Ref. CNS-55/2016

Dictamen en relació amb la consulta d'un Grup Parlamentari, en relació amb els sistemes de missatgeria exprés que s'adapten o no als requisits de la Resolució 280/XI del Parlament de Catalunya, sobre l'ús de serveis de comunicació pel Govern

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'un Grup Parlamentari, en què s'explica que en data 21 de setembre la Comissió d'Afers Institucionals del Parlament de Catalunya va aprovar per unanimitat la Resolució 280/XI, sobre l'ús de serveis de comunicació pel Govern (BOPC número 220, de 27 de setembre de 2016).

El Grup parlamentari sol·licita a aquesta Autoritat un estudi sobre els sistemes de missatgeria exprés que s'adapten als requisits que s'esmenten a la Resolució 280/XI, així com aquells altres que no s'hi adapten.

Analitzada la petició, que s'acompanya de còpia de la Resolució 280/XI, del Parlament, vista la normativa vigent aplicable, l'informe del Coordinador d'Auditoria i Seguretat de la Informació de l'Autoritat, i l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

Com consta en la Resolució 280/XI del Parlament, la Comissió d'Afers Institucionals, en la sessió tinguda el dia 21 de setembre de 2016, ha debatut el text de la Proposta de resolució sobre l'ús de Whastapp com a mitjà de comunicació (tram. 250-00495/11), presentada pel Grup Parlamentari de Ciutadans, i les esmenes presentades per altres grups parlamentaris.

La Resolució 280/XI, del Parlament de Catalunya, sobre l'ús de serveis de comunicacions pel Govern, finalment adoptada, té el següent contingut:

"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."

La proposta de Resolució debatuda a la Comissió d'Afers Institucionals del Parlament, es referia a l'ús d'una aplicació de missatgeria instantània en concret -Whatsapp-. La Resolució 280/XI finalment aprovada es refereix en termes generals a *"l'ús de serveis de comunicacions pel Govern",* sense referir-se a cap aplicació de missatgeria en concret.

Atès que la consulta sol·licita específicament un estudi sobre els sistemes de missatgeria exprés que s'adapten als requisits que s'esmenten a la Resolució 280/XI, així com aquells altres que no s'hi adapten, per tal de concretar l'abast d'aquest dictamen cal fer una consideració prèvia.

Actualment el mercat ofereix un nombre cada vegada més extens *"sistemes de missatgeria exprés"* (o *"sistemes de missatgeria instantània",* denominació més habitual per designar aquests tipus de sistemes de comunicació, i que utilitzarem en aquest dictamen amb l'acrònim "SMI"), més enllà dels que poden ser els més populars o utilitzats. Una simple recerca en xarxes socials i mitjans de comunicació permet identificar, fàcilment, desenes de serveis de missatgeria instantània. A tall il·lustratiu, podem esmentar Facebook Messenger, Skype, Line, Hangouts, Telegram y Whatsapp, Spotbros, Skype, WeChat, Wire, BBM, Snapchat, Viber, FaceTime, SureSpot, Threema, Nepcom o Woowos, entre molts d'altres. Fem notar que diversos webs, com ara el d'*Electronic Frontier Foundation* (www.eff.org, que remet al web "*surveillance self-defense*", https://ssd.eff.org/), identifiquen i comparen característiques de desenes de sistemes de missatgeria disponibles al mercat. Si bé, com indica el web de la EFF, aquestes llistes comparatives requeririen actualitzacions posteriors, d'entrada són indicatives de diversos elements que, en matèria de seguretat, caldria tenir en compte a l'hora de considerar la utilització de determinats SMI i de prioritzar-ne la utilització d'uns per davant d'altres, com veurem més endavant.

En qualsevol cas, un estudi com el que sol·licita el Grup Parlamentari requeriria fer una comparativa de les característiques dels diferents SMI disponibles (clàusules informatives –les quals cal tenir en compte que són modificades periòdicament per les empreses responsables-, la informació disponible als webs de cada sistema, condicions dels serveis oferts en cada cas, garanties de confidencialitat, clàusules contractuals, etc), i examinar aquestes característiques a la llum de les condicions establertes en la normativa europea de protecció de dades, a què es refereix la Resolució 280/XI.

Atesos els termes de la consulta, en la que no es fa referència específica a un o diversos sistemes o apps (aplicacions) de missatgeria instantània, i tenint en compte l'ampli nombre de sistemes i aplicacions existents i disponibles en el mercat, d'ús més o menys habitual entre els usuaris, en aquest dictamen es farà 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 SMI.

III

La Resolució 280/XI, el Parlament insta el Govern a establir una sèrie de criteris en relació amb la utilització de mitjans i serveis de comunicació en general (apartats a), b), c) i e) de la Resolució 280/XI). En síntesi, es preveu que ofereixin garanties de seguretat i de privacitat; que siguin econòmicament assequibles; que els prestadors d'aquests serveis de comunicació compleixin llurs deures de col·laboració amb òrgans de l'Administració i la justícia, i que incorporin les noves mesures que estableix el Reglament general de protecció de dades (UE) 2016/679 (en endavant, RGPD). L'apartat d) de la Resolució, insta el Govern a fomentar l'ús de SMI que utilitzen els organismes públics dependents de la Generalitat, les administracions públiques, els cossos i forces de seguretat, etc, que compleixin les característiques següents:

> *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.*

Atesa la consulta formulada, en aquest dictamen ens referirem principalment als SMI (apartat d) de la Resolució), tot i que a continuació fem algunes consideracions sobre els apartats a), b), c) i e) de la Resolució del Parlament, que es refereixen, en general, a mitjans o serveis de comunicació.

D'entrada, els "mitjans o serveis de comunicació" que poden utilitzar les administracions públiques, ja sigui per relacionar-se amb els ciutadans o amb altres administracions públiques, o com a canal de comunicació intern dins la seva pròpia estructura, poden ser molts i de naturalesa molt variada. Així, abastaria tant els mitjans de comunicació tradicionals (premsa, ràdio o televisió), com Internet, webs pròpies dels organismes i ens públics, Intranets corporatives, correu ordinari, comunicació per via telefònica, comunicació presencial, etc.

En la mesura que l'ús de qualsevol mitjà, canal o servei de comunicació per part de les Administracions públiques comporti un tractament d'informació personal, aquest tractament haurà de sotmetre's als principis i garanties de la protecció de dades, és a dir, a la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), així com al Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de l'LOPD (en endavant, RLOPD), així com 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).

L'LOPD s'aplica a qualsevol tractament de dades personals quan el tractament s'efectua en territori espanyol, o quan al responsable del tractament no establert en territori espanyol li és aplicable la legislació espanyola (article 2.1.a) i b) de la LOPD). Segons l'article 2.1.c) de l'LOPD, aquesta llei s'aplica en els casos en què el responsable no està establert a la UE però utilitza, per a tractar les dades personals, mitjans situats en territori espanyol.

Pel que fa a l'àmbit d'aplicació territorial del RGPD (Considerant 23 RGPD), segons l'article 3 del RGPD:

> *"1.El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del* ***responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.***
>
> *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*
> > *b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.*
>
> *(...)."*

Atès que la Resolució 280/XI del Parlament es refereix, en termes generals, a la utilització de diferents mitjans de comunicació per part de l'Administració de la Generalitat i els ens que en depenen, el tractament de dades dels afectats o interessats (art. 3.e) LOPD i art. 4.1 RGPD), que se'n derivi, haurà d'estar sotmès als principis i garanties de la normativa de protecció de dades, en els termes de la normativa esmentada.

Lògicament, les previsions i obligacions derivades del RGPD s'han de tenir especialment en compte en el procés d'elecció i priorització de determinats canals o mitjans de comunicació que hagin de comportar el tractament de dades personals, especialment, quan es prevegi que aquest tractament ha de tenir continuïtat més enllà d'aquesta data (25.5.2018). En relació amb mitjans o serveis de comunicació que ja s'estiguin utilitzant actualment, es recomana que es facin les oportunes revisions o actualitzacions en relació amb les previsions específiques del RGPD, per tal d'adaptar el tractament de dades personals que es faci a través dels dits canals o mitjans de comunicació, a les exigències del RGPD.

En qualsevol cas, atès que el *"tractament de dades personals"* (art. 3.c) LOPD), s'ha de sotmetre als principis i garanties de la normativa europea de protecció de dades, cal valorar positivament l'expressa menció, en l'apartat e) de la Resolució 280/XI, a la necessària incorporació de les mesures establertes pel RGPD en matèria de protecció de dades.

En la mateixa línia, com no pot ser d'altra manera, i sens perjudici de les consideracions que es concretaran més endavant, cal valorar positivament la previsió de l'apartat d.1) de la Resolució 280/XI, referit específicament als SMI, en el sentit que cal fomentar l'ús de SMI que *"tinguin una política de privacitat d'acord amb la legislació vigent en matèria de protecció de dades."*

IV

Segons l'article 3.d) de la LOPD, és responsable d'un fitxer o tractament de dades *"la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament".* (veure art. 4.7 RGPD).

El responsable del fitxer o tractament és qui, en primera instància, estarà obligat a donar compliment als principis i garanties de la protecció de dades personals.

Quan una administració pública ha de tractar informació personal dels afectats per al compliment de les seves funcions i competències, aquesta administració és la primera responsable dels fitxers o del tractament de dades que duu a terme (art. 3.b) LOPD).

Una administració pública responsable pot encarregar a un tercer la prestació d'un determinat tractament de dades personals, i haurà de vetllar perquè aquest tercer, si escau, sota la forma d'un encàrrec del tractament (arts. 3.g) i 12 LOPD, arts. 20 a 22 RLOPD, i art. 28 RGPD), assumeixi les responsabilitats que li pertoquin en relació amb el dit tractament de dades.

Aquesta Autoritat ha analitzat la relació entre responsables i encarregats del tractament en diverses ocasions, en concret, quan s'utilitzen aplicacions o serveis de determinades empreses. Fem referència al Dictamen 24/2012, relatiu a la contractació per part d'una administració pública del servei "Google Apps for bussiness", o al Dictamen 57/2013, sobre l'ús de "Google Drive", "Microsoft Skydrive" i "Dropbox" en l'àmbit professional de les relacions entre advocat i client, que es poden consultar al web de l'Autoritat (www.apd.cat). Com s'analitza en aquests dictàmens, quan una administració pública contracta i utilitza determinats sistemes de comunicació que implementen terceres empreses alienes a l'administració responsable (a tall d'exemple, un servei de "*cloud storage*" d'una tercera empresa), aquest tercer seria l'encarregat del tractament. En aquest esquema, caldria estar a les obligacions que imposa la normativa de protecció de dades (art. 12 LOPD, arts 20 a 22 RLOPD), i específicament, les previsions del capítol IV del RGPD, referides a les responsabilitats del responsable i de l'encarregat del tractament, atès l'àmbit territorial d'aplicació esmentat (art. 3 RGPD).

En aquest sentit, l'administració responsable està obligada a elegir un encarregat del tractament que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme al RGPD (art. 28.1 RGPD).

Aquesta consideració resulta pertinent, atès que la Resolució 280/XI es refereix, en termes generals, a mitjans i serveis de comunicació en els quals es pot donar aquest esquema (administració pública responsable que formalitza un encàrrec de tractament amb un tercer). Sens perjudici d'això, pel que fa específicament als SMI, convé precisar el següent.

A diferència del que hem comentat en relació amb l'esquema en què un responsable (una administració pública) contracta els serveis d'un tercer (un encarregat del tractament), cal tenir en compte que, en relació amb els SMI, és l'usuari (la persona física) qui decideix instal·lar-se una determinada aplicació de missatgeria instantània, a través de la qual es pot relacionar amb tercers, entre d'altres, amb les administracions públiques. Aquest serà el cas en què una administració pública ofereixi al ciutadà, com a un canal més de comunicació i, normalment, sense descartar-ne d'altres, la utilització d'un o més SMI.

Aquesta Autoritat ha analitzat en el Dictamen 24/2013, relatiu a l'ús de les aplicacions "Whatsapp" i "Spotbros" en l'àmbit professional en les relacions entre advocat i client, diverses qüestions relacionades amb els SMI. Entre d'altres qüestions, cal destacar que en el funcionament dels sistemes o apps de missatgeria instantània s'identifiquen diversos intervinents (empreses titulars de les apps, empreses que les creen, desenvolupen o comercialitzen, empreses relacionades amb la creació dels diferents dispositius (telèfons intel·ligents, tabletes...) en què els usuaris s'instal·len les apps, o empreses proveïdores de publicitat que rep l'usuari pel fet d'utilitzar-les). A aquests

efectes es podrien identificar diversos responsables o, com a mínim, diversos graus de responsabilitat sobre el tractament de les dades dels usuaris o "afectats". Com ha posat de manifest aquesta Autoritat, l'existència de diversos intervinents pot suposar en sí mateixa un cert risc per a la privacitat, en la mesura que el tractament de la informació dut a terme per algun d'ells no compleixi els principis i obligacions de la normativa de protecció de dades.

Sens perjudici de la resta d'intervinents, podem apuntar que són les empreses titulars dels SMI (les que hem citat a títol il·lustratiu en aquest dictamen, entre moltes d'altres), les que decideixen quin tractament fan de les dades dels usuaris que volen utilitzar el servei, i estableixen les condicions d'ús corresponents. En la informació que, habitualment, es posa a disposició dels usuaris a través dels respectius llocs web, aquestes empreses determinen quina informació utilitzaran i quina no, incloent dades personals de l'usuari i dels contactes de l'usuari, i per a quines finalitats.

Per tant, aquestes empreses són les responsables del tractament de dades personals dels usuaris –els quals s'han instal·lat un o més SMI en els seus dispositius, amb els quals podran interaccionar amb les administracions públiques-, als efectes de la normativa de protecció de dades.

Això no vol dir, òbviament, com reflecteixen les previsions de la pròpia Resolució 280/XI, i com ha fet avinent aquesta Autoritat, que les administracions públiques que ofereixen als ciutadans una via de comunicació i interacció a través de SMI, no hagin de valorar el grau de compliment, per part de les empreses responsables d'aquestes SMI, de les exigències derivades de la normativa europea de protecció de dades personals, a través dels indicadors als que farem referència en aquest dictamen.

Per tot l'exposat, les administracions públiques, com a responsables de tractar dades dels ciutadans per al compliment de llurs funcions, han d'assegurar-se que els tercers prestadors de serveis i de sistemes de comunicació compleixen, al seu torn, llurs responsabilitats, ja sigui com a encarregats del tractament o, si escau, com a responsables de tractar les dades dels usuaris (en el cas dels SMI), atès que aquests tractaments es troben sotmesos a les exigències dels principis i garanties de la normativa europea de la protecció de dades (LOPD, RLOPD, i RGPD).

V

Fem notar que l'**apartat a)** de la Resolució, es refereix a la necessitat d'utilitzar mitjans de comunicació que ofereixin garanties de seguretat i de privacitat quan es tractin dades sensibles (o, atesa la terminologia pròpia de la normativa de protecció de dades, *"dades especialment protegides"* –ex. art. 7 LOPD- i, segons el RGPD, les *"categories especials de dades personals"* –ex. art. 9 RGPD), i dades confidencials, respecte les que la normativa imposa un deure de secret o de confidencialitat (art. 10 LOPD), sens perjudici de les previsions referides al deure de secret o de confidencialitat d'altra normativa aplicable.

En qualsevol cas, puntualitzem que la normativa de protecció de dades (LOPD, RLOPD i RGPD) exigeix que els mitjans o canals de comunicació que utilitzin les administracions públiques, donin correcte compliment a les previsions sobre seguretat i confidencialitat de la dita normativa, independentment que la categoria o grau de sensibilitat de la informació tractada.

El mateix apartat a) de la Resolució, fa referència a les "garanties de seguretat". El RGPD, aplicable a partir del 25 de maig de 2018, configura un sistema de seguretat que no es basa en l'esquema de nivells de seguretat bàsic, mitjà i alt, previstos (art. 9 LOPD i Títol VIII RLOPD), que continuen temporalment vigents, 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 i art. 24 RGPD).

En línia amb el que apunta la Resolució 280/XI, efectivament, les administracions públiques hauran de vetllar pel compliment d'un nivell de seguretat adequat en base als paràmetres del RGPD, i a la informació tractada, especialment, si es tracta d'informació personal especialment protegida (art. 7 LOPD, Títol VIII RLOPD, i arts. 9, 10 i 24 RGPD, citats), també per part d'aquells tercers –empreses prestadores de serveis de comunicació i, particularment, als efectes que ens ocupen, de SMI-, que es trobin sotmesos a les exigències de la normativa europea de protecció de dades.

Tornarem sobre aquesta qüestió més endavant, en relació amb els SMI.

Respecte la previsió de **l'apartat b)** de la Resolució 280/XI, segons el qual cal utilitzar preferiblement els mitjans i serveis de comunicació *"que siguin econòmicament més assequibles, d'acord amb llur nivell de seguretat i de privacitat",* fem avinent que, des de la perspectiva de la protecció de dades de caràcter personal, el paràmetre econòmic (la major o menor despesa o càrrega econòmica que pugui suposar la utilització d'un o altre canal o servei de comunicació per part de les administracions públiques) no és, en sí mateix, un indicador d'una major o menor garantia en relació amb el tractament de dades de caràcter personal. Això, sens perjudici que, en l'elecció d'un o altre canal o servei de comunicació, les administracions públiques hagin de tenir en compte el factor econòmic o de despesa que la implementació del sistema de comunicació pot suposar, per aplicació de la normativa aplicable.

Dit això, cal tenir en compte que alguns SMI són gratuïts per als usuaris, i d'altres no. En funció de la gratuïtat del servei que s'ofereix, el model de negoci d'alguns SMI pot estar basat en l'explotació de les dades que genera l'ús del sistema, amb finalitats, principalment, de màrqueting i de publicitat. Aquestes finalitats concorren habitualment (tot i que no exclusivament) en SMI d'utilització gratuïta. Des de la perspectiva de la protecció de dades, caldria tenir en compte aquest element.

L'apartat c) de la Resolució, insta el Govern a 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."*

En atenció a les previsions de la normativa de protecció de dades, les administracions responsables hauran de tenir en compte, a l'hora de seleccionar un determinat servei o sistema de comunicació, que els *"prestadors de serveis"* (als que es refereix l'apartat c) de la Resolució, en referència general a mitjans i serveis de comunicació), hagin de complir, en la mesura que ho exigeixi la normativa europea de protecció de dades, requeriments de col·laboració de les administracions corresponents, singularment, de l'Administració de justícia. Aquesta seria una conseqüència necessària en aquells casos en què l'administració, com a responsable, encarregui un determinat tractament a un tercer (ex. art. 28.3 RGPD, ja esmentat), i també haurà de ser un element a tenir especialment en compte, en aquells casos en què una administració valori l'ús d'un SMI.

La normativa de protecció de dades preveu l'obligació d'atendre a una comunicació de dades, sense consentiment dels afectats, quan els destinataris o cessionaris de les

dades són les autoritats judicials (art. 11.2.d) LOPD). També el RGPD preveu expressament la no aplicació de la prohibició general de tractar dades de categories especials de dades quan el tractament és necessari per a la formulació, l'exercici o la defensa de reclamacions, o *"quan els tribunals actuïn en exercici de la seva funció judicial"* (art. 9.1 i 9.2.f) RGPD, i Considerant 52).

És a dir, el marc normatiu europeu de protecció de dades habilitaria la comunicació de dades (el "deure de col·laborar", en els termes de l'apartat c) de la Resolució) amb les autoritats judicials, quan aquestes facin un requeriment.

A banda dels requeriments judicials, pel que fa a la resta de sol·licituds de comunicació d'informació que provinguin de l'administració en general, cal tenir en compte que el tractament de dades que sigui necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics atorgats al responsable del tractament, es considera ajustat al principi de licitud (art. 6.1.e) RGPD). En aquest cas, l'habilitació haurà d'estar concretada en una llei o en el dret de la Unió Europea (art. 6.3 RGPD)

A això cal afegir que l'article 4.9 del RGPD, considera destinatari:

> *"la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;"*

És a dir, la normativa europea de protecció de dades preveu –i considera ajustat al principi de licitud si es fa en els termes del RGPD-, que una autoritat judicial, o una altra autoritat administrativa puguin sol·licitar, en l'exercici de les seves competències, determinada informació a un responsable, dins l'àmbit territorial de la UE.

Una sol·licitud de dades formulada per una administració pública o una autoritat judicial d'un Estat membre de la UE, a un responsable que presti un servei de comunicació a les administracions públiques a què es refereix la Resolució 280/XI, comportaria un flux informatiu que la normativa preveu, que serà lícit si es produeix en els termes previstos al RGPD, i que per tant el responsable (el prestador del servei) haurà d'atendre.

En altre cas, és a dir, quan una administració pública o una autoritat judicial d'un Estat que no forma part de la UE sol·liciti informació a un "prestador de serveis de comunicació" d'una administració pública catalana, cal tenir en compte que el flux informatiu també s'ha de produir de conformitat amb el que disposa el RGPD (atès l'art. 3 RGPD, ja esmentat).

En definitiva, en relació amb sol·licituds d'informació formulades per autoritats judicials o administracions públiques, de dades d'usuaris que utilitzaran determinats SMI en el supòsit que planteja la consulta, el RGPD és d'obligat compliment.

Per tant, des de la perspectiva de la protecció de dades, el que resulta rellevant és que el prestador de serveis conegui que els accessos a informació personal que pugui tractar d'usuaris de serveis d'administracions catalanes, es troben subjectes al règim previst en el RGPD, tant si es tracta de fluxos informatius entre països de la UE (dins el territori de la UE), com de fluxos informatius que tinguin com a destinatàries administracions o autoritats judicials d'altres Estats fora de la UE.

VI

La Resolució 280/XI, (**apartat d**)), insta el Govern a 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, i afegeix quines haurien de ser les característiques d'aquests sistemes de missatgeria exprés.

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.

Les consideracions exposades per aquesta Autoritat en el Dictamen 24/2013 poden ser d'interès en el context de la utilització de SMI per a comunicacions entre els ciutadans (els afectats, segons l'article 3.e) LOPD) i les administracions públiques, o per a comunicacions entre diverses administracions o dins d'una mateixa administració, sens perjudici que l'Autoritat en el dictamen esmentat es pronuncia en relació amb les condicions de privacitat i de seguretat de determinats serveis en el moment d'emetre el dictamen, condicions que poden haver canviat posteriorment.

També fem recordatori que el Dictamen 2/2003 del Grup de Treball de l'Article 29 (GT 29), disponible al web http://ec.europa.eu/justice/data-protection/article-29/, constata l'existència de riscos per a la protecció de dades personals i la privacitat, generats per l'ús de les anomenades "apps" (aplicacions) per a aparells o dispositius intel·ligents ("smart devices"). Aquests riscos s'analitzen a partir del marc legal aplicable al tractament de dades personals en el desenvolupament, distribució i ús de les apps, en el moment d'emetre el dit dictamen (Directiva 95/46/CE, i Directiva 2002/58/CE, sobre la privadesa i les comunicacions electròniques).

Si bé algunes de les consideracions fetes tant per aquesta Autoritat com pel GT 29, poden considerar-se vigents, cal tenir en compte que, en el moment de fer efectiva la Resolució 280/XI i analitzar les repercussions d'utilitzar SMI per part de les administracions públiques, resulta fonamental analitzar l'ús d'aquests sistemes atenent a les previsions i exigències del RGPD (en algun cas noves i, en d'altres, complementàries a les ja previstes per l'LOPD i la Directiva 95/46/CE. En concret, cal tenir en compte que el RGPD deroga la Directiva 95/46/CE (art. 94 RGPD), tot i que es manté vigent la Directiva 2002/58/CE (art. 95 RGPD).

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. Alguns dels sistemes permeten a més d'utilitzar la missatgeria bàsica, els usuaris d'alguns d'aquests sistemes poden fer videoconferències, crear grups, "xats", i compartir-hi informació, arxius o contactes.

En definitiva, es tracta de solucions de comunicació que es configuren com a serveis, és a dir, el sistema està composat per aplicacions que els usuaris utilitzen per accedir a uns servidors que gestionen i poden emmagatzemar els missatges. Aquestes aplicacions són les conegudes com a "apps" dels dispositius mòbils (tabletes, *smartphones*...) tot i que també s'utilitzen aplicacions instal·lades en ordinadors (ja siguin aplicacions client específiques o en base a l'accés mitjançant navegador web).

Així, ens podem referir a solucions de programari que estan formades per dues parts. D'una banda, per una aplicació que permet a l'usuari la creació, tramesa, recepció i administració de missatges, i de l'altra, uns servidors pels quals passen els missatges que intercanvien els usuaris.

Atesos els termes generals de la consulta, ens referirem a l'esquema probablement més habitual, que és el del prestador del servei que, per ell mateix, desenvolupa i subministra l'aplicació i proveeix els servidors.

VII

Pel que fa la previsió de la Resolució 280/XI (apartat d.1a) de la Resolució), segons la qual els SMI han de tenir una política de privacitat d'acord amb la legislació vigent en matèria de protecció de dades, cal tenir en compte que el responsable (art. 3.d) LOPD) és a qui correspon, en primera instància, vetllar perquè un determinat sistema de comunicació tingui una política de privacitat adequada.

Com s'ha fet avinent des d'una perspectiva general, per aplicació del RGPD (art. 3), si l'establiment de l'empresa responsable d'un SMI està ubicat a la UE, el tractament de dades dels usuaris s'haurà de sotmetre a les exigències del RGPD. I no només així, sinó que el RGPD també s'aplicarà al tractament que una empresa responsable d'un sistema o app de missatgeria electrònica d'un país aliè a l'UE, faci de persones interessades que resideixen a la UE, quan les activitats del tractament estan relacionades amb l'oferta de béns i serveis a aquests usuaris, amb independència que a aquests se'ls requereixi un pagament. És a dir, en principi, i amb independència que els serveis a què ens referim siguin gratuïts o s'ofereixin sota pagament, si els usuaris ("afectats", segons l'art. 3.e LOPD, o "interessats", segons art. 4.1 RGPD), resideixen a la UE, cal aplicar els principis i garanties del RGPD al tractament que, respecte els ciutadans europeus (persones residents a la UE), facin aquestes empreses responsables de SMI, per bé que siguin empreses externes a la UE.

Fem notar que aquesta qüestió ja havia estat analitzada, en relació amb el marc legal anterior (Directiva 95/46/CE), pel GT29 en el Document de treball relatiu a l'aplicació internacional de la legislació comunitària sobre protecció de dades al tractament de les dades personals a Internet per llocs web establerts fora de la UE, de 2002.

A manera introductòria, cal tenir en compte que les solucions que ofereixen les empreses prestadores de SMI poden ser de tres grans tipus, que exemplifiquem a efectes il·lustratius:

1. 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 (habitualment mitjançant número de línia telefònica mòbil, tot i que en algunes solucions no és necessari disposar-ne, i seria suficient una connexió a xarxa –per exemple, mitjançant WIFI-). Entre les aplicacions comercials de missatgeria de tipus

públic tenim “Whastapp”, “Line”, “Telegram”, “WeChat”, “Skype”, “iMessage” (Apple), “Viber”, “Facebook Messenger”, “KakaoTalk”, “Spotbros”, “Kik Messenger”, “Google Allo”, “Signal” o “Threema”, entre moltes altres.

2. Una solució comercial que tingui l’opció d’us corporatiu, i que s’implanta de tal manera que només podria servir per intercanviar missatges entre persones autoritzades per l’organització, si bé les infraestructures de servidors seran habitualment compartides amb tercers, sens perjudici de que es puguin oferir d’altres models que permetin segregar els diferents serveis corporatius responsabilitat del proveïdor de la solució. En aquest grup podem trobat solucions com “UPCnet uTalk”, “Enjoystr”, “Imbox.me” (solució corporativa d’Spotbros), “Cotap” o “BlackBerry Messenger” o, per a centres educatius, la solució anomenada “iEduca Tokapp”.

3. Una solució corporativa pròpia, que implica el desenvolupament d’una aplicació pròpia i es desplega un servei de manera exclusiva per a una organització, sens perjudici que pugui estar basada en solucions comercials. Solucions d’aquest tipus poden aportar més control sobre les operacions de tractament de les dades personals, ja que són solucions “a mida”. Per exemple la Junta d’Andalusia té una aplicació de missatgeria pròpia, així com alguna Universitat, i recentment l’Institut Catala de la Salut (ICS) ha posat en marxa una aplicació per als professionals de la institució, per ús assistencial, entre d’altres.

En termes generals, podem apuntar que en funció del servei que vulguin prestar les administracions públiques, pot ser més convenient una o altra solució. 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. En canvi, si el número d’usuaris del SMI és més limitat (el personal al servei d’una administració), una solució corporativa pròpia pot ser més adient.

En qualsevol cas, fem avinent que seria necessària una anàlisi més detallada, atenent a les particularitats de cada cas, per tal de determinar quina solució pot ser la més adequada.

Dit això, a continuació analitzarem diferents elements que resulten rellevants des de la perspectiva de la protecció de dades i, per tant, que les administracions públiques haurien de tenir especialment en compte als efectes de la consulta formulada, en concret:

- La informació personal que cal tractar
- El consentiment de les afectades
- El model de seguretat i avaluació de l’impacte i les mesures de seguretat aplicades
- Els mecanismes de certificació
- Les transferències internacionals de dades i la ubicació dels servidors
- El dret d’informació i la transparència

VIII

La informació personal que cal tractar

Una administració pública pot utilitzar canals de comunicació per oferir informació als ciutadans -per exemple, en moltes solucions d’informació de les anomenades *smart cities-,* o pot establir una comunicació amb l’afectat a través de diversos mitjans, de

manera que aquest afectat o usuari no només rep informació general, sinó que comunica les pròpies dades a l'administració. Des de la perspectiva de la protecció de dades, no suposa el mateix tractament la comunicació que es realitzi per donar, rebre i 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 la que es realitzi per comunicar un possible fet delictiu, un accident, etc. (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.

Cal tenir en compte que moltes comunicacions dins les administracions, o entre aquestes i els ciutadans, no comportaran un tractament d'informació especialment protegida o sensible. En d'altres casos, quan es transmetin, per exemple, dades de salut o dades relatives a la comissió d'infraccions penals o administratives, que és possible que es tractin en el context dels missatges tramesos entre un usuari i els serveis sanitaris, o entre una víctima d'una agressió i els cossos de seguretat, etc, cal fer avinent que són dades que la normativa protegeix especialment. L'especial naturalesa, mereixedora de protecció reforçada, de determinades categories de dades personals, entre d'altres, les que revelen l'origen ètnic o racial, la religió, les dades relatives a la salut i la vida sexual, i les condemnes i infraccions penals o mesures de seguretat connexes, queda palesa en el RGPD (Considerant 75 i article 9 RGPD).

A més, la informació personal que es pot comunicar a través de molts SMI no només poden ser missatges de text, sinó arxius d'imatge o so, que poden ser informació especialment sensible. La privacitat i els drets dels afectats poden veure's afectats, si hi ha un accés indegut a la informació de text i, amb més motiu, tractant-se d'informació sensible, a arxius adjunts d'imatge i so. Per exemple, l'accés indegut a informació sensible referida a la salut d'una persona o a un incident violent que ha generat una denúncia als cossos de seguretat a través d'un SMI, pot suposar un perjudici major si s'acompanya d'imatges o sons relatius a aquest incident violent.

En definitiva, el tipus de comunicació que s'estableixi per part de les administracions amb els ciutadans condiciona el tipus d'informació personal que previsiblement haurà de ser tractada en aquesta comunicació. Des de la perspectiva de la protecció de dades, aquest és un primer element a tenir en compte per a seleccionar un sistema de missatgeria instantània adequat, atenent a les característiques que la pròpia empresa responsable faciliti i expliqui a l'hora de protegir la informació dels usuaris, especialment, la informació sensible.

A títol il·lustratiu, i com va fer avinent aquesta Autoritat en el seu Dictamen 24/2013, hi ha determinades empreses responsables de SMI, que fins i tot desaconsellen els seus usuaris d'utilitzar les seves apps per comunicar informació sensible o íntima (ja siguin missatges de text o imatges). Evidentment, el fet que l'empresa responsable d'una app de missatgeria instantània expliciti en les seves condicions de servei que no es pot comprometre a protegir adequadament la informació sensible, hauria de ser tingut en compte com un indicador prou significatiu.

Per tot això, la tipologia d'informació que pugui ser habitualment tractada (si és previsible que es tracti informació especialment protegida o que pugui afectar la intimitat i altres drets dels usuaris), en funció del servei que l'administració vulgui atendre a través d'un SMI, és un element especialment rellevant a tenir en compte, a l'hora de considerar el seu ús.

IX

El consentiment de les persones afectades

Un altre dels indicadors a tenir en compte 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). Com ha fet avinent aquesta Autoritat, resulta 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.

Si bé 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 d'un servei de missatgeria, això no implica que resulti adequada la prestació d'un consentiment general, en el sentit d'una acceptació incondicionada, per utilitzar les dades de l'usuari o de terceres persones per a finalitats que no resultin estrictament necessàries per a la prestació del servei.

Cal tenir en compte que, segons l'article 4.11 del 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;"*

Als efectes que interessen, cal tenir en compte que el considerant 32 del RGPD disposa el següent:

"El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. (...)."

Tenint en compte el que ja recomanava el Dictamen 2/2013 del GT29, i com aquesta Autoritat ha recordat en diferents ocasions, un indicador rellevant a tenir en compte des de la perspectiva de la protecció de dades, seria el fet que les empreses que presten SMI sol·licitin un *"consentiment granular"*, específic, per cada tipus de dades a les que el servei accedirà, en funció que el tractament de dades sigui necessari per a la prestació del servei, o no. A tall d'exemple, el SMI hauria de donar control a l'usuari sobre la informació addicional que aquest facilita (fotos de perfil, informació sobre darreres connexions, en definitiva, facilitar a l'usuari un control sobre qui podrà veure informació del seu perfil), i sobre altres qüestions que no han d'afectar, en principi, la prestació del servei.

Que la recollida del consentiment de l'afectat s'ajusti a les exigències de la normativa de protecció de dades resulta un element clau a l'hora d'avaluar la pertinença d'utilitzar un o altre SMI en el context de la consulta formulada.

Serveixi com a exemple del problema que acabem d'exposar, els recents canvis de les condicions d'ús de Whatsapp, que preveuen la comunicació de dades a Facebook,

que està essent motiu d'anàlisi per part de diverses Autoritats de protecció de dades de la UE i que ha donat lloc a una comunicació del GT 29, de data 27 d'octubre de 2016, a Whatsapp, 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.

X

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

Com ja es va fer avinent en el Dictamen 24/2013 (FJ VIII), les previsions que puguin explicitar les empreses respecte la confidencialitat amb la que tracten les dades dels usuaris, no eximeixen de les obligacions que, en funció de la informació tractada, siguin exigibles (article 9 LOPD i Títol VIII RLOPD).

Com s'ha apuntat, el RGPD, aplicable a partir del 25 de maig de 2018, configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt, previstos a l'LOPD i que segueixen temporalment vigents, 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, el RGPD estableix un esquema integral de seguretat, en el qual cal determinar quines mesures cal aplicar, a partir de les característiques del tractament, i d'una anàlisi de riscos en els termes del RGPD (Considerants 83 i 84).

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

Per altra banda, el 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.

Seria recomanable que les administracions que es plantegin la utilització de SMI per prestar determinats serveis als ciutadans, o per a comunicacions intra o interadministratives, realitzin una avaluació de l'impacte sobre la privacitat i les dades personals, 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.

Sens perjudici de les concrecions que requereixi cada cas, en termes generals, l'avaluació d'impacte en la protecció de dades que haurien de fer les administracions a l'hora de valorar la possibilitat d'implementar un SMI, haurà de tenir en compte les garanties i salvaguardes que acrediti cada empresa per tal de protegir la confidencialitat de la informació tramesa, que no es produiran accessos no autoritzats, així com la integritat de la informació (que no es produeixi una alteració no autoritzada del contingut del missatge sigui accidental o malintencionada) i l'autenticitat (garantia de l'autoria del missatge o de la identitat dels interlocutors).

En qualsevol cas, seria convenient integrar l'anàlisi sobre la utilització de SMI ja des de la fase del disseny d'un determinat servei a l'usuari, atesos els principis de privacitat en el disseny i de privacitat per defecte als quals el RGPD dóna carta de naturalesa (Considerant 78 RGPD). Així, segons l'article 25 RGPD:

> *"1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*
>
> *2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*
>
> *3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."*

Com ja 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 d'informació especialment protegida (o categories especials de dades) i s'hagi d'extremar, en conseqüència, la seguretat en relació amb aquesta informació.

Així, pot ser pertinent tenir en comte 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 "extrem a extrem". Sobre això, un dels sistemes que el web eff.org, citat, esmenta, és la utilització de l'encriptació d'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 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, i la integritat i autenticitat dels missatges, si s'acompanya d'altres mesures.

Per tot això, pel que fa a la selecció d'un SMI per part de les administracions públiques, seria molt recomanable, des de la perspectiva de la protecció de dades, comprovar quines polítiques o protocols d'encriptació i xifratge apliquen.

Això, sens perjudici que, com ja ha manifestat aquesta Autoritat en les seves anàlisis anteriors de SMI, encara que les converses es transmetin en forma segura (encriptada o xifrada), queden emmagatzemades en el terminal en una base de dades, que tot i estar xifrada, té una contrasenya que, si no es protegeix adequadament pot ser accessible per tercers, que podrien accedir a les converses. Per tant, que els SMI requereixin als usuaris contrasenyes robustes, podria ser un indicatiu a tenir en compte.

Altres indicadors de seguretat que, segons la informació consultada, poden ser d'interès a l'hora d'avaluar la seguretat en els SMI són, entre d'altres, si l'usuari té mecanismes per verificar que no s'està produint una suplantació de l'interlocutor amb el qual està intercanviant missatges; si seria possible desxifrar missatges antics si algú aconsegueix les claus de xifrat; si ha estat possible verificar la robustesa del sistema per part d'experts independents, etc..

Sens perjudici que aquests indicadors que hem esmentat puguin ser rellevants, cal fer avinent que aquests no cobreixen totes les necessitats que es puguin derivar dels tractaments de dades de caràcter personal, com posa de manifest, en relació amb el cas de "Whatsapp", l'informe de setembre de 2016, del "Centro Criptológico Nacional" (CCN-CERT IA-21/16, disponible al web: www.cnn-cert.cni.es).

Des de la perspectiva de la seguretat resulta essencial que, en relació amb el SMI que es pretengui utilitzar, 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.

Així mateix, també pot ser un indicador de valoració als efectes que ens ocupen, si l'empresa o responsable que ha d'aportar una solució de SMI a una administració, disposa d'un DPO, **delegat de protecció de dades** (arts. 37 a 39 RGPD), figura que

és obligatòria en alguns casos, i que en qualsevol cas pot evidenciar, des de la perspectiva organitzativa, que es gestionen les obligacions en relació amb la protecció de dades personals.

Finalment, hi pot haver altres elements rellevants als efectes de la normativa de protecció de dades, que en l'avaluació que facin les administracions públiques a l'hora de seleccionar un o altre canal o servei de comunicació, es tinguin en compte elements com ara la **usabilitat** per part dels afectats o usuaris del servei (art. 3.e) LOPD). Un altre indicador a tenir en compte, relacionat amb la **disponibilitat** del propi SMI, és el d'assegurar que el proveïdor de la solució sigui solvent tècnicament, des de la perspectiva del manteniment del sistema i de l'aplicació del conjunt de mesures de seguretat previstes, tant tècniques com organitzatives (art. 32.1.c) RGPD). També cal tenir en compte les salvaguardes que ofereix una empresa responsable d'un SMI en relació amb la **continuïtat del servei** (sobretot, en relació amb serveis que es puguin oferir les administracions i que tinguin a veure amb la seguretat i l'atenció als ciutadans, com ara trucades d'emergència a través de SMI per alertar a cossos de seguretat, bombers, urgències mèdiques, etc).

XI

Els mecanismes de certificació

Com es desprèn de l'article 25.3 RGPD, per tal de certificar la implantació adequada de mesures de seguretat en cada cas (per al cas que ens ocupa, en relació amb l'elecció de solucions de SMI per part de les administracions públiques per a determinats serveis o fluxos informatius), el RGPD preveu la utilització de mecanismes de certificació. Segons disposa l'article 42 del RGPD:

> *"1.Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.*
>
> *(...)".*

Tenint en compte aquesta previsió, es recomana que les administracions públiques tinguin en compte si el responsable que ofereix una solució de SMI disposa de segells o certificacions en matèria de protecció de dades, a mesura que aquests es vagin implantant.

A l'hora d'avaluar una determinada solució de SMI, que les empreses compleixin amb certs estàndards de seguretat, com ara la norma ISO 27001, a què fa referència l'apartat d.3) de la Resolució 280/XI, pot ser un indicador a tenir en compte.

Ara bé, sens perjudici d'això, com ha fet avinent aquesta Autoritat en el Dictamen 57/2013, disposar d'aquesta o altra certificació o estàndard internacional en matèria de seguretat, per sí sola, no garanteix el compliment de les mesures de seguretat exigibles, especialment, en casos en què s'utilitza la computació en el núvol, com pot ser habitual en el cas que ens ocupa. Tenint en compte això, cal destacar que aquesta certificació ISO, a la que es refereix la Resolució 280/XI, o qualsevol altra, hauria d'anar acompanyada de la resta de mesures de seguretat pertinents (en els termes del RGPD), i de les corresponents auditories.

XII

Les transferències internacionals de dades i la ubicació dels servidors

Pel que fa a la menció de **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.

Els SMI són sistemes de comunicació que es configuren com a serveis, és a dir, que el sistema està composat per aplicacions que utilitzen els usuaris per accedir a uns servidors que gestionen i emmagatzemen els missatges. Els missatges enviats i rebuts pels usuaris de SMI, passen a través dels servidors responsabilitat de l'empresa que gestiona aquest SMI. El cas que pot ser més habitual en relació amb SMI, és aquell en què un mateix prestador del servei desenvolupa i subministra l'aplicació i proveeix del servidors. La informació relativa a la ubicació dels servidors pot ser, en relació amb diversos SMI, una informació difícil d'obtenir, cosa que pot dificultar la valoració que les administracions públiques hagin de fer de cara a triar un o altre SMI per comunicar-se amb els ciutadans.

Com s'ha apuntat (art. 3 RGPD), podria donar-se el cas que les empreses responsables de 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 al RGPD; també podria ser que part del tractament que fa una empresa responsable d'un SMI (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, o perquè es duu a terme un tractament a través de la computació en el núvol). Inclús en aquests casos, caldria aplicar els principis i garanties de la normativa europea de la protecció de dades, ateses les previsions sobre l'àmbit d'aplicació d'aquesta, ja exposats.

En aquest sentit, com ja va posar de manifest el Grup de Treball de l'Article 29 en el Dictamen 5/2012, sobre computació en el núvol, *"(...) una condición previa para los acuerdos de computación en nube es que el responsable del tratamiento realice una evaluación de riesgos adecuada,* ***incluyendo las ubicaciones de los servidores*** *donde se tratan los datos y la consideración de los riesgos y ventajas desde la perspectiva de la protección de datos, con arreglo a los criterios indicados en los apartados que figuran a continuación."*

En aquest mateix dictamen, el GT 29 fa avinent que *"cabe añadir una advertencia especial en cuanto a la necesidad de un organismo público de evaluar en primer lugar si la comunicación, tratamiento y* ***almacenamiento de datos fuera del territorio nacional puede exponer a riesgos inaceptables*** *la seguridad y privacidad de los ciudadanos y la economía y la seguridad nacional, en particular en el caso de bases de datos sensibles (por ejemplo, datos del censo) y servicios sensibles (por ejemplo, servicios de salud). Deberá prestarse esta especial consideración, en cualquier caso, siempre que se traten datos sensibles en la computación en nube.* (…)".

En qualsevol cas, 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.

A l'hora de seleccionar un SMI per part d'una administració pública, el fet que els servidors estiguin ubicats físicament en països de la UE, sotmesos clarament al règim del RGPD, podria facilitar, d'entrada, el control per part de l'usuari respecte la seva informació, l'exercici dels seus drets i la possibilitat de denunciar o reclamar en cas d'infracció de la normativa de protecció de dades. Des d'aquesta perspectiva, certament, la ubicació a la UE dels servidors de l'empresa responsable d'un SMI que tracta dades dels usuaris, pot ser un element de simplificació pel que fa al compliment dels principis i obligacions de la normativa europea de protecció de dades.

Ara bé, tampoc no es pot generalitzar, en el sentit que la ubicació dels servidors fora del territori de la UE hagi de conduir necessàriament a descartar la utilització, en el context de la consulta plantejada, d'un determinat SMI, atès que pot resultar igualment d'aplicació el RGPD (art. 3 RGPD).

El que correspondrà fer a les administracions públiques que valorin la utilització d'un determinat SMI, serà constatar si l'empresa responsable del SMI compleix amb les exigències previstes per al règim de transferències internacionals de dades (TID), previstos a l'LOPD i al RGPD, per tal d'assegurar que el tractament de la informació dels usuaris del SMI s'adequarà a les exigències de la normativa europea de protecció de dades.

Així, quan una empresa responsable d'un SMI -que un usuari té instal·lat i que utilitzarà per comunicar-se amb una administració pública-, utilitza sistemes de *"cloud storage",* 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 del RGPD, esmentat, ens trobarem davant d'una transferència internacional de dades (TID), que estarà sotmesa al règim previst en els articles 33 i 34 LOPD, als quals ens remetem, així com al règim previst en els articles 44 a 50 del RGPD.

El 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 (dels usuaris del SMI) a un tercer país (situació que, en relació amb els SMI, pot ser força habitual, en els termes apuntats), si ofereix garanties adequades i a condició que els interessats (en el cas que ens ocupa, els usuaris que utilitzaran els SMI per comunicar-se amb les administracions públiques) disposin de drets exigibles i d'accions legals efectives (art. 46 RGPD). Cal tenir en compte que els mecanismes que estableix el RGPD per tal de considerar que s'ofereixen garanties adequades, són diversos –normes corporatives vinculants (BCR), clàusules tipus, mecanismes de certificació, etc- (art. 46.2 RGPD) i, per tant, les administracions públiques hauran de tenir en compte si, en cada cas, concorre algun d'aquests instruments per considerar que les TID que es produeixen pel fet que l'empresa responsable d'un SMI tingui els seus servidors fora de l'àmbit d'aplicació territorial del RGPD.

En connexió amb aquesta qüestió, i pel que fa a la comprovació del nivell adequat de protecció, fem avinent que, a partir del 12 de juliol de 2016, la UE ha posat en marxa "l'Escut de la privacitat UE- EEUU" ("Privacy shield"), en substitució de l'anterior acord "U.S.-E.U. Safe Harbor", al que s'adherien entitats d'Estats Units per certificar el compliment de principis i obligacions de protecció de dades, amb la finalitat d'habilitar TID (veure, al respecte, les consideracions fetes pel GT 29 en el Dictamen 1/2016, sobre el projecte d'Escut de Privacitat entre la UE i EE.UU). La STJUE de 6 d'octubre de 2015, va declarar invàlida la Decisió 2000/520/CE, sobre l'adequació de la

protecció conferida pels principis de Port Segur ("*Safe Harbor*"), sistema que ha estat substituït pel nou marc ("Escut de la privacitat UE-EE.UU").

Convé per això consultar la informació disponible a la *"Guía del Escudo de la Privacidad UE-EE.-UU"* (disponible al web oficial de la UE: http:// europa.eu). Pel que fa a la llista d'entitats adherides a l'Escut de Privacitat, es pot consultar el web del Departament de Comerç d'Estats Units (https://www.privacyshield.gov/welcome).

Per tant, les administracions públiques que vulguin utilitzar SMI hauran de tenir en compte, si escau, si l'empresa responsable està adherida a l'Escut de Privacitat i, en conseqüència, si ha de respectar les previsions de l'Escut en relació amb la protecció de dades (obligacions en matèria de dret d'informació a l'afectat, exercici de drets, comunicació de dades, etc). En qualsevol cas, la vinculació d'una empresa responsable d'un SMI a l'Escut de Privacitat podria donar validesa i fiabilitat a la comunicació de dades (TID) als servidors d'aquesta empresa, quan la informació s'emmagatzemi únicament en servidors ubicats als Estats Units, i no en d'altres territoris.

En conclusió, si bé la ubicació 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 el RGPD (BCR, clàusules tipus, mecanismes de certificació, escut de privacitat, etc).

XIII

El dret d'informació i la transparència

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".*

Cal tenir en compte que la informació que la pròpia empresa responsable d'un SMI difon sobre les seves polítiques de privacitat i sobre el tractament de dades, a banda que són modificades periòdicament, sovint no són prou entenedores per a l'usuari, qüestió que cal tenir en compte a l'hora de seleccionar un determinat SMI, atès que els afectats tenen dret a ser informats adequadament.

Segons el RGPD, les dades personals han de ser tractades de manera lícita, lleial i transparent en relació amb l'interessat ("licitud, lleialtat i transparència" ex. art. 5.1.a) RGPD). El RGPD exigeix que els responsables del tractament de dades personals donin correcte compliment, específicament, al 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 dret d'informar els afectats sobre una sèrie de qüestions, en els termes de l'article 13 RGPD (que en alguns aspectes va més enllà del que disposa l'article 5 LOPD), que recull la informació que el responsable, en aquest cas l'empresa responsable d'un SMI, ha de donar a l'afectat.

Fins la plena aplicació del RGPD (25 de maig de 2018), segueix vigent el règim previst a l'LOPD i a l'RLOPD, però cal tenir present que, a partir de la data esmentada, el nou Reglament europeu comporta, entre d'altres, haver d'informar respecte dels extrems següents que siguin d'aplicació al cas concret (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.

En relació amb la previsió de l'apartat d.4) de la Resolució 280/XI, cal fer notar que ni l'article 5 de l'LOPD, ni l'article 13 del RGPD exigeixen, estrictament, que s'hagi de donar informació als afectats sobre els encàrrecs del tractament subscrits pel responsable d'un fitxer o tractament amb un encarregat, tot i que pot ser una pràctica recomanable. En qualsevol cas sí que obliga a informar en aquells casos en què amb ocasió de l'emmagatzematge, o un altre tractament, es produeixi una transferència internacional de dades.

Malgrat que la informació relativa a nous aspectes (allò que preveu l'article 13 RGPD i que va més enllà del que preveu l'article 5 LOPD) no és exigible fins el mes de maig de 2018, als efectes d'aquest dictamen resulta especialment recomanable que les administracions públiques que vulguin establir serveis de comunicació amb els ciutadans a través de missatgeria instantània, tinguin en compte aquestes noves previsions, a efectes de comprovar quines SMI donen un compliment al dret d'informació dels afectats adequat, en els termes exigits pel RGPD.

En línia amb el que hem apuntat en relació amb la ubicació dels servidors, val a dir que la informació disponible referida a si les empreses responsables dels SMI practiquen realment la transparència respecte dels accessos per part de les autoritats públiques, o sobre quines terceres empreses utilitzen com a encarregats de tractaments, sovint no resulten senzilles d'obtenir, si bé algunes empreses difonen informació sobre aquestes qüestions.

Així, diverses empreses de comunicació i xarxes socials, així com empreses que gestionen SMI, com ara, simplement a tall d'exemple, Facebook o Google, Twitter, Dropbox, Snapchat, LinkedIn,Microsoft, entre moltes altres (atesa la informació disponible als respectius web: www.google.es; www.dropbox.com; https://transparency.twitter.com; www.snap.com; www.linkedin.com, etc), publiquen periòdicament –en molts casos, cada sis mesos-, 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

les que es demana informació, la freqüència amb la que l'empresa ha proporcionat la informació requerida, etc.

Val a dir que, per la informació consultada, aquest tipus d'informes de transparència no inclouen informació específica sobre "contractes d'encàrrec del tractament amb els prestadors", entenent per tals (apartat d.4) de la Resolució del Parlament) contractes que les empreses responsables de SMI hagin pogut subscriure amb tercers.

En qualsevol cas, des d'una perspectiva àmplia del que suposa la transparència informativa, el fet que una empresa responsable d'un SMI emeti aquest tipus d'informes de transparència, que inclouen informació agregada sobre sol·licituds d'informació per part, principalment, d'autoritats d'Estats Units, pot ser un indicador a tenir en compte per part de les administracions públiques que vulguin seleccionar un determinat SMI per a oferir-lo als ciutadans com a canal de comunicació, més, tenint en compte els casos prou coneguts de sol·licituds d'informació per part d'autoritats d'Estats Units, que poden afectar usuaris europeus de determinades xarxes socials, que generen preocupació des de la perspectiva de la protecció de dades.

En qualsevol cas, cal destacar que, segons explicita la Guia de l'Escut de privacitat entre la UE i els Estatus Units, a què ens hem referit, 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, pel que fa als SMI que tinguin la seva seu radicada als Estats Units i s'hagin adherit a l'Escut de privacitat, sembla que l'obligació d'informar (o de mostrar transparència, en els termes de la Resolució 280/XI, sobre accessos per part de cossos policials), hauria d'incloure informació sobre sol·licituds formulades per autoritats públiques d'Estats Units, qüestió rellevant a l'hora d'avaluar la pertinença de l'ús de determinats SMI d'empreses que s'han sotmès a l'Escut de privacitat.

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

Conclusions

Les administracions públiques, com a responsables de tractar dades dels ciutadans per al compliment de llurs funcions, han d'assegurar-se que els tercers prestadors de serveis i de sistemes de comunicació compleixen, al seu torn, llurs responsabilitats, ja sigui com a encarregats del tractament o, si escau, com a responsables del tractament de les dades dels usuaris (en el cas dels SMI), atès que el tractament es troba sotmès a les exigències dels principis i garanties de la normativa europea de la protecció de dades (LOPD, RLOPD, i RGPD).

Les administracions públiques, quan considerin l'elecció d'un determinat sistema de missatgeria instantània (SMI) haurien de tenir en compte, especialment, la finalitat de la comunicació, la informació personal que cal tractar; el consentiment dels afectats; el model de seguretat i l'avaluació d'impacte i les concretes mesures de seguretat aplicades; els mecanismes de certificació; les transferències internacionals de dades i la ubicació dels servidors; el dret d'informació i la transparència, en atenció a les previsions de la normativa europea de protecció de dades.

Barcelona, 10 de novembre de 2016