d'octubre de 2016, 16 de desembre de 2016 i 24 d'octubre de 2017), en què s'han posat de manifest diverses deficiències en el mecanisme de prestació del consentiment dels usuaris arran de la previsió de comunicació de dades a Facebook, ("*Facebook family of companies*"), per un conjunt de finalitats que inclouen el màrqueting i la publicitat. I en relació amb aquesta qüestió, més recentment (15 de març de 2018), cal destacar Resolució R/00259/2018, de l'Agència Espanyola de Protecció de Dades (AEPD), en què es sanciona a Whatsapp per cedir a Facebook

dades personals sense el consentiment adequat dels afectats, qüestió sobre la que tornarem més endavant, així com actuacions d'investigació recent dutes a terme per altres Autoritat de protecció de dades, com ara l'Autoritat francesa (CNIL), en relació amb el tractament de dades dels usuaris per part de Whatsapp (desembre de 2017).

V

Fetes aquestes consideracions generals, cal descriure breument les tres aplicacions (apps) a què es refereix la consulta, i les seves característiques principals, en base a la informació disponible en les seves respectives pàgines web.

Segons el seu web, **Whatsapp** és una aplicació de missatgeria multiplataforma que permet enviar i rebre missatges de text i arxius de tipus imatge, vídeo i àudio, de forma gratuïta. A més d'utilitzar la missatgeria bàsica, els usuaris de Whatsapp poden crear grups (xats), de fins a 50 contactes, de manera que l'usuari, que en serà l'administrador, pot incloure a la resta d'usuaris per a participar en el xat. Whatsapp també permet als usuaris enviar entre els membres del xat imatges, vídeos i missatges d'àudio. Pel que fa al seu funcionament, Whatsapp utilitza la connexió a Internet de l'usuari, per que aquest pugui enviar missatges als seus contactes, segons s'explica en les FAQ (preguntes freqüents). En el moment que algú s'instal·la Whatsapp en un terminal, la plataforma accedeix a tots els telèfons de contacte emmagatzemats en aquest terminal, independentment de si tenen instal·lat o no Whatsapp.

Pel que fa a **Telegram,** segons el seu web, és una aplicació que *"siempre será gratuita inspirada en código abierto obert* (open source), *la más segura gracias a su cifrado fuerte y basado en la nube".* Segons el web, Telegram permet compartir amb els contactes fotos, documents, vídeos de fins a 1 gb, i mantenir converses amb fins a 200 contactes, crear "supergrups" de fins a 30000 persones, o utilitzar canals per a fer difusions a audiències il·limitades.

Segons el web, Telegram també permet la possibilitat de tenir "xats secrets" i que s'autodestrueixin els missatges en qüestió de segons ("*Cualquier conversación vídeos fotos o frases estarán disponibles durante un tiempo que previamente podrá configurar para que el contenido sea autodestruido."*). Pel que fa al seu funcionament, segons el web: *"Los chats secretos son establecidos entre los dos dispositivos en los que fue creado. Esto significa que todos esos mensajes no están disponibles en la nube y no se puede acceder a ellos desde otros dispositivos. Por otra parte, los chats secretos están también atados a la sesión actual en tu dispositivo. Si finalizas tu sesión y vuelves a iniciarla, perderás todos tus chats secretos."*

Pel que fa a **Nepcom,** és una aplicació de missatgeria instantània per a ús en entorns empresarials que pretén facilitar la comunicació entre professionals, especialment entre els que han de tractar informació confidencial i sensible. Segons el web, Nepcom proporciona xifratge d'extrem a extrem de les converses, i aplica el protocol de xifratge OTR (off the record messaging), de manera que els missatges no es guarden en els servidors. També ofereix converses efímeres que s'autodestrueixen, a través del "mode confidencial", que permet que determinada informació no es mantingui en els dispositius després de ser compartida. El *"mode d'autodestrucció de missatges"* de Nepcom no ve activat per defecte, de manera que l'usuari l'hauria d'activar en obrir un xat. En activar-lo, l'altre contacte rep una sol·licitud d'activació d'aquest mode i, en cas que accepti farà que tots els missatges es destrueixin tan bon punt l'usuari tanqui la conversa o l'aplicació.

El web afegeix que *"Nepcom no fa ús de l'agenda de contactes del telèfon",* ja que el sistema funciona mitjançant invitacions entre les persones.

Dit això, cal recordar que aquest dictamen no s'emet en exercici de les funcions de control d'aquesta Autoritat (potestat d'inspecció i potestat sancionadora, *ex. art*. 5, apartats j) i k) Llei 32/2010), ni amb la realització de plans d'auditoria (art. 5.l) Llei 32/2010), de manera que aquesta Autoritat no ha dut a terme cap tipus de verificació material, ni tasques d'investigació o auditoria respecte del funcionament de les apps sobre les que es consulta, verificació que seria necessària per constatar el compliment d'alguns dels requisits de la Resolució 280/XI per part dels SMI referits, com ara les prestacions, la ubicació real dels servidors o l'efectiu compliment de les mesures de seguretat a què es fa referència en aquest dictamen. Les consideracions d'aquest dictamen tenen en compte, principalment, la informació que les pròpies empreses difonen en els seus web, respecte el tractament de dades que duen a terme, sens perjudici d'altra informació d'abast general.

A més, pel que fa a **Whatsapp** i **Telegram**, existeix a disposició del públic en general una ingent quantitat de literatura, opinions, articles de premsa, valoracions d'experts, anàlisis comparatives, rànquings, valorant "pros i contres" d'aquests i altres SMI (com ara Line, Signal, etc....), respecte el nivell de seguretat i privacitat d'aquestes apps, sistemes d'encriptació, vulnerabilitats, etc. Sens perjudici que no és objecte d'aquest dictamen contrastar la fiabilitat d'aquests estudis comparatius –ni tampoc la informació que les pròpies empreses difonen als seus llocs web-, és cert que tota aquesta informació pot ser d'utilitat respecte Whatsapp i Telegram, abastament analitzades. En canvi, pel que fa a **Nepcom**, atesa la seva recent creació i l'àmbit geogràfic en què es desenvolupa el propi servei, no hi ha encara opinions o crítiques provinents de tercers externs i independents a la pròpia empresa, que puguin tenir-se en consideració –més enllà del que pugui constar en el propi web-, de manera que només s'ha pogut tenir en compte, bàsicament, la informació que genera la pròpia empresa.

Fem notar que el jurat del Premi de Protecció de Dades en el Disseny 2017, que concedeix aquesta Autoritat, va reconèixer amb un accèssit l'aplicació de missatgeria instantània Nepcom. En qualsevol cas, la valoració que en el seu moment hagi fet el jurat del Premi no permet comparar aquesta aplicació amb les altres dues aplicacions de missatgeria analitzades, que no van presentar-se al Premi. Per altra banda, s'ha de tenir en compte que es tracta, en qualsevol cas, d'un Premi que valora la incorporació, des d'un bon inici de la protecció de dades en el disseny d'aplicacions, i que no prejutja el resultat final d'altres solucions que malgrat no haver incorporat la protecció de dades des del primer moment del seu disseny, l'hagin pogut esmenar o millorar amb posterioritat.

Fetes aquestes consideracions, a continuació ens referirem d'una banda a les previsions, en els SMI en qüestió, sobre el consentiment dels usuaris i la informació que se'ls facilita i, d'altra banda, a diferents qüestions referides a la seguretat que apliquen aquests SMI, en relació amb les previsions de la resolució del Parlament i el marc normatiu derivat de l'RGPD.

VI

El consentiment de les persones afectades

Com ha destacat abastament aquesta Autoritat, un dels indicadors clau a l'hora de valorar determinats SMI es refereix al control de l'usuari respecte el tractament de les

seves dades, el qual s'articula a partir del principi de consentiment (art. 4 LOPD). Segons l'article 4.11 de l'RGPD, el consentiment de l'interessat és: *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;"*

Pot ser habitual que els SMI incloguin condicions generals o estàndards, que les empreses fixen i, sovint, modifiquen de manera unilateral, sense deixar marge d'opció a l'usuari. En aquests casos es constata un clar desequilibri contractual entre les parts.

Si s'examinen les condicions d'ús i la política de privacitat de Whatsapp, de Telegram i de Nepcom, es pot comprovar que en totes tres s'hi inclouen condicions generals o estàndards, que aquestes empreses fixen i, si s'escau modifiquen, de manera unilateral i que no deixen marge a la possibilitat d'elecció per part de l'usuari.

Així, pel que fa a **Whatsapp**, el web inclou afirmacions com ara: *"A menos que un acuerdo mutuo entre tú y nosotros estipule lo contrario, nuestros Términos constituyen todo el acuerdo entre tú y nosotros en relación con WhatsApp y nuestros Servicios, y sustituyen cualquier acuerdo previo."* I afegeix: *"Podemos modificar o actualizar estos Términos. Te avisaremos de las modificaciones a nuestros Términos, según sea apropiado, y actualizaremos la fecha de "Última modificación" en la parte superior de nuestros Términos. Al continuar tu uso de nuestros Servicios, confirmas tu aceptación de nuestros Términos, con cualquier modificación. Si no estás de acuerdo con nuestros Términos y con sus modificaciones, debes dejar de usar nuestros Servicios. Por favor revisa nuestros Términos de vez en cuando."* En l'apartat "Información legal de Whatsapp", les previsions són igual o més àmplies, respecte la possibilitat establerta unilateralment, de recopilar, usar, conservar i compartir la informació de l'usuari de Whatsapp considera *"de bona fe que és raonable fer-ho"*, per a diferents finalitats.

Pel que fa a la informació disponible en el web de **Telegram**, en l'apartat de *"Privacy policy"* (disponible en anglès), trobem afirmacions com ara que Telegram només emmagatzema les dades que són necessàries perquè l'aplicació funcioni, metre l'usuari vulgui utilitzar Telegram. D'aquesta afirmació general, sembla desprendre's que, des del moment que l'usuari s'instal.la l'app, ha d'acceptar que Telegram utilitzi aquella informació que consideri "necessària per prestar el servei", sense més concreció. Ara bé, sens perjudici del llenguatge més directe i fins i tot col·loquial que, en general, utilitza Telegram al seu web, cal posar de manifest que, de la informació disponible, no es desprèn quins tractaments estaria consentint o no l'usuari, ni per a quines finalitats.

Pel que fa a **Nepcom**, en l'apartat d'avís legal del web, s'explica que *"Nepcom se reserva el derecho de modificar cualquier tipo de información que pudiera aparecer en el sitio web, sin que exista obligación de preavisar o poner en conocimiento de los usuarios dichas obligaciones, entendiéndose como suficiente con la publicación en el sitio web Nepcom."* L'apartat de *"Términos y condiciones"* afegeix que: *"El hecho de descargar, instalar, copiar o utilitzar el software de algun modo, implica la aceptación plena y sin reservas de todas y cada una de las condiciones de los presentes "Términos y condiciones" así como el "Aviso legal"(...), la "Política de Privacidad" (...) y la "Política de cookies" (...). Si no acepta (...) le rogamos que se abstenga de descargar y/o utilitzar el software."*

Així doncs, una característica que podríem considerar comuna als tres SMI sobre els que es formula la consulta, és que es parteix d'una situació de desequilibri entre el

responsable del SMI i l'usuari, qüestió a la que fa una especial atenció el GT 29, com explicita en el recent document de *"Guidelines on Consent under Regulation 2016/679",* de 28 de novembre de 2017.

Ara bé, tot i que pot ser raonable que l'usuari hagi d'acceptar necessàriament un cert nivell de tractament de les seves dades en la mesura que això pugui ser necessari des d'un punt de vista tècnic per a la prestació del servei de missatgeria, això no implica que resulti adequada la prestació d'un consentiment general i, podríem dir, "indiscriminat", en el sentit d'una acceptació incondicionada, per utilitzar les dades de l'usuari o de terceres persones per a finalitats que no resulten estrictament necessàries per a la prestació del servei.

En qualsevol cas, com es desprèn de les previsions de l'RGPD, l'acceptació necessària d'un cert grau de tractament de dades per poder fer ús dels SMI, no justificaria en cap cas un abús per part de les empreses, en el sentit de considerar que l'usuari atorga un consentiment (que, en els termes de l'RGPD, difícilment podria considerar-se "lliure"), per utilitzar no només la informació que els requeriments tècnics d'utilització del SMI poden justificar, sinó també altra informació de l'usuari i de tercers, per a finalitats diverses i, sovint, no explicitades. En aquest sentit, resulta especialment il·lustratiu l'exemple que proposa el dit document del GT 29 (apartat 3.1): *"Una aplicación móvil para edición de fotos solicita a sus usuarios tener activada su localización de GPS para el uso de sus servicios. La aplicación también les dice a sus usuarios que usará los datos recopilados con fines publicitarios de comportamiento. Ni la geolocalización ni la publicidad conductual en línea son necesarios para la provisión del servicio de edición de fotografías y van más allá de la prestación del servicio principal proporcionado. Dado que los usuarios no pueden usar la aplicación sin dar su consentimiento para estos fines, no se puede considerar que el consentimiento sea otorgado libremente."*

En aquest context, el RGPD (Considerants 32 i 43) estableix la rellevància de la granularitat en la prestació del consentiment, element que no resulta nou en l'àmbit que ens ocupa, doncs ja havia estat expressament citat i recomanat pel GT 29, en el seu Dictamen 2/2013, sobre apps en dispositius intel·ligents ("*Opinion 2/2013, on apps on smart devices*"), de 27 de febrer de 2013. Ens remetem, sobre això, a les consideracions fetes al FJ VI del Dictamen CNS 24/2013 d'aquesta Autoritat.

Com reitera el GT 29 en el document *"Guidelines on Consent under Regulation 2016/679",* citat, si un responsable fusiona o combina diverses finalitats amb el tractament de les dades, i no intenta aconseguir un consentiment granular o específic per a cadascun dels tractaments, hi ha una mancança en l'element de "lliure" consentiment. Segons aquestes mateixes Directrius del GT 29, l'establiment de mecanismes de prestació de consentiments separats per a diferents usos de les dades, permet considerar que es dóna un consentiment no només "lliure", sinó també "específic". Així, quan el tractament de les dades pretén aconseguir diverses finalitats, la solució per a donar compliment a les exigències d'un consentiment vàlid recau, precisament, en la granularitat. Fem notar que, segons l'article 7.4 RGPD, a l'avaluar si el consentiment es dóna lliurement, s'ha de tenir en compte si l'execució d'un contracte, inclosa la prestació d'un servei, es supedita al consentiment el tractament de dades personals que no són necessàries per a l'execució del dit contracte.

Amb tot això, als efectes d'aquest dictamen, cal tenir en compte si els usuaris dels SMI objecte de consulta, estan en disposició d'escollir lliurement per a quines finalitats presten el seu consentiment.

Pel que fa a **Whatsapp**, partim del que ja es va fer avinent en el FJ VI del Dictamen 24/2013, en el sentit que aquesta empresa no aplica un consentiment granular que permeti l'usuari seleccionar els contactes a què tindrà accés Whatsapp. En aquest sentit, com s'explicita en el web (apartat "Actualizaciones clave", subapartat "Términos de Servicio de Whatsapp"): *"Libreta de direcciones. Nos proporcionas regularmente los números de teléfono de los usuarios de Whatsapp y los demás contactos que tienes en la libreta de direcciones de tu teléfono móvil."* En l'apartat "política de privacidad y datos del usuario", s'afegeix que Whatsapp recopila informació automàticament: ("*Uso e información de registro (…). Esto incluye información sobre tu actividad (como la forma en que usas nuestros Servicios, la forma en que interactúas con otros mediante nuestros Servicios y datos similares). Información sobre transacciones (…). Información sobre tu conexión y dispositivos. Recopilamos información específica de tu dispositivo (…). Esto incluye la información del sistema operativo, información sobre el navegador, la dirección IP e información de la red móvil…).Información sobre mensajes de estado. Recopilamos información sobre tus cambios de mensaje de estado y en línea en nuestros Servicios, "estado de conexión", "estado de última conexión"(…)"*). A això s'afegeix, en el mateix apartat, que també es rep informació de tercers, entre d'altres, de proveïdors externs: *"Estos proveedores externos pueden proporcionarnos información sobre ti en ciertas circunstancias; por ejemplo, las tiendas de aplicaciones pueden enviarnos informes que nos ayudan a diagnosticar y solucionar problemas con el servicio."*

Vistes aquestes i altres previsions del web de Whatsapp, sembla clar que no s'aplica un consentiment granular, de manera que l'usuari pugui seleccionar els contactes a què té accés Whatsapp, i no només això, sinó que tampoc sembla fàcilment gestionable, per part dels usuaris, la possibilitat de determinar quina utilització es fa de la seva informació, vist que fins i tot tercers (com ara proveïdors no identificats) estan en disposició de facilitar informació de l'usuari a Whatsapp, sense que això depengui del seu consentiment.

A més, pel que fa a Whatsapp, cal tenir en compte novament la recent sanció imposada per l'AEPD, per haver comunicat dades a Facebook sense haver obtingut un consentiment vàlid dels usuaris (a banda de la sanció imposada a Facebook per tractar aquestes dades per a les seves pròpies finalitats, sense consentiment). Recordem que Whatsapp fou adquirida, l'any 2014, per Facebook. L'any 2016, després d'una actualització de les condicions de servei i la política de privacitat, es va procedir a compartir la informació dels usuaris amb Facebook. Per la informació disponible, als nous usuaris de Whatsapp no se'ls donava l'opció de negar-se a la cessió de les seves dades a Facebook i, pel que fa als usuaris que ja tenien instal·lada l'aplicació, només podien refusar que la informació cedida a Facebook fos utilitzada per a finalitats de "*millora de l'experiència amb els productes i la publicitat de Facebook*", però no amb altres finalitats no concretades.

Aquest canvis de les condicions d'ús de Whatsapp (veure apartats: *"Actualizaciones clave"* i *"Información a los usuarios de la UE",* al web), van ser motiu d'anàlisi per part de diverses Autoritats de protecció de dades de la UE. Cal esmentar especialment, pel seu interès, els escrits que el GT 29 va adreçar a Whatsapp (16 de desembre de 2016, i 24 d'octubre de 2017), posant de manifest la seva preocupació per les noves polítiques d'aquesta empresa, segons les quals aquest SMI compartiria informació dels usuaris amb el grup d'empreses de Facebook ("*Facebook family of companies*"), per un conjunt de finalitats que inclouen el màrqueting i la publicitat. A criteri del GT 29, entre d'altres qüestions, les mancances detectades en la informació facilitada als usuaris en relació amb aquesta cessió de dades (de Whatsapp al grup d'empreses de Facebook) posen en dubte la validesa del consentiment dels afectats. En concret, el

GT va posar de manifest que l'enfocament de forçar a l'usuari a acceptar una comunicació de dades que no seria, estrictament, necessària, de manera que, en cas de no fer-ho, l'empresa impossibilita l'ús del servei ("*take it or leave it" approach*), no permet considerar que hi hagi un consentiment adequat.

Resulta evident, com es desprèn de les consideracions i advertiments provinents de les Autoritats de protecció de dades europees en els darreres anys i, més recentment, de la Resolució sancionadora de l'AEPD, a la que ens remetem, que Whatsapp no hauria aplicat el consentiment parcel·lat en relació amb les cessions de dades dels usuaris a tercers, i no hauria permès als afectats excloure determinada informació personal de les dites cessions a Facebook, que a tenor de les recents opinions i resolucions de diverses Autoritats de protecció de dades, serien cessions clarament innecessàries i, per tant haurien hagut d'estar subjectes al consentiment específic dels usuaris.

Pel que fa a **Telegram,** com es preveu en el seu web (apartat de "Privacy policy", no disponible en castellà): *"Telegram utiliza números de teléfono como identificadores únicos, por lo que es fácil cambiar de otras aplicaciones de mensajería (SMS, WhatsApp, etc.)…. Le pedimos su permiso antes de sincronizar sus contactos. Almacenamos sus contactos para avisarle tan pronto como uno de sus contactos se registre en Telegram y para que muestre correctamente los nombres en las notificaciones. Solo necesitamos el número y el nombre (el primero y el último) para que esto funcione y no almacenamos otros datos sobre sus contactos."*

Tot i que Telegram explica que demana permís per sincronitzar els contactes del telèfon ("*We ask your permission before syncing your contacts"*), d'entrada, i tenint en compte la informació disponible, és com a mínim dubtós que l'usuari pugui -en cas de no consentir la sincronització esmentada-, utilitzar l'app. De la informació de conjunt facilitada al web, no sembla que sigui així.

En qualsevol cas, de la informació disponible de Telegram, aquesta empresa simplement "informa" del tractament que fa (veure apartat de política de privacitat), amb afirmacions com les esmentades, segons les quals mai comparteixen dades amb ningú, o que no emmagatzemen més informació que la necessària perquè l'app funcioni. Ara bé, en aquests termes, no es pot considerar que Telegram articuli un consentiment granular.

Dit això, l'apartat de FAQ de Telegram, afegeix el següent:

"P: ¿A quiénes les puedo escribir?: Puedes escribirle a las personas que están en tus contactos del teléfono y que tienen Telegram. También puedes seleccionar un alias público para tu cuenta de Telegram. Otras personas podrán buscarte y encontrarte a través de ese alias y enviarte mensajes aunque no conozcan tu número. Puedes conocer más sobre los alias aquí.

P: ¿Cómo puedo saber quién de mis contactos tiene Telegram?: Tus contactos, que tienen Telegram, son mostrados en la parte alta de tus Contactos de la aplicación. También tienen fotos."

Per tant, sembla clar que Telegram tracta la informació relativa als contactes de l'usuari. No es troben en el web altres mencions explícites o, al menys, aclaridores, sobre el consentiment que es demana a l'usuari, per a aquest tractament (i sincronització) dels contactes.

Si ens atenim a la informació del web, pel que fa a l'ús de la llibreta d'adreces i contactes de l'usuari que fa Telegram, sembla clar que per utilitzar el servei l'usuari ha de facilitar necessàriament el seu número de telèfon i el dels seus contactes. En definitiva, com es desprèn de la informació disponible, Telegram accedeix als números de telèfon dels contactes de l'usuari, en termes similars no només a Whatsapp, sinó a moltes altres apps de missatgeria instantània. Per tant, en aquest cas també es constata la manca de consentiment granular.

Dit això, pel que fa a Telegram, en relació amb les cessions de dades previstes, les FAQ expliciten que: *"En Telegram pensamos que los dos componentes más importantes de la privacidad en internet deberían ser: (...) 2. Proteger tus datos personales de terceras partes, como vendedores, anunciantes, etc."*

L'apartat de FAQ *"Políticas de Privacidad"* (que remet a informació disponible en anglès), afegeix que: *"Nunca compartimos tus datos con nadie. Hasta el día de hoy, hemos divulgado 0 bytes de datos de usuarios a terceros, incluidos los gobiernos."*

En qualsevol cas, la contundència amb què Telegram nega qualsevol comunicació, sembla contradir-se amb algunes afirmacions extretes del mateix document de polítiques de privacitat, com ara que: *"Información de envío: Cuando ingresa información de envío en el proceso de realizar un pedido, lo enviamos directamente al desarrollador de bot de comerciante",* o que: *"Puede borrar toda la información de pago asociada con su cuenta en cualquier momento (…). Si elige eliminar su información de pago, borraremos la información de envío almacenada y los tokens de pago de todos los proveedores y le pediremos a los proveedores que eliminen la información de su tarjeta de crédito que almacenan."* De la informació disponible, sembla que difícilment Telegram podrà demanar als proveïdors (tercers) que esborrin informació, si no hi ha hagut cessió prèvia de dades. Si bé en l'apartat "*Credit card information"* del document *"Privacy policy"* de Telegram, l'empresa afirma que *"No accedim ni conservem la informació de la targeta de crèdit",* per la informació disponible no podem descartar que alguna d'aquesta informació sigui efectivament emmagatzemada i tractada per Telegram.

Pel que fa a **Nepcom**, d'una banda, el web explica que *"Nepcom no fa ús de l'agenda de contactes del telèfon",* ja que el sistema funciona mitjançant invitacions entre les persones. També s'afegeix que: "*No es necesario facilitar el número de teléfono, la agregación se realiza a través de e-mail (ID). De este modo, el usuario podrá mantener conversaciones con Nepcom sin necesidad que otros usuarios conozcan su número de teléfono y de este modo evitar recibir llamadas no deseadas. El usuario podrá incluir o modificar el número de teléfono de forma opcional en cualquier momento. Una vez añadido, todos sus contactos podrán visualizarlo."* L'apartat de *"Política de privacidad"* indica que: *"Los datos de geolocalización y agenda de contactos a los que accedemos bajo consentimiento expreso, se tratarán únicamente si el usuario desea compartir su ubicación con otro usuario/s y si desea comunicar un contacto de su agenda con otro usuario/s."*

Dit això, en el document FAQs s'explica que: *¿Qué significa el apartado "Contactos sugeridos" dentro del menú opciones?: Nepcom contempla sugerencias de contactos para facilitar así su agregación a los miembros de una misma compañía u organización. A parte del buscador "Agregar contacto", "Contactos sugeridos" muestra todas aquellas personas que usen la aplicación y tengan en su ID el mismo domino (sean de la misma empresa) que el del usuario. Recordamos que para poder agregar a un contacto, este tiene siempre que aceptar la solicitud."*

En relació amb la informació que recull Nepcom, el web explica que: *"Obtenemos mediante formulario de registro la información mínima e indispensable. En dicho formulario usted facilitará los siguientes datos: e-mail, nombre y apellidos, fecha de nacimiento y género. De forma plenamente voluntaria, usted puede además facilitar la siguiente información: nombre de su empresa, cargo, teléfono, notas (cualquier texto de máx. 140 caracteres) y foto de perfil. Al facilitarlos, dichos datos se encontrarán disponibles para sus contactos."*

Atesa la informació disponible, sembla que Nepcom accediria (com altres SMI) a l'agenda de contactes –cosa que semblaria necessària, entre d'altres coses, per poder dur a terme el "suggeriment de contactes" a l'usuari, pel que fa a aquells que pertanyin a l'empresa o organització-. Sembla que perquè Nepcom pugui seleccionar i suggerir determinats contactes a l'usuari, haurà d'accedir a l'agenda de contactes. Si és així, semblaria que aquest tractament entra en contradicció amb l'afirmació, explicitada en el web, que Nepcom *"no fa ús de l'agenda de contactes del telèfon".*

Dit això, en el mateix apartat de "Política de privacidad" es preveu que: *"Podremos utilizar sus datos para contactarle, tanto por vía electrónica como no electrónica, para obtener su opinión sobre el servicio prestado y, ocasionalmente, para notificarle cambios, desarrollos importantes de la aplicación y ofertas o promociones de Nepcom en el caso que sea usuario de Nepcom. Puede revocar en cualquier momento su consentimiento remitiendo un escrito con el asunto "Baja" a info@nepcom.es."*

En línia amb el que s'ha apuntat, els tractaments que es preveuen en aquest darrer apartat no serien estrictament necessaris per a la prestació del servei (notificar ofertes o promocions...) de manera que hauria d'estar sotmès a un consentiment previ ("opt-in"), sens perjudici que es prevegi la possibilitat de revocació del consentiment, previsió que es valora positivament.

Encara en relació amb Nepcom, el web informa que: *"Nepcom no lleva a cabo ninguna cesión o comunicación de datos ni dentro ni fuera de la UE."* Ara bé, fent extensibles algunes consideracions fetes sobre Telegram en relació amb una afirmació similar, fem notar que de la informació disponible (el propi web), Nepcom preveu el tractament, entre d'altres, de dades bancàries dels usuaris, de manera que, per la informació disponible, podrien ser objecte de comunicació a l'entitat bancària corresponent als efectes oportuns, cosa que, de ser així, posaria en qüestió la dita previsió sobre la inexistència total de cessions. En qualsevol cas, de produir-se alguna cessió, mancaria en la informació disponible al web informació precisa sobre la petició de consentiment als afectats.

VII

El dret d'informació i el principi de transparència

Atès que, pel mer fet d'instal·lar les apps objecte de consulta es produeix una acceptació incondicionada de l'usuari a determinades condicions d'ús que l'empresa estipula de forma unilateral -amb les matisacions que s'han apuntat en relació amb les apps objecte de consulta-, resulta rellevant, als efectes de la consulta, comprovar si l'usuari rep una informació prou detallada del tractament de les seves dades, i del que comporta acceptar la instal·lació de l'app.

Segons disposa l'article 5.1.a) de l'RGPD, les dades han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat.

El RGPD exigeix que els responsables donin compliment a aquest principi de transparència, segons el qual *"toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento."* (Considerant 39 RGPD).

El principi de transparència, vinculat en el RGPD als principis de licitud i de lleialtat, engloba específicament el deure d'informar els afectats sobre una sèrie de qüestions, en els termes de l'article 13 RGPD. En concret, a partir de la data d'aplicació de l'RGPD, caldrà informar dels següents aspectes (article 13 RGPD): les dades de contacte del delegat de protecció de dades; la base jurídica del tractament; els interessos legítims perseguits en què es fonamenti el tractament; la intenció de transferir les dades a un país tercer o organització internacional i la base per a fer-ho; el termini durant el qual es conservaran les dades; l'existència del dret a demanar la portabilitat; el dret a retirar en qualsevol moment el consentiment que s'hagi prestat; si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte; el dret a presentar una reclamació davant una autoritat de control; l'existència de decisions automatitzades, incloent la lògica aplicada i les seves conseqüències.

Les clàusules que no tenen en compte el grau de comprensió del ciutadà mig, sinó que, fins i tot, abusen de terminologia legal, no serien admissibles, segons afirma el GT29, en el document de Directrius sobre el consentiment, citat: *"Al solicitar el consentimiento, los controladores deben garantizar que utilicen un lenguaje claro y sencillo en todos los casos. Esto significa que un mensaje debe ser fácilmente comprensible para la persona promedio y no solo para los abogados. Los controladores no pueden usar largas políticas de privacidad ilegibles o declaraciones llenas de jerga legal.*"

A més, la informació que sovint faciliten les empreses (no només en relació amb els SMI sinó, en general, en relació amb serveis oferts per via electrònica), als seus usuaris, sovint resulta extensa i confusa, de manera que un determinat apartat del web remet a d'altres apartats del mateix web, en els que es concreta, s'amplia, es matisa i, fins i tot en algun cas, es duplica la informació ja facilitada primerament, de manera que es genera en l'usuari un efecte de fatiga ("*click fatigue*", en expressió del GT 29), que dificulta la comprensió adequada de la informació que el responsable ha de facilitar, per donar compliment al "consentiment informat" que exigeix el RGPD. Segons el GT 29: *"En el contexto digital, muchos servicios necesitan datos personales para funcionar, por lo tanto, los sujetos de datos reciben múltiples solicitudes de consentimiento que necesitan respuestas a través de clics y golpes cada día. Esto puede dar como resultado un cierto grado de fatiga de clic: cuando se encuentra demasiadas veces, el efecto de advertencia real de los mecanismos de consentimiento está disminuyendo. Esto da como resultado una situación donde las preguntas de consentimiento ya no se leen. Este es un riesgo particular para los sujetos de datos, ya que, típicamente, se solicita el consentimiento para acciones que, en principio, son ilegales sin su consentimiento. El RGPD impone a los responsables la obligación de desarrollar formas de abordar este problema."*

En definitiva, com ja s'ha fet avinent en ocasions anteriors (i és un argument que el RGPD reforça), els termes en què el responsable ha de donar informació als afectats exigeix un alt estàndard a nivell de claredat i d'accessibilitat (art. 7.2 i Considerant 32 RGPD).

Pel que fa a **Whatsapp**, ja s'ha apuntat la problemàtica específica arran de la manca d'informació respecte els destinataris de la informació i les conseqüències d'aquesta compartició d'informació amb Facebook. Les autoritats de protecció de dades han qüestionat reiteradament la indefinició de les referències a "empreses afiliades" per part de Whatsapp, entre d'altres qüestions. El fet que aquesta empresa tingui la seva seu (i remeti qualsevol conflicte amb els usuaris) a jurisdicció nord-americana, planteja una mancança clara en relació amb la informació que caldria donar sobre l'aplicabilitat de la normativa europea de protecció de dades, qüestió a la qual ja ens hem referit, i la possibilitat d'exercir els drets que preveu. La informació de contacte per presentar queixes o reclamacions, tant al web ("*Información legal de Whatsapp. Contáctanos*"), com a través del web de l'escut de privacitat, citat, seria una adreça de Califòrnia, cosa que, a efectes pràctics, pot dificultar l'exercici de drets, com s'ha fet avinent. Val a dir que, arran de la problemàtica amb Facebook, el web de Whatsapp va publicar informació específicament adreçada *"als usuaris de la UE",* que, sens perjudici que pugui ser d'interès, no inclou referències a l'exercici de drets. Vist l'article 13 RGPD, fem notar que, entre d'altres qüestions, també falta informació sobre el representant del responsable i el delegat de protecció de dades -DPD- (arts. 37 a 39 RGPD i, especialment, les Directrius sobre delegats de protecció de dades (DPD) del GT 29, de 5 d'abril de 2017).

Pel que fa a **Telegram**, algunes de les consideracions apuntades en relació amb la informació que caldria donar als afectats, com ara les relatives a l'exercici de drets, les dades de contacte del representant o DPD, tampoc estan previstes, al menys, en la informació consultada que l'empresa posa a disposició dels usuaris. La informació sobre la seu o seus de Telegram, sobre el responsable, els seus representants a la UE o el DPD, són clarament insuficients. En qualsevol cas, als efectes que interessen, malgrat que l'empresa consideri, amb afirmacions breus i explícites del web, que en cap cas fa "cap cessió de dades", o que Telegram no emmagatzema dades, això no eximeix d'informar sobre qüestions com ara l'exercici de drets, informació que no es troba al web de Telegram, al menys per la informació consultada. En definitiva, la informació d'aquesta empresa, en els termes de l'article 13 RGPD, podria considerar-se insuficient. A tall d'exemple, per bé que el web de Telegram informa sobre l'eliminació del compte (FAQ), en el sentit que: *"Al borrar tu cuenta se remueven todos tus mensajes, grupos y contactos (...), toda tu información será vaciada desde nuestro sistema: todos los mensajes, grupos y contactos asociados a tu cuenta se borrarán",* i sens perjudici que aquesta pugui ser una previsió ajustada a la normativa de protecció de dades, això no exclou que el responsable hauria d'informar sobre el dret de cancel·lació dels usuaris i, per extensió, sobre l'exercici de la resta de drets.

Pel que fa a **Nepcom,** atesa la informació disponible, atès que la ubicació de la seu social de l'empresa es troba a Espanya, informacions que poden resultar d'especial utilitat per als usuaris, a efectes pràctics, com ara l'adreça de contacte o el DPD, es faciliten als usuaris a través del web. Fem notar que en l'apartat *"Aviso legal. Ap. 2, Protección de datos",* s'informa als usuaris de l'existència d'un fitxer de dades inscrit a l'AEPD. Pel que fa a la informació sobre l'exercici de drets, fem notar que es refereix als drets ARCO, informació que s'ajusta en el moment de fer aquest dictamen a l'article 5 LOPD, però que en el seu moment (a partir de l'aplicació de l'RGPD), caldria adequar aquestes previsions en el dit apartat. Sens perjudici d'això, fem notar que

l'apartat "*Política de Privacidad. Derechos de las personas interesadas",* d'aquest web, ja inclou referències als nous drets previstos al RGPD.

VIII

Els informes de transparència i els contractes d'encàrrec del tractament

L'apartat d.4) de la Resolució preveu com a element a exigir als SMI, o més exactament, a les empreses que en són responsables, que *"practiquin la transparència incorporant informació sobre els accessos pels cossos policials i sobre els contractes d'encàrrec del tractament amb els prestadors".*

Diverses empreses de comunicació i xarxes socials, publiquen periòdicament informes de transparència, en els quals s'informa els usuaris de qüestions diverses. Entre d'altres, i als efectes que interessen, es dóna informació agregada sobre sol·licituds d'informació de comptes d'usuaris que utilitzen aquell servei, per part d'autoritats judicials de tercers països, principalment, d'Estats Units. En els informes de transparència, i amb major o menor grau de detall, aquestes empreses informen sobre el número i tipologia de sol·licituds de dades d'usuaris per part d'autoritats d'altres països, el número de comptes sobre els que es demana informació, la freqüència amb la que l'empresa ha proporcionat la informació requerida, etc. El fet que les empreses difonguin aquests informes de transparència, pot ser un indicador a tenir en compte a l'hora de valorar si un SMI s'ajusta al marc normatiu europeu de protecció de dades.

Pel que fa a **Whatsapp,** d'entrada, fem notar que Whatsapp (i també Facebook) consta com a empresa adherida a l'Escut de Privacitat entre la UE i els Estats Units, segons informació disponible al web oficial: www.privacyshield.gov. Segons explicita la Guia de l'Escut de privacitat entre la UE i els Estats Units, i com ha recordat en anteriors dictàmens aquesta Autoritat, tenint en compte, entre d'altres, el Dictamen 1/2016, del GT 29, tota empresa adherida ha d'informar els interessats, entre d'altres, sobre *"la possibilitat que hagi de comunicar la seva informació personal per donar resposta a sol·licituds legítimes de les autoritats legítimes dels Estats Units."*

Per tant, el fet que Whatsapp, amb seu radicada als Estats Units, s'hagi adherit a l'Escut de privacitat, pot ser tingut en compte als efectes de donar compliment a la previsió de la Resolució 280/XI (ap. 4.d).

Dit això, segons el document *"Who has your back? Protecting your data from government requests"* (2015), de l'organització "*Electronic Frontier Foundation* (www.eff.org), Whatsapp no donaria suficient informació als usuaris respecte les sol·licituds d'informació per part de governs, si bé valora positivament la política de Whatsapp respecte la no utilització de *"backdoors"* ("portes del darrere", o inclusió obligada de programes que permetrien vulnerabilitats i debilitats del sistema de seguretat i, per tant, l'obtenció d'informació per part de tercers). L'EFF posa en valor la signatura per part de Facebook, en nom propi i de Whatsapp, de la carta de compromís de *l'Open Technology Institute*, segons la qual: *"Le instamos a que rechace cualquier propuesta de que las empresas estadounidenses debiliten deliberadamente la seguridad de nuestros productos (...). Ya sea que los llame "puertas de entrada" o " puertas traseras", la introducción de vulnerabilidades intencionales en productos seguros para el uso del gobierno los hará menos seguros contra otros atacantes (...)."*

Per contra, fem notar que l'informe d'Amnistia Internacional (AI): *"For your eyes only?. Ranking 11 technology companyies on encryption and human rights"* (https://www.amnesty.org/download/Documents/POL4049852016ENGLISH.PDF), atorga una puntuació alta en relació amb Facebook (incloent Whatsapp), pel que fa a la informació facilitada respecte el número de peticions d'informació rebudes de diferents governs. A més, AI afirma que no hi ha evidències que Facebook (i Whatsapp) hagin trencat la seva política d'evitar les citades "backdoors".

Dit això, el web de Whatsapp inclou directrius força detallades sobre aquesta qüestió (apartat *"Información para las fuerzas del orden a cerca de Whatsapp*"), sobre els requisits per a sol·licituds d'informació per a processos legals a Estats Units i per a processos legals internacionals, en aquest cas: *"Únicamente revelamos datos de las cuentas de nuestros usuarios de acuerdo con nuestras condiciones de servicio y la legislación aplicable. Para exigir la revelación del contenido de una cuenta, es posible que se deba presentar una solicitud de asistencia judicial mutua o un exhorto."* El web també és força concret –cosa que cal valorar positivament- respecte la informació que han d'incloure les sol·licituds ("*nombre de la autoridad que realiza la solicitud, número de placa o identificación del agente responsable…*"). Ara bé, més enllà d'això, no sembla que la informació facilitada al web de Whatsapp detalli la informació (agregada) sobre les peticions que efectivament s'haurien dut a terme. Qüestió que, d'altra banda, tampoc no caldria qualificar com "determinant" a l'hora de prejutjar si Whatsapp s'ajusta a l'apartat 4.d) Resolució 280/XI, ja que és ingent la quantitat d'informació que els mitjans de comunicació faciliten respecte aquesta mena de peticions d'informació tant a Facebook com a Whatsapp.

Pel que fa a **Telegram**, com s'ha apuntat, en el seu web s'explica que "Telegram no comparteix dades amb ningú". Segons les FAQ de Telegram: "*Los chats secretos usan el cifrado end-to-end. Por lo tanto, no tenemos ningún dato que pudiera ser revelado. Para proteger los datos que no están cubiertos con el cifrado end-to-end, Telegram utiliza una infraestructura repartida. Los datos de los chats en la nube son almacenados en múltiples centros de datos alrededor del mundo, que son controlados por diferentes entidades legales y que se extienden en diferentes jurisdicciones. Las claves de cifrado relevantes son divididas en partes y nunca se mantienen en el mismo lugar que los datos protegidos. Como resultado, varias órdenes de diferentes jurisdicciones son requeridas para forzarnos a entregar algún dato. Gracias a esta estructura, podemos asegurar que ningún gobierno o bloque de países afines puedan entrometerse en la privacidad de las personas y su libertad de expresión. Telegram puede ser forzada a entregar datos sólo si un problema es tan grave y universal que pueda pasar el escrutinio de diferentes sistemas legales alrededor del mundo. Hasta hoy, hemos entregado 0 bytes de datos de usuarios a terceros, incluyendo gobiernos."*

Ara bé, sens perjudici d'aquesta afirmació per part de la pròpia empresa, fem notar que, segons l'informe d'AI, esmentat, Telegram no ha publicat un informe de transparència detallat que concreti totes les peticions de governs que ha rebut, i la resposta que hauria donat en cada cas.

En qualsevol cas, en relació amb aquest particular, Telegram hauria afirmat, en resposta a la petició d'AI, que: *"Telegram pot confirmar que no ha introduït cap tipus de "portes del darrere" i que no ho farà en el futur. Ens oposem a les lleis anti-encriptació que s'han proposat en diversos països i refusem públicament la possibilitat d'implementar portes del darrere en el nostre servei (...)."*

En el web de Telegram s'afegeix que: "*¿Procesan solicitudes de datos?*: "(...) *Los datos de los chats en la nube son almacenados en múltiples centros de datos*

alrededor del mundo, que son controlados por diferentes entidades legales y que se extienden en diferentes jurisdicciones. (…).”

De fet, segons informacions de premsa (març de 2018), l'ens regulador de les telecomunicacions a Rússia hauria sol·licitat a Telegram l'entrega al Servei Federal de Seguretat, les claus de xifratge. Segons informació disponible, Telegram hauria considerat aquesta exigència impossible de complir, atesa la seva política de privacitat i la normativa aplicable.

En definitiva, es pot considerar que també Telegram posa a disposició dels usuaris informació sobre aquesta qüestió.

Pel que fa a **Nepcom**, el web facilita un *“Informe de transparencia”,* en el que es concreten els requeriments de dades de governs rebuts, els atesos, i els requeriments da dades sota ordre judicial rebudes -informa que no n'hi ha hagut cap, en tots els apartats-, i s'inclou -a diferència d'altres apps-, la data del dit informe (19 de gener de 2017), informació que cal valorar positivament.

Igualment, el web de Nepcom indica que: *“Manifestamos de forma pública que Nepcom no dispone de puertas traseras o vulnerabilidades que faciliten a terceras partes el acceso a datos personales.”*

Ara bé, a diferència d'altres apps com ara Whatsapp o Telegram, pel que fa a Nepcom no es disposa d'informacions o comprovacions de fonts d'informació externes a la pròpia empresa que permetin contrastar el compliment del dit compromís.

En definitiva, com a mínim a partir de la informació disponible respecte dels tres SMI als que fa referència la consulta, es pot concloure que les tres empreses donen informació sobre els accessos i sol·licituds d'informació que aquestes empreses han rebut per part de cossos policials o instàncies governamentals.

Pel que fa a la informació específica sobre **“contractes d'encàrrec del tractament amb els prestadors”** (apartat d.4) de la Resolució del Parlament), és a dir, contractes que les empreses responsables de SMI hagin pogut subscriure amb tercers, amb independència que es pugui qualificar o no com a comunicació, també és una informació que permet a l'usuari valorar d'una manera més acurada les repercussions del tractament que pot estar consentint.

Pel que fa a **Whatsapp**, segons la Resolució sancionadora de l'AEPD citada (FJ X), no pot considerar-se que l'accés a les dades d'usuaris de Whatsapp per part de Facebook respongui a un encàrrec dels tractament, ja que no s'hauria efectuat, segons la investigació duta a terme per l'AEPD, amb l'exclusiva finalitat de prestar un servei al responsable (Whatsapp). Als efectes que interessen en aquest dictamen, de la informació disponible no es pot concloure que Whatsapp informi als usuaris –en els termes que recomanaria l'apartat d.4) de la Resolució del Parlament-, sobre els contractes d'encàrrec del tractament amb prestadors de serveis. Pel que fa a **Telegram,** atesa la informació general de què es disposa, tampoc no consten referències específiques, al menys, per la informació consultada, a aquesta qüestió. Finalment, fem notar que el web de **Nepcom** inclou informació sobre un contracte d'encàrrec del tractament amb una tercera empresa.

IX

El model de seguretat i avaluació de l'impacte i les mesures de seguretat aplicades

El RGPD configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt, previstos a l'LOPD i RLOPD, sinó en determinar, arran d'una prèvia valoració dels riscos, quines mesures de seguretat són necessàries en cada cas, tenint en compte el tipus d'informació tractada (Considerant 83 RGPD).

Segons l'article 24.1 RGPD: *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."*

I segons l'article 32.1 RGPD: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (...)".*

És a dir, més que l'establiment de mesures concretes predeterminades en atenció al tractament i la informació tractada, l'RGPD estableix un esquema integral de seguretat, en el qual caldria determinar quines mesures aplicar, a partir de les característiques del tractament i d'una anàlisi de riscos en els termes de l'RGPD (Considerants 83 i 84).

Per tant, un element a tenir en compte és el model de seguretat que implementen les empreses responsables de SMI.

Per altra banda, l'RGPD preveu que en els casos en què sigui probable que les operacions de tractament de dades comportin un alt risc per als drets i llibertats de les persones físiques, el responsable del tractament ha de vetllar perquè es digui a terme una avaluació d'impacte relativa a la protecció de les dades que avaluï, en particular, l'origen, la naturalesa, la particularitat i la gravetat del risc (Considerant 84 RGPD). Els riscos per als drets i llibertats de les persones físiques són de gravetat i probabilitat variables (Considerant 75). Per tant, cal analitzar els riscos que es podrien presentar en un cas concret, i a partir d'això fer, si escau, una valoració o avaluació de l'impacte que suposarà utilitzar determinat SMI en un cas concret.

Ara bé, com ha quedat exposat, la consulta no fa menció al context en què es podrien utilitzar els SMI (quin tipus d'informació es tractarà, en relació amb quin servei o prestació, a quines persones o col·lectius va adreçada la comunicació, si podria ser habitual el flux informatiu d'informació sensible...). Com ha fet avinent aquesta Autoritat, quan aquests elements portin a considerar que podria existir una situació d'alt risc, convindria que les administracions que es plantegin la utilització de SMI per prestar determinats serveis als ciutadans, o per a comunicacions intra o interadministratives (recordem que la consulta no concreta aquests aspectes), realitzin una avaluació de l'impacte sobre la protecció de dades de caràcter personal, per tal de considerar quina solució de SMI és la que s'ajusta de forma més adequada als principis i garanties de la normativa de protecció de dades personals, en particular, en

l'àmbit de la seguretat que ofereixen (en relació amb la protecció de la confidencialitat de la informació tramesa, que no es produiran accessos no autoritzats, així com la integritat de la informació i l'autenticitat o garantia de l'autoria del missatge o de la identitat dels interlocutors.

Com va fer avinent aquesta Autoritat en el Dictamen 24/2013 (FJ VIII), un dels elements de seguretat clau a tenir en compte és el relatiu al **xifratge o encriptació** dels missatges (art. 104 RLOPD, i art. 32.1.a) RGPD), que puguin oferir les empreses responsables de SMI, sobre tot en aquells casos en què el servei que ofereixin les administracions públiques pugui comportar la comunicació de categories especials de dades.

Així, pot ser pertinent tenir en compte si els missatges s'envien xifrats entre els usuaris i els servidors (això implica que els missatges només es xifren en trànsit, i que en el servidor no resten xifrats i podrien ser accedits pel proveïdor, o per tercers no autoritzats que obtinguessin un accés maliciós als servidors), o si els missatges estan xifrats o encriptats "extrem a extrem", o punt a punt, de manera que només el receptor i l'emissor poden llegir els missatges, i que ni els proveïdors de telecomunicacions, ni d'Internet, ni l'empresa que facilita l'app o l'SMI poden accedir-hi. Aquests mecanismes d'encriptació són solucions de seguretat de la informació que poden aportar garanties en relació amb la confidencialitat de la informació, la integritat i l'autenticitat dels missatges.

En el Dictamen 55/2016 ja vam referir-nos a l'estudi l'elaborat "*Electronic Frontier Foundation"* (www.eff.org), que identifica i compara característiques de desenes d'aplicacions de missatgeria instantània, entre les quals, **Whatsapp** i **Telegram**. Si bé el propi web de EFF explicita que la versió 1.0 de l'anàlisi comparativa (amb actualitzacions fins a abril de 2016), requeriria d'actualitzacions posteriors, aquesta anàlisi continua resultant d'interès.

En concret, l'informe de l'EFF, citat, verifica els elements següents:

1. (*"Is your communication encrypted intransit?"):* Si els missatges s'envien xifrats entre els usuaris i els servidors. Això implica que els missatges només es xifren en trànsit i que en el servidor no resten xifrats, de manera que el proveïdor, o terceres persones no autoritzades que obtinguessin un accés maliciós als servidors, podrien accedir-hi;

2: *("Is your communication encrypted with a key provider doesn't have access to?").* Si els missatges estan xifrats "extrem a extrem", és a dir que en cap cas el proveïdor del servei pot accedir al contingut dels missatges, ni tan sols mentre estan emmagatzemats al servidor esperant que els usuaris els recullin;

3: *("Can you independently verify your correspondent's identity?*"). Si l'usuari té algun mecanisme per verificar que no s'està produint una suplantació de l'interlocutor amb el qual està intercanviant missatges;

4: ("*Are past communications secure if your keys are stolen?"*). Si és possible desxifrar missatges antics, si algú aconsegueix les claus de xifrat;

5: ("*Is the code open to independent review?"*). Si algú independent pot verificar el codi de l'aplicació, especialment la part de xifrat;

6: *("Is the crypto design well-documented?"*). Si la part de xifrat està ben documentada i experts independents hi poden accedir;

7: *("Has there been an independent security audit?"*). Si s'ha fet una auditoria independent de l'aplicació en els darrers dotze mesos.

Segons l'anàlisi de l'EFF, **Whatsapp** compliria amb sis d'aquests paràmetres (exceptuant el paràmetre núm. 5, referit a la possibilitat de fer revisió independent del codi de l'aplicació). Pel que fa a Telegram, l'estudi comparatiu de EFF destaca que, quan l'usuari utilitza els "xats secrets" de Telegram, es dóna compliment als set paràmetres analitzats per EFF, la qual cosa seria, com a mínim, un element a tenir en compte a l'hora de valorar positivament certes garanties de seguretat i privacitat implementades per Telegram. Pel que fa als xats secrets, segons el web de Telegram: *"Los chats secretos especiales de Telegram usan cifrado end-to-end, no dejan rastros en nuestros servidores, permiten la autodestrucción de mensajes y no admiten el reenvío de los mismos. Además, los chats secretos no son parte de la nube de Telegram y sólo se puede acceder a ellos a través del dispositivo de origen".*

Respecte el funcionament de l'autodestrucció de missatges a Telegram, el web *(apartat de "Privacy policy")* explica que: *"Los mensajes en Chats secretos pueden ordenarse para autodestruirse. En cuanto se lee dicho mensaje (aparecen 2 comprobaciones), comienza la cuenta regresiva. Cuando se acaba el tiempo, ambos dispositivos que participan en un chat secreto reciben instrucciones para eliminar el mensaje (foto, video, etc.)."* El web de Telegram explica que *"podrás tener fotos autodestruibles al estilo Snapchat".*

Fem notar que, a banda de **Telegram**, altres apps incorporen a les seves prestacions l'autodestrucció de missatges (entre d'altres, segons diversa informació disponible, Signal, Snapchat, Wickr, Bleep, Cover Me, SpeakOn, etc), possibilitat que resulta d'interès des de la perspectiva de la privacitat dels usuaris.

De manera similar a l'estudi de l'organització EFF, l'informe d'AI *"For your eyes only?.* (...)*",* citat, focalitza la seva anàlisi en l'ús de l'encriptació d'extrem a extrem, i examina cinc criteris:

1. Si els SMI analitzats –entre els que es troben Facebook, inclòs el servei de missatgeria de Whatsapp, i Telegram-, reconeixen, en les seves polítiques, possibles amenaces per a la privacitat dels usuaris;

2. Si estableixen per defecte l'encriptació d'extrem a extrem;

3. Si informen els usuaris de les amenaces a la privacitat i de l'ús d'encriptació;

4. Si són transparents a l'hora d'informar sobre les peticions d'informació d'usuaris que formulen alguns governs;

5. Si publiquen detalls tècnics dels sistemes d'encriptació.

En còmput global, tant Facebook (inclòs Whatsapp) com Telegram, que haurien atès la sol·licitud d'informació d'AI, obtenen en aquest informe una valoració alta (obtenen la primera i la tercera posició, amb 73 i 67 punts sobre 100, respectivament). En concret, i sens perjudici d'alguna menció que farem més endavant, l'informe d'AI valora positivament el protocol d'encriptació extrem a extrem dels dos SMI.

Pel que fa a **Whatsapp**, l'informe citat d'AI destaca que disposa d'encriptació d'extrem a extrem per defecte, en el sentit que és aplicable automàticament a totes les

comunicacions. Així, en el document *"Whatsapp Encryption Overview"* (6 de juliol 2017), que es troba al web de Whatsapp, s'indica que els missatges (incloent xats, grups, imatges, vídeos, arxius i missatges de veu) entre usuaris de Whatsapp estan protegits per un protocol d'encriptació d'extrem a extrem, de manera que ni Whatsapp ni tercers poden llegir-los, i només es poden desencriptar pel destinatari. El document afegeix que els servidors de Whatsapp no tenen accés a les claus privades dels usuaris, els quals tenen l'opció de verificar les claus per assegurar la integritat de les seves comunicacions.

En l'article *"WhatsApp rolls out end-to-end encryption to its over one billion users",* de l'Organització EFF, disponible en traducció al castellà: https://www.eff.org/es/deeplinks/2016/04/whatsapp-estrena-cifrado-de-fin-fin-para-mas-de-un-billon-de-usuarios), s'analitza el sistema de xifratge de Whatsapp, que es qualifica com un sistema fort. Segons aquest document: *"En un documento técnico publicado el 4 de Abril, WhatsApp describe en detalle el intercambio criptográfico subyacente que se produce cuando los usuarios mensajean entre sí. Está basado en el protocolo de la aplicación Signal (bautizado Axolotl) desarrollado por Open Whisper Systems, y que utiliza el algoritmo Double Ratchet para proporcionar una confidencialidad directa incluso si las llaves de sesión se ven comprometidas. Esto significa que si un adversario es capaz de descubrir las claves de cifrado utilizadas por la aplicación, esto no pone en peligro las comunicaciones realizadas con los contactos en el pasado, ya que seguirá estando protegida.(…)."*

Així, per la informació disponible (inclòs el seu web), Whatsapp incorpora el xifratge d'extrem a extrem, de manera que només l'emissor i el receptor (i no Whatsapp) poden llegir el missatge. Aquest tipus de xifratge estaria activat per defecte per a tots els usuaris que utilitzen les darreres versions de l'app, i no es podria deshabilitar.

Ara bé, cal fer notar que, segons altra informació disponible, si bé el xifratge d'extrem a extrem de Whatsapp ofereix garanties, també es detecten certes mancances que podrien portar a que aquestes mesures no fossin prou operatives. En concret, l'informe d'AI, citat, hauria detectat que Whatsapp no informa els usuaris que, si es fan còpies de seguretat al núvol, aquesta informació no estaria xifrada. Aquests informes també posen de manifest que, si s'utilitza el navegador per accedir a Whatsapp, l'encriptació extrem a extrem no es podria garantir. Aquestes són, doncs, vulnerabilitats detectades, segons la informació disponible, que caldria tenir en compte.

A això afegim que, segons el document *"Where Whatsapp Went Wrong: EFF's Four Biggest Security Concerns"*, de l'organització EFF (octubre de 2016), posa de manifest altres vulnerabilitats, com ara que els usuaris no reben per defecte la notificació (i sol·licitud d'acceptació) de canvi de la clau d'encriptació dels seus contactes, o que l'accés a Whatsapp mitjançant els navegadors web no es consideren prou segurs. En qualsevol cas, el propi informe d'EFF recomana l'activació de totes les opcions de seguretat que Whatsapp permet, com la desactivació de les còpies de seguretat al núvol, o l'activació de notificació de canvi de claus, mesures que, en conseqüència, sembla que podrien pal·liar algunes vulnerabilitats detectades.

Pel que fa a **Telegram,** aquesta empresa assegura que el seu sistema de xifratge és pràcticament invulnerable, fins al punt d'oferir una recompensa econòmica a qui pugui desxifrar el codi. Segons el web*: "Estamos basados en el protocolo MTProto (...), construido con algoritmos testeados en el tiempo, para hacer la seguridad compatible con las entregas de mensajes a alta velocidad y confiabilidad en conexiones débiles."*

Així mateix, s'explica que tota la informació (ja siguin textos, arxius multimèdia o documents), són encriptats de la mateixa manera. Pel que es desprèn de l'informe d'AI, citat, Telegram disposa d'encriptació d'extrem a extrem però, per la informació disponible, no la té instal·lada per defecte i per tant, no s'aplicaria per defecte. En conseqüència, és important comprovar si Telegram informa d'aquesta qüestió als usuaris, per tal que puguin implementar l'encriptació, cosa que podria contrarestar –en principi- la vulnerabilitat que suposa que l'encriptació no estigui prevista per defecte. Segons els informes consultats, Telegram no adverteix clarament als usuaris que les seves dades podrien quedar compromeses si utilitzen el servei sense encriptació d'extrem a extrem. Sobre això, el web de l'empresa explica que: *"Tenemos dos capas de cifrado seguro. El cifrado servidor-cliente es usado en los Chats en la Nube (privados y grupales). Los chats secretos usan una capa adicional de cifrado cliente-cliente. Todos los datos, sin importar su tipo, son cifrados de la misma manera, ya sean textos, multimedia o archivos."* Sobre els xats secrets (que, seguint el que es desprèn, entre d'altres, de l'informe d'AI, sí incorporaria el xifratge per defecte), el web de Telegram explica que: *"Los chats secretos están pensados para quienes quieren más seguridad que una persona promedio. Todos los mensajes en los chats secretos usan un cifrado end-to-end. Esto significa que sólo tú y tu receptor pueden leer esos mensajes; nadie más puede descifrarlos, incluyéndonos a nosotros en Telegram. Los mensajes no pueden ser reenviados desde los chats secretos. Y, cuando eliminas mensajes en tu lado de la conversación, la app en el otro lado del chat secreto tendrá como orden eliminarlos también."*

Vista la informació de conjunt que Telegram facilita sobre els seus xats secrets (que, per la informació disponible, incorporarien el xifratge per defecte), podria considerar-se que l'usuari té prou informació.

En aquest sentit, pel que fa a la claredat i extensió de la informació que proporciona Telegram, les FAQ exposen que*: "Si tienes razones para preocuparte de tu seguridad personal, te recomendamos usar sólo chats secretos en aplicaciones oficiales o, al menos, con código abierto verificable para tu información sensible, de preferencia con autodestrucción. También recomendamos activar la verificación en dos pasos y establecer un código de acceso fuerte para bloquear tu aplicación. Puedes encontrar ambas opciones en Ajustes > Privacidad y seguridad."*

Pel que fa a **Nepcom**, el seu web indica que *"Este sitio web cumple con la normativa española de protección de datos y garantiza el cumplimiento íntegro de las obligaciones dispuestas, así como la implementación de las medidas de seguridad contempladas en el art. 9 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) así como su Reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre."* Convindria, com s'ha apuntat, tenir en compte que l'RGPD canvia l'esquema d'aplicació de mesures de seguretat previst a l'LOPD i RLOPD. L'afirmació que aquest SMI compleix les mesures previstes a l'article 9 de l'LOPD vigent, sense més concreció, no permet conèixer quines mesures ha valorat l'empresa que requereix el tractament de les dades dels usuaris. En línia amb aquesta qüestió, fem notar que el web de Nepcom fa referència al compliment de la certificació ISO/27001 en matèria de seguretat –que cita la Resolució del Parlament-, si bé no és objecte d'aquest dictamen verificar el compliment d'aquesta certificació, ni es disposa d'altra informació, externa a l'empresa, que permeti contrastar el compliment del contingut d'aquesta certificació per part de Nepcom.

Segons el web de Nepcom, aquest SMI utilitza en alguns casos el "xifratge" ("*el protocolo de cifrado utilizado es el TLS/SSL. Cifra únicamente el canal de*

comunicación entre el terminal y el servidor, y viceversa."), i en d'altres, el "xifratge total" ("*el protocolo de cifrado utilizado es el OTR (Off The Record). Cifra toda la comunicación desde un terminal al otro, de extremo a extremo. Mediante este modo, incluso los propios servidores de Nepcom no pueden descifrar la comunicación y por tanto actúan como meros transmisores de información."*).

El web explica, en els següents termes, per què no s'utilitza sempre el xifratge total:

"(…), resulta técnicamente imposible aplicar el "cifrado total" en todos los casos. Se podrá disponer de cifrado total cuando ambos usuarios se encuentren conectados a la aplicación y se haya establecido el protocolo de intercambio de claves públicas y privadas entre ambos terminales. En Nepcom anteponemos la seguridad por encima de todo, y por ese motivo cada vez que se inicia una sesión con cifrado de extremo a extremo, se intercambian claves nuevas, imposibilitando así este modo cuando alguno de los 2 usuarios no esté conectado. (…). Todos los mensajes enviados en modo "confidencial" serán enviados siempre mediante "cifrado total".

Per tant, de manera similar a l'esquema que seguiria Telegram, Nepcom donaria als usuaris dos nivells d'encriptació o xifratge, més o menys robusts en funció de l'elecció del propi usuari. De manera similar al cas de Telegram, i reiterant que no és objecte d'aquest informe verificar ni auditar el compliment dels estàndards de xifratge que apliquen els SMI, es pot considerar que l'usuari de Nepcom té prou informació sobre la utilització del "xifratge total" que ofereix Nepcom en el "modo confidencial" (ens remetem, sobre això, al document *"Medidas de seguridad implementadas por Nepcom",* de gener de 2017, disponible al web de Nepcom).

A banda d'això, des de la perspectiva de la seguretat resulta essencial que s'hagi previst un **programa d'auditoria independent**, que garanteixi que, amb la periodicitat necessària (ja sigui de manera ordinària o extraordinària), es verifica que el sistema segueix convenientment protegit dels riscos als quals pugui estar exposat.

Pel que fa a **Whatsapp**, l'informe d'AI, citat, destaca que Facebook (incloent, segons l'empresa, a Whatsapp) es sotmet a una auditoria periòdica ("*regular independent assessment*") per una empresa independent, *"Global Network Iniciative (GNI)",* la qual va concloure que l'empresa complia amb els principis establerts per aquesta organització per a la protecció de la intimitat dels usuaris; tot i així, AI afegeix que l'auditoria de GNI és confidencial i que AI no l'hauria pogut verificar. Ara bé, l'informe es refereix en aquest punt a Facebook, i es desconeix si la dita auditoria integra també a Whatsapp.

Pel que fa a **Telegram**, en la documentació disponible (document FAQ, *"FAQ for the Technically inclined",* i altra documentació, com ara l'informe d'AI), no es disposa de referències sobre si aquesta empresa es sotmet a auditories periòdiques. De tota manera, les FAQ de Telegram indiquen que: *"Telegram es abierta. Cualquiera puede revisar nuestro código fuente, protocolo y API, ver cómo todo trabaja y tomar una decisión informada. De hecho, recibimos de buena manera a expertos de seguridad para que revisen nuestro sistema y apreciamos cualquier feedback (security@telegram.org). Ofrecemos recompensas por las vulnerabilidades efectivas encontradas."* Segons l'empresa, experts en seguretat externs a l'empresa poden fer revisions del servei, si bé aquesta previsió no semblaria quelcom equiparable amb una auditoria externa, a banda que es desconeix amb quina periodicitat i detall es fan aquestes revisions.

Pel que fa a **Nepcom**, en el web s'indica que: *"Realizamos de forma periódica auditorías internas en materia de Protección de datos."* Ara bé, el web no ofereix més informació al respecte, ni es disposa d'informació externa a l'empresa, per tal de contrastar aquesta qüestió. En qualsevol cas, seria convenient que la mateixa empresa prestadora del servei preveiés un programa d'auditoria independent, que verifiqués que efectivament el sistema té implantades les mesures de seguretat declarades i que aquestes mesures són adequades a les exigències de l'RGPD, en funció de l'anàlisi de riscos pertinent. En relació amb la recomanació de la Resolució del Parlament, que les empreses compleixin certs estàndards de seguretat, fem notar que en el web de Nepcom, s'explicita que aquesta empresa es sotmet al compliment de la norma ISO 27001. Sens perjudici de la pertinència d'aquesta previsió, no es disposa d'informació sobre l'efectiu compliment d'aquest estàndard per part de l'empresa.

X

Les transferències internacionals de dades i la ubicació dels servidors

En relació amb l'apartat d.2) de la Resolució, relativa a que els SMI tinguin els servidors en el territori de la UE), cal fer les següents consideracions.

Com s'ha apuntat (art. 3 RGPD), podria donar-se el cas que les empreses responsables de l'SMI tinguin el seu establiment (o una delegació) a la UE, amb la qual cosa el tractament que faci aquesta empresa de dades de ciutadans europeus, estaria sotmès a l'RGPD; també podria ser que amb independència d'on estigui la seu, el tractament o part del tractament de dades de ciutadans residents a la Unió (per exemple, l'emmagatzematge d'informació dels usuaris) es dugui a terme fora de la UE en servidors que físicament estan ubicats en tercers països. Aquests servidors poden estar físicament ubicats en un lloc determinat, dins o fora del territori de la UE, o podem trobar altres casos de *"cloud storage",* que són serveis d'emmagatzematge de la informació (els missatges i altres continguts que l'usuari envia o rep a través d'un SMI), que operen en el núvol i, per tant, en ubicacions físiques que poden ser diverses. Com hem vist, en qualsevol d'aquests casos serà d'aplicació el RGPD.

Quan l'empresa de SMI utilitza sistemes de *"cloud storage"* (com és el cas de Whatsapp o Telegram), o quan simplement els servidors on s'emmagatzemen les dades (missatges de text, les imatges, etc, enviats i rebuts pels usuaris), estiguin ubicats fora de l'àmbit territorial d'aplicació de l'RGPD, esmentat, ens trobarem davant d'una transferència internacional de dades (TID), que estarà sotmesa al règim previst en els articles 44 a 50 de l'RGPD (arts. 33 i 34 LOPD fins el 25 de maig de 2018). L'RGPD preveu que la Comissió de la UE pot decidir que un tercer país, un territori o un o varis sectors específics d'un país, garanteix un nivell de protecció adequat (art. 45). A manca d'aquesta decisió de la Comissió, l'empresa responsable d'un SMI només podria transmetre dades personals a un tercer país si ofereix garanties adequades i els interessats disposen de drets exigibles i d'accions legals efectives (art. 46 RGPD) o concorre alguna de les excepcions previstes a l'art. 49 RGPD. Cal tenir en compte que els mecanismes que estableix l'RGPD per tal de considerar que s'ofereixen garanties adequades, són diversos –normes corporatives vinculants (BCR), clàusules tipus, autorització de l'autoritat de control, codis de conducta, mecanismes de certificació, etc- (art. 46 RGPD).

Pel que fa a **Whatsapp,** segons l'informe de AI, citat, *"WhatsApp no hace lo suficiente para advertir a los usuarios sobre las implicaciones de privacidad de la copia de seguridad de los mensajes a la nube. Al igual que muchas aplicaciones de mensajería,*

WhatsApp tiene una opción que permite a los usuarios realizar copias de seguridad de sus historiales de chat en Google Drive, iCloud o una copia de seguridad local (…)". Hi hauria, doncs, una mancança en aquest punt, des de la perspectiva de la seguretat de la informació dipositada al núvol.

Pel que fa a **Telegram**, segons el seu web, *"Los servidores de Telegram están alojados por todo el mundo, garantizando seguridad y velocidad",* i afegeix, en l'apartat "*Telegram es seguridad*", que *"una de las claves es que los centros de servidores se encuentran descentralitzados y se conectan los usuarios al más cercano, ofreciendo un mejor Servicio".*

El web de Telegram ("*¿Procesan solicitudes de datos?*"), explica que: "(...) *Los datos de los chats en la nube son almacenados en múltiples centros de datos alrededor del mundo, que son controlados por diferentes entidades legales y que se extienden en diferentes jurisdicciones. Las claves de cifrado relevantes son divididas en partes y nunca se mantienen en el mismo lugar que los datos protegidos. Como resultado, varias órdenes de diferentes jurisdicciones son requeridas para forzarnos a entregar algún dato."*

El web de Telegram explicita que*: los chats secretos no son parte de la nube de Telegram y sólo se puede acceder a ellos a través del dispositivo de origen."*

Fem notar que l'informe: *"Principales riesgos en el uso de Telegram",* de CCN-Cert (disponible al web www.ccn-cert.cni.es), destaca la següent problemàtica: *"Sobre todos los chats que no sean secretos, es decir, que no tengan activado el cifrado punto a punto, se realizará una copia de seguridad en los servidores de Telegram, de tal forma que si el usuario realiza un acceso a su cuenta desde otro dispositivo, pueda acceder a su historial de forma sencilla. Esta es una opción muy desaconsejable desde el punto de vista de seguridad, ya que expone datos de forma histórica frente a un compromiso, y no sólo durante lo que dure éste. Un atacante podría engañar a un usuario con técnicas de ingeniería social o tener acceso al teléfono de la víctima durante un breve espacio de tiempo para obtener las conversaciones y ficheros (...)."*

Pel que fa a **Nepcom,** tant a la política de privacitat com en el document de mesures tècniques s'afirma que els seus servidors es troben allotjats a Espanya. Fem notar que, sempre segons informació de la pròpia empresa, alguns experts haurien comprovat que *"la aplicación establece un par de conexiones con servidores de Amazon AWS."* Entenent que aquest fet podria contravenir la política de privacitat de l'empresa, segons la qual les dades dels usuaris s'emmagatzemen, tracten i conserven de forma plena i íntegra a Espanya, l'empresa aclareix que aquestes connexions no afectarien a dades personals *("estas conexiones no contienen ningún tráfico de datos personales de los usuarios"*). En qualsevol cas, no es disposa de més informació que permeti contrastar aquest extrem.

En qualsevol cas, com ha fet avinent aquesta Autoritat en ocasions anteriors, si bé la ubicació dels servidors en territori de la UE podria simplificar l'anàlisi del compliment d'obligacions previstes en la normativa europea de protecció de dades, tampoc no es pot desaconsellar, al menys amb caràcter general, la utilització de SMI que tinguin ubicats els seus servidors fora del territori de la UE, si ofereixen garanties adequades d'acord amb l'RGPD.

D'acord amb les consideracions fetes en aquest dictamen, es fan les següents,

Conclusions

Per la informació oferta per les mateixes empreses gestores de les solucions de SMI analitzades, i dels informes i estudis que s'han pogut consultar, es desprèn que les aplicacions analitzades compleixen certs aspectes dels previstos a la Resolució 280/XI del Parlament de Catalunya, si bé en alguns aspectes, com a mínim pel que fa a la informació que s'ofereix al respecte, podria ser clarament millorable. En qualsevol cas l'anàlisi dels diferents aspectes feta respecte les tres solucions analitzades (Whatsapp, Telegram i Nepcom), en el marc de l'anàlisi general que ja s'havia fet en el Dictamen CNS 55/2016, pot ser un element a tenir en compte a l'hora d'escollir una determinada aplicació per part de les administracions públiques catalanes.

Un pronunciament més precís sobre el compliment o incompliment per part d'alguna d'aquestes entitats, requeriria dur a terme un procés d'investigació o auditoria sobre aquestes entitats, que, en tot cas no correspondria fer a aquesta Autoritat sinó a l'Agència Espanyola de Protecció de Dades.

Barcelona, 7 de maig de 2018