Dictamen en relació amb la consulta d'una associació en què participen els col·legis d'advocats de Catalunya sobre els riscos que comporta l'ús de missatges de text i les comunicacions per veu a través de dispositius mòbils en l'àmbit professional de l'advocat

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una associació en què participen els col·legis d'advocats de Catalunya en relació amb els riscos que comporta l'ús de missatges de text i les comunicacions per veu a través de dispositius mòbils en l'àmbit professional de l'advocat.

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

I

(...)

II

L'entitat que formula la consulta manifesta en el seu escrit tenir constància de l'existència de diversos mecanismes que actualment permeten interceptar fàcilment les comunicacions que s'efectuen a través de dispositius mòbils, ja sigui per veu (trucada) ja sigui mitjançant l'enviament de missatges de text curts (SMS), fet que li planteja dubtes sobre la idoneïtat d'emprar aquest canal de comunicació per transmetre dades sensibles.

Per aquest motiu, planteja a aquesta Autoritat si les dites comunicacions compleixen les exigències de l'article 104 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, RLOPD), és a dir, si es tracta d'un canal adequat per a que l'advocat pugui comunicar dades sensibles.

A aquesta qüestió ens referim en els apartats següents d'aquest dictamen.

III

La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) imposa l'obligació al responsable del tractament i, si s'escau, a l'encarregat del tractament d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries per tal de garantir la seguretat de les dades personals que seran tractades, així com per evitar la seva alteració, pèrdua, tractament o accés no autoritzat (article 9).

Aquestes mesures de seguretat venen regulades en el Títol VIII del RLOPD, que les classifica en tres nivells diferents –bàsic, mitjà i alt- en funció de la tipologia de dades personals que en cada cas es prevegin tractar, i tenen un caràcter acumulatiu, de tal manera que les establertes per a cada nivell exigeixen incorporar les previstes per als nivells inferiors (articles 79 i següents).

L'article 104 del RLOPD a què es fa esment en l'escrit de consulta -inserit en la Secció 3a del Capítol III d'aquest Títol VIII del RLOPD, relatiu a les mesures de seguretat de nivell alt aplicables als fitxers i tractaments automatitzats- estableix el següent:

"Quan conforme a l'article 81.3 s'hagin d'implantar les mesures de seguretat de nivell alt, la transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fil de comunicacions electròniques s'ha de fer xifrant les dades esmentades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers."

Les dades a què es refereix l'article 81.3 del RLOPD, al qual remet l'article 104 de la mateixa norma, són aquelles que requereixen nivell alt de seguretat, això és els fitxers o tractaments de dades personals següents:

"a) Els que es refereixin a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual.
b) Els que continguin o es refereixin a dades obtingudes per a fins policials sense consentiment de les persones afectades.
c) Els que continguin dades derivades d'actes de violència de gènere."

D'acord amb aquests preceptes, per tant, l'advocat, com a responsable, en el present cas, d'informació personal de caràcter sensible (article 3.d) LOPD), ha de garantir la confidencialitat i la integritat d'aquestes dades durant el seu transport pels canals de comunicació esmentats en el dit article 104 del RLOPD, és a dir, per xarxes públiques o xarxes sense fil de comunicacions electròniques.

Actualment, la manera més eficaç i eficient d'aconseguir la confidencialitat i la integritat de les dades en la seva transmissió és l'ús de la criptografia, sempre que es tingui en compte que hi ha diverses alternatives a l'hora d'emprar-la i que, segons l'escenari que es vulgui protegir, l'ús d'una o altra alternativa poden oferir o no suficients garanties per a l'adequada protecció de les dades trameses.

De fet, el dit article 104 del RLOPD permet garantir la seguretat de les dades xifrant-les o bé utilitzant *"qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers",* és a dir, xifrant el canal de comunicació.

En el present cas, la transmissió de les dades sensibles per l'advocat es duria a terme a través de dispositius mòbils. Per tal d'establir si aquest canal de comunicació compleix amb l'obligació imposada pel dit article 104 del RLOPD, tal com es planteja en l'escrit de consulta, és necessari examinar-ne el funcionament, la seguretat que ofereix, així com les amenaces o vulnerabilitats que pot presentar.

El dit examen s'efectua en els apartats següents d'aquest dictamen.

IV

Per dispositiu mòbil cal entendre aquell aparell d'ús personal o professional de reduïdes dimensions que permet al propietari-usuari la gestió d'informació i l'accés a xarxes de comunicacions, tant de veu com de dades, i que sovint disposa de capacitats de telefonia (per exemple, telèfons mòbils, telèfons mòbils intel·ligents (*smartphones*) o agendes telefòniques (PDA)).

Els dispositius mòbils, especialment els més avançats, ofereixen funcionalitats similars o, fins i tot, superiors a les ofertes per altres dispositius de computació més tradicionals (ordinadors portàtils, de sobretaula...), tals com, l'accés als serveis de telefonia (missatges de text (SMS) i multimèdia (MMS), veu i dades), l'accés complet a xarxes de dades (privades o Internet), inclosa la gestió del correu electrònic, l'accés a les xarxes socials, la navegació web, la missatgeria instantània, els serveis de localització (mitjançant GPS i la xarxa de dades), etc.

Com bé s'apunta a l'escrit de consulta, totes aquestes funcionalitats o capacitats presenten nombroses amenaces i vulnerabilitats que posen en risc la seguretat tant del mateix aparell com de la informació que gestiona. Aquests riscos de seguretat són múltiples i abasten des de la pèrdua o robatori de l'aparell -afectant a la seva disponibilitat- fins l'obtenció de la informació emmagatzemada, enviada o rebuda per l'aparell -afectant a la seva confidencialitat-, passant per la suplantació del seu propietari o usuari -aspecte que afectaria la seva integritat i autenticitat-.

Atesos els termes en què s'efectua la consulta, cal dir que en el present dictamen s'examinen els riscos que pot comportar l'ús del dispositiu mòbil per part del seu propietari (l'advocat) relacionats amb els mecanismes de comunicació emprats per transmetre la informació propis d'aquests aparells i, en concret, les tecnologies de comunicacions mòbils 2G i 3G (és a dir, no s'inclou en l'examen la tecnologia de comunicacions mòbils 4G, atès el nivell escàs de desplegament i ús en què es troba actualment, ni altres tecnologies de comunicació dels dispositius mòbils, tals com *Bluetooth*, xarxes sense fils WI-FI o NFC, entre d'altres).

Aquestes tecnologies de telefonia mòbil són, precisament, les que permeten enviar i rebre trucades de veu, missatges de text curts (SMS) i multimèdia (MMS), així com accedir a Internet. En aquest sentit, convé apuntar breument que:

- La segona generació de comunicacions mòbils (2G) la va constituir (i la constitueix) l'estàndard GSM. Aquest servei inicialment només permetia establir comunicacions de dades punt a punt (per les trucades de veu) i enviar missatges de text curts (SMS). Posteriorment, amb la incorporació dels protocols GPRS i EDGE, permetia (i permet) accedir a Internet, si bé a velocitats força reduïdes.
- La tercera generació de comunicacions mòbils (3G) la constitueix l'estàndard UMTS. Aquest servei disposa de la capacitat de commutar tant circuits (per les trucades de veu) com paquets (per les connexions de dades) i l'accés a Internet. Amb la incorporació dels protocols HSDPA, HSUPA i HSPA+ es va augmentar la velocitat de navegació considerablement.

Aquesta distinció del funcionament de les tecnologies de comunicacions mòbils existents en l'actualitat (no s'inclou, com s'ha dit, la quarta generació (4G), atès el seu nivell escàs de desplegament) s'efectua per tal de poder exposar, de manera separada, els riscos que per a la seguretat de la informació tramesa presenten cadascuna d'elles, així com la manera en què podrien ser atacades.

A tal efecte, s'han tingut en compte les vulnerabilitats detectades i analitzades en publicacions consultades, com ara, entre d'altres, en la *Guía de Seguridad de las TIC (CCN-STIC-450): Seguridad en dispositives móviles* del *Centro Criptológico Nacional*, disponible al seu web www.ccn-cert.cni.es.

V

En relació amb les comunicacions efectuades a través de dispositius mòbils que empren la tecnologia 2G (GSM), cal posar de manifest que, malgrat néixer dita tecnologia amb l'objectiu de garantir la seguretat i privacitat de les comunicacions –empra criptografia tant per l'autenticació dels usuaris com per al xifratge de les dades trameses-, actualment es considera totalment insegura, ateses les vulnerabilitats que s'han detectat en els darrers anys. Així, cal tenir present que:

- L'identificador únic de l'usuari sovint es transmet sense xifrar, de manera que es revela la presència d'un determinat usuari en una ubicació i es permet identificar les seves comunicacions i activitats.
- L'algoritme de xifratge que empra per protegir la confidencialitat de les comunicacions de veu i SMS, anomenat A5/1, va ser trencat (desxifrat) públicament l'any 2009, de manera que és possible obtenir la clau de sessió amb què es xifren les dades trameses.
- Els dispositius estan obligats a suportar l'algoritme de xifratge A5/0, que equival a l'absència de xifratge, si la xarxa així li ho indica.
- La norma GSM defineix un procediment d'autenticació de l'usuari vers la xarxa (per facturar el servei), però no un procediment d'autenticació invers o mutu que requereixi que la xarxa s'hagi d'autentificar també vers la targeta SIM, de tal manera que un terminal mòbil no té forma de diferenciar si l'estació base que li ofereix servei és l'operador real o bé n'és una de falsa.

Aquestes vulnerabilitats poden ser aprofitades per tercers aliens al propietari del dispositiu mòbil per tal d'atacar les comunicacions (de veu o de SMS) que s'efectuïn en el sentit següent:

- Atacs al dispositiu mòbil: interceptar la comunicació de veu o de SMS a través de la col·locació d'un dispositiu d'escolta (maquinari o programari) en el dispositiu mòbil, per tal d'enregistrar i retransmetre les trucades fetes o rebudes i els SMS enviats o rebuts. És necessari que l'atacant tingui accés físic al dispositiu mòbil per instal·lar-hi tal maquinari, si bé cab la possibilitat que el mateix propietari de l'aparell instal·li programari maliciós sense ser-ne conscient.

- Atacs passius: escoltar converses alienes i obtenir còpies dels SMS enviats i rebuts de qualsevol dispositiu mòbil, utilitzant una antena de ràdio receptora programable, un ordinador i un programari que es pot trobar gratuïtament a Internet. És necessari que l'atacant estigui situat dins de l'àrea de cobertura de la mateixa estació base que està donant servei a la víctima.

L'atacant ha de capturar tot el trànsit de comunicacions amb l'estació base, identificar el dispositiu de la víctima (mitjançant la realització de trucades perdudes a la víctima o bé enviant-li un SMS) i obtenir la clau de sessió que està utilitzant per xifrar les seves comunicacions. L'obtenció de dita clau de sessió no és complexa atès que, recordem, l'algoritme de xifrat utilitzat en xarxes 2G (A5/1) està trencat. Una cop obtinguda la clau de sessió, l'atacant pot desxifrar en temps real les comunicacions entre la víctima i l'estació base, i escoltar les trucades telefòniques entrants i sortints, així com els SMS enviats i rebuts en aquell moment.

- Atacs actius: disposar del control complet de les comunicacions del dispositiu mòbil (veu i SMS), fins i tot, suplantant l'estació base (aquest fet li permetria, per exemple, redirigir trucades sortints, manipular la recepció i enviament de SMS, etc.), utilitzant un escàner de freqüències de ràdio per interceptar la comunicació entre el dispositiu mòbil i l'estació base. Aquest atac explota la vulnerabilitat de la norma GSM ja esmentada de no verificar l'autenticitat de l'estació base a què es connecta el dispositiu mòbil.

Atès que els dispositius mòbils cerquen l'estació base amb el senyal més fort, l'atacant pot utilitzar l'escàner de freqüències de ràdio per fer-se passar per una estació base i que els dispositius mòbils de l'àrea s'hi connectin, transmetent un senyal més fort que l'estació base legítima. Una vegada que l'atacant obté el control del dispositiu mòbil, pot fer atacs d'intermediari (*man-in-the-middle*) en què l'atacant es connecta amb el dispositiu mòbil i amb l'estació base legítima -fent-se passar pel dispositiu mòbil de la víctima- i capturar i desxifrar totes les comunicacions de veu i SMS que s'hi estableixin.

Emprant també una estació base falsa mòbil, és a dir, establerta en algun tipus de vehicle i realitzant càlculs de triangulació sobre la senyal rebuda del dispositiu de l'usuari, cabria la possibilitat de geolocalitzar el dispositiu mòbil i, per tant, al seu propietari.

La dita geolocalització també seria possible utilitzant un conjunt d'unitats de mesura de posició (LMUs) distribuïdes espacialment en la zona en què es troba el dispositiu a localitzar. Aquestes unitats mesuren les diferències en el temps que triga la senyal del dispositiu en arribar a les diferents LMUs i, en base a aquestes diferències, s'estima la posició de l'aparell mòbil.

Així mateix, emprant una estació base falsa i configurant-la de manera que s'enviïn codis de rebuig concrets als dispositius mòbils d'interès per a l'atacant, seria possible realitzar un atac de denegació del servei de manera selectiva, és a dir, afectant només a l'usuari desitjat. Es tracta d'un atac que explota la funcionalitat de SMS sempre activa en els dispositius mòbils.

Aquesta funcionalitat de SMS també pot ser explotada per l'atacant per a la propagació d'enllaços a llocs web maliciosos. Utilitzant de manera combinada l'ús del SMS amb les capacitats d'accés a Internet dels dispositius i l'enginyeria social, seria possible instar a l'usuari a visitar una pàgina web a través de la qual infectar el seu terminal amb un virus troià, fent possible, per exemple, l'obtenció per l'atacant de credencials d'accés o d'informació sensible.

Dit això, cal fer avinent que, si bé no es coneixen vulnerabilitats en relació amb els algoritmes de xifratge que empren els protocols GPRS i EDGE (anomenats GEA1 i GEA2) per a la transmissió de dades -incorporats a la tecnologia 2G amb posterioritat al GSM-, la vulnerabilitat d'autenticació existent en GSM ja esmentada, en què un tercer podria suplantar l'estació base, continua sent completament viable en aquest cas.

A més, convé destacar que, en la mesura en què les comunicacions de dades a través de GPRS i EDGE fan servir els protocols TCP/IP, els dispositius mòbils també estarien exposats a totes les amenaces de seguretat existents en aquestes xarxes (diversos atacs a cada capa del model TCP/IP, com ara, per exemple, suplantació de missatges, modificació de dades, retards i denegació de missatges, problemes de control d'accés i de confidencialitat, etc.).

VI

En relació amb les comunicacions efectuades a través de dispositius mòbils que empren la tecnologia 3G (UMTS), cal posar de manifest que, ara per ara, es consideren raonablement segures, atès que, tret petits atacs teòrics, encara no s'ha publicat cap atac pràctic realment efectiu contra dita tecnologia.

En la tecnologia 3G s'empra un mecanisme d'autenticació mutu entre el terminal i la xarxa, de tal manera que no és possible realitzar l'atac de suplantació de l'estació base a què s'ha fet referència en l'apartat anterior. Així mateix, empra un algoritme de xifrat (anomenat A5/3) diferent a l'emprat a la tecnologia 2G (A5/1) que impedeix capturar i desxifrar el trànsit de veu.

Ara bé, cal tenir en compte que, en la mesura que la majoria de dispositius mòbils són capaços d'utilitzar tant les comunicacions 2G com les 3G, per tal de poder accedir a Internet quan la tecnologia de comunicació mòbil 3G no està disponible (per manca de cobertura o de servei), aquests aparells són també vulnerables a tots els atacs contra la tecnologia de comunicació mòbil 2G a què s'ha fet referència anteriorment.

Així mateix, atès que la major part dels operadors i proveïdors de telefonia mòbil fan servir la mateixa clau pre-compartida entre el terminal de l'usuari i la xarxa tant per a les comunicacions 2G com per a les 3G, cal tenir present que, en la mesura que el dispositiu faci ús d'ambdues xarxes, si un tercer obté la clau de sessió de la tecnologia 2G també podrà desxifrar el trànsit efectuat amb la tecnologia 3G.

L'opció més viable per evitar la captura del trànsit en infraestructures GSM (2G) passa per canviar l'algoritme de xifratge (A5/1) al que es fa servir en les infraestructures de telefonia 3G (A5/3).

L'ús d'un algoritme de xifratge robust, com l'A5/3, però no evitaria la vulnerabilitat de suplantació de l'estació base durant el procés d'autenticació. L'única opció per fer-ho seria no utilitzar la tecnologia GSM (2G), sinó la UMTS (3G). Ara bé, cal tenir present que l'ús únic de la xarxa 3G dependrà de les opcions de configuració establertes en el dispositiu mòbil de què disposi l'usuari.

VII

D'acord amb les consideracions efectuades en els apartats anteriors d'aquest dictamen, cal dir, en relació amb la qüestió plantejada, que l'ús de dispositius mòbils per a la comunicació de dades sensibles per part d'un advocat podria no resultar adequat des del punt de vista de la seguretat de la informació, especialment, quan tals comunicacions (veu i SMS) s'efectuen valent-se de la tecnologia de comunicació mòbil 2G.

Com s'ha dit, l'article 104 del RLOPD obliga el responsable del tractament (l'advocat) a garantir la confidencialitat i la integritat de les dades sensibles que es transmetin a través del dispositiu mòbil, ja sigui xifrant aquestes dades o bé utilitzant *"qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers",* com ara, a través del xifratge del canal de comunicació.

Tenint en compte les vulnerabilitats o riscos per a la seguretat de la informació detectats en el canal de comunicació examinat, per tal de garantir la confidencialitat i la integritat de la informació personal sensible tramesa per l'advocat –i així donar compliment a l'esmentat article 104 del RLOPD- és necessari emprar software que permeti el xifratge de la informació en trànsit d'extrem a extrem (per exemple, en el cas de comunicacions de veu (trucades), el proporcionat per *Cellcrypt o Sigillu*, o bé per aplicacions gratuïtes com, per exemple, *Redphone o Signal*, sent necessari, en aquest darrer cas, verificar el nivell de seguretat ofert; i/o en el cas de missatges de text curt (SMS), el software proporcionat per aplicacions gratuïtes com *TextSecure o Signal,* sent necessari també verificar el nivell de seguretat ofert).

En la mesura que s'adoptin sistemes d'encriptació o xifratge d'extrem a extrem que permetin que la informació no sigui intel·ligible ni manipulada per tercers en el seu trànsit, la transmissió d'informació sensible a través de les comunicacions efectuades amb dispositius mòbils (veu i SMS) pels advocats podria arribar a considerar-se que es realitza de manera segura, tal com exigeix l'article 104 del RLOPD.

Tot i així, cal tenir present que les mesures de seguretat s'han d'adoptar sempre tenint en compte l'estat de la tecnologia i els riscos a què estan exposades les dades personals, de tal manera que un determinat sistema d'encriptació o de xifratge emprat en un determinat moment podria deixar de ser adequat després d'un temps perquè, per exemple, s'ha descobert una vulnerabilitat.

Per a aquest motiu, i amb la finalitat sempre de garantir el dret fonamental a la protecció de dades de caràcter personal (article 18.4 CE), caldria valorar amb caràcter prioritari l'ús d'altres tecnologies per a la transmissió d'aquest tipus d'informació especialment protegida.

Sempre que això no sigui possible, per tal de dificultar l'accés dels possibles atacants a les comunicacions efectuades per l'advocat a través del seu dispositiu mòbil, convindria seguir les recomanacions següents:

- Inhabilitar la funcionalitat de connexió al servei de dades de telefonia mòbil (GPRS, EDGE o UMTS) quan es consideri que no és necessari establir una connexió mitjançant aquestes tecnologies (si bé es presumeix que les capacitats de comunicació de veu de telefonia dels dispositius mòbils seran necessàries en tot moment, podria valorar-se la conveniència de la seva inhabilitació en determinats entorns i escenaris).
- En atenció a les nombroses vulnerabilitats existents en les comunicacions efectuades amb la tecnologia 2G, inhabilitar, quan sigui possible, l'ús d'aquesta tecnologia en els dispositius mòbils o, el que és el mateix, configurar-los per tal que emprin només la tecnologia de comunicació mòbil 3G (o, en el seu cas, 4G).
- Eliminar els serveis disponibles a través de l'operador de telefonia mòbil, tals com, per exemple, l'absència de capacitats de comunicacions de dades associades al contracte de la targeta SIM o el bloqueig en la recepció de SMS originats en Internet.
- Aplicar les actualitzacions de software proporcionades pel fabricant del terminal.
- No obrir cap missatge SMS/MMS que no s'esperi o d'origen desconegut (pràctica habitual amb els correus electrònics), així mateix, no executar, obrir o permetre la instal·lació de continguts adjunts (configuracions, enllaços web (URLs), binaris o multimèdia) associats a missatges SMS/MMS no esperats i procedir al seu immediat esborrat.
- Prestar atenció a les aplicacions mòbils (app) que es puguin instal·lar en el dispositiu, ja que tot i que no vagin adreçades a interceptar el contingut de les comunicacions d'una forma malintencionada, sí que poden sol·licitar permisos excessius per a la seva instal·lació i ús, i posar en risc les dades relacionades amb l'establiment i l'activitat de les comunicacions fetes des del dispositiu mòbil (per exemple, accés a dades del registre de trucades o enviament de SMS sense la intervenció de l'usuari).

VIII

Arribats a aquest punt, es considera pertinent fer alguna consideració addicional en relació amb la possibilitat que l'advocat emmagatzemi en el seu dispositiu mòbil informació especialment sensible, ja sigui perquè es vol transmetre a un tercer ja sigui perquè es rep d'un tercer.

No es pot oblidar que els dispositius mòbils més avançats emmagatzemen i permeten emmagatzemar elevades quantitats d'informació, inclosa informació de caràcter personal que pot ser especialment sensible (per exemple, SMS/MMS, documents privats i confidencials, fotografies, vídeos, gravacions de veu, etc.).

Una de les principals amenaces de seguretat conegudes en els dispositius mòbils és, precisament, que un tercer aliè accedeixi a tota aquesta informació, bé perquè tingui accés físic al terminal, bé perquè disposi d'accés remot a través d'una vulnerabilitat d'algun dels seus components o mitjançant una aplicació prèviament instal·lada (programari maliciós) per ell mateix (fet que implicaria accedir físicament a l'aparell) o pel mateix propietari sense ser-ne conscient.

Per tal de protegir la confidencialitat, la integritat i la disponibilitat d'aquesta informació és necessari adoptar també mecanismes de xifratge de les dades. El xifratge ha d'ésser aplicat tant a les capacitats d'emmagatzematge internes del dispositiu mòbil com a les targetes de memòria externes. Ara bé, cal tenir en compte que, tot i aplicar el xifratge al dispositiu per complet, cab la possibilitat que un tercer accedeixi a la informació de manera transparent si ha obtingut prèviament l'accés al dispositiu, és a dir, si compta amb el codi d'accés al terminal.

Per aquest motiu, a banda de mantenir l'aparell sota control en tot moment, es recomana emprar programari de xifratge independent del sistema operatiu del dispositiu de què es tracti. En aquest darrer cas, s'empra una contrasenya per gestionar la informació que és diferent a la del codi d'accés al terminal.

Així mateix, a banda de l'adopció de mesures de xifratge de la informació emmagatzemada, es recomana realitzar una còpia de seguretat actualitzada dels continguts del dispositiu mòbil, emprar antivirus i no instal·lar programari de fonts poc confiables.

En qualsevol cas, tal i com s'ha posat de manifest en l'apartat anterior d'aquest dictamen, caldria valorar i avaluar la tipologia de la informació emmagatzemada en els dispositius mòbils, no sent recomanable, des del punt de vista de la garantia del dret a la protecció de dades personals dels afectats, emmagatzemar-hi informació especialment sensible.

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

Conclusions

La normativa de protecció de dades de caràcter personal imposa a l'advocat, com a responsable de la informació personal sensible de què disposa, l'obligació d'assegurar que la transmissió d'aquestes dades a través del seu dispositiu mòbil s'efectua emprant mecanismes que garanteixin que la dita informació no és intel·ligible ni manipulada per tercers (article 104 RLOPD).

Les comunicacions efectuades a través de dispositius mòbils que empren la tecnologia 2G (GSM) no es consideren segures, atès que la dita tecnologia presenta diverses vulnerabilitats (algoritme de xifratge trencat, no verificació de l'autenticitat de l'estació base, etc.) que posen en risc la seguretat de la informació personal tramesa.

Les comunicacions efectuades a través de dispositius mòbils que empren la tecnologia 3G (UMTS), tot i considerar-se segures, podrien ser vulnerables a tots els atacs existents contra la tecnologia 2G, en la mesura que aquests dispositius també facin ús de la dita tecnologia 2G.

Ateses les vulnerabilitats detectades en les comunicacions mòbils esmentades i els atacs a què poden veure's exposades, es considera que, per tal de garantir la confidencialitat i la integritat de la informació personal sensible en la seva transmissió a través de dispositius mòbils, és necessari emprar software que permeti el xifratge de la dita informació en trànsit d'extrem a extrem.

Barcelona, 29 de setembre de 2014