CNS-19/2016

Dictamen en relació amb la consulta d'un Ajuntament sobre l'entrega d'un telèfon mòbil a la persona que el va trobar

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per l'Alcalde d'un Ajuntament en què planteja si pot lliurar un telèfon mòbil a la persona que el va entregar en el seu dia a l'Oficina d'objectes perduts de la Policia un cop ha transcorregut el termini legal per a que el seu propietari el reclami, atès que s'hi contenen dades de caràcter personal.

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

I

(...)

II

L'Ajuntament planteja, en el seu escrit de consulta, si pot lliurar un telèfon mòbil a la persona que el va entregar en el seu dia a l'Oficina d'objectes perduts de la Policia en no haver estat reclamat pel seu propietari un cop transcorregut el termini legal establert a tal efecte, atès que l'aparell contindria dades de caràcter personal.

Als efectes que interessen en el present dictamen, convé fer avinent que es desconeix el model de telèfon mòbil de què es tracta, el sistema operatiu amb què opera (tractant-se d'un telèfon mòbil intel·ligent (*smartphone*), com així semblaria ser) i la naturalesa de la informació de caràcter personal que podria contenir l'aparell.

En qualsevol cas, cal tenir present que els telèfons 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.

Totes aquestes funcionalitats o capacitats permeten al seu propietari-usuari gestionar un gran volum d'informació, principalment, informació de caràcter personal (pròpia o de terceres persones), que queda emmagatzemada al dispositiu. Aquesta informació pot comprendre des de les dades dels contactes del seu propietari (agenda), incloses adreces electròniques, fins a dades bancàries, passant per correus electrònics, missatges de text i/o multimèdia, recerques fetes a Internet (com ara, a Google) o imatges, les quals poden fer referència a persones menors d'edat o poden haver estat realitzades en contextos de caràcter privat o íntim.

En definitiva, no es pot descartar que, en un cas com el plantejat, el telèfon mòbil emmagatzemi dades íntimes o dades que la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) considera, en el seu article 7, especialment protegides (ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual).

Fins i tot, podria contenir dades que, més enllà del fet que puguin ser considerades com a íntimes o no, podrien requerir una especial protecció des del punt de vista del dret a la protecció de dades (article 18.4 CE i STC 292/2000), atesa l'existència d'altres

circumstàncies qualificades (per exemple, dades de menors, la possibilitat d'elaborar perfils, per motius de seguretat, etc.).

Dit això, atesos els termes en què s'efectua la consulta, s'entén que l'Ajuntament hauria dut a terme totes les actuacions al seu abast per, de conformitat amb la legislació vigent, intentar identificar el propietari del telèfon mòbil que ara es pretén lliurar a la persona que el va trobar.

A tall d'exemple, pot assenyalar-se, en aquest sentit, actuacions tals com:

- Accedir a l'agenda de contactes telefònics de l'aparell.

  Aquesta actuació podria dur-se a terme si el telèfon mòbil no es troba protegit per algun dels mecanismes que habitualment incorporen aquests dispositius (PIN, patró, empremta, etc.), però també si només ho està pel número PIN de la targeta SIM de l'operador de telefonia utilitzat en l'aparell. En aquest darrer cas, es podria accedir a la dita agenda de contactes –emmagatzemada a la memòria de l'aparell- simplement extraient l'esmentada targeta SIM, de manera que al reiniciar el dispositiu no seria necessari introduir-hi el PIN.

  En funció dels noms assignats als contactes inclosos en aquesta agenda per la persona propietària del telèfon mòbil (per exemple, *casa*, *mare* o *pare*) podria resultar relativament fàcil la seva localització.

- Accedir al número IMEI de l'aparell (número que permet identificar inequívocament el telèfon mòbil a nivell internacional).

  En el supòsit que l'aparell no estigui protegit per cap dels mecanismes que habitualment incorporen aquests dispositius (PIN, patró, empremta, etc.) per obtenir-lo només és necessari consultar l'apartat de configuració de l'aparell o bé marcar la combinació *#06#.

  Amb independència que el telèfon mòbil estigui o no protegit, aquest número també pot obtenir-se, en funció del model de què es tracti, mirant la superfície de l'aparell que hi ha sota la bateria (cal retirar-la) o bé la lletra petita que consta impresa en el mateix aparell (part del darrera del telèfon o on es col·loca la targeta SIM).

  L'obtenció d'aquest número permetria constatar l'existència d'una denúncia prèvia del propietari del telèfon mòbil per furt o robatori, fins i tot, d'una comunicació de pèrdua de l'aparell i, per tant, la seva identificació i localització.

  Així mateix, cabria l'opció de comunicar aquest número a l'operadora mòbil corresponent, als efectes que aquesta es posés en contacte amb el propietari i li comuniqués la troballa del seu telèfon mòbil i on es troba custodiat.

III

Fetes aquestes consideracions, cal fer avinent que lliurar un telèfon mòbil a una persona diferent al seu propietari, en què es continguin dades de caràcter personal (article 3.a) LOPD i article 5.1.f) del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la LOPD (en endavant, RLOPD)), constituiria, des del punt de vista de la protecció de dades personals, una cessió de dades (article 3.i) LOPD) que s'hauria de sotmetre al règim previst, amb caràcter general, per a les cessions o comunicacions de dades a l'LOPD.

L'article 11.1 de l'LOPD estableix que *"les dades de caràcter personal objecte del tractament només poden ser comunicades a un tercer per al compliment de finalitats directament relacionades amb les funcions legítimes del cedent i del cessionari amb el consentiment previ de l'interessat".* El mateix article disposa, en el seu apartat 2, que el

dit consentiment no és necessari quan, entre d'altres excepcions, la cessió està autoritzada per una llei o norma amb rang de llei (lletra a).

Per tant, la comunicació de dades pretesa requeriria a priori el consentiment previ de l'afectat (o possibles afectats) o, a manca d'aquest, una previsió legal que l'habilités.

Però, és més, en el cas que aquestes dades incloguessin informació sensible o especialment protegida –quelcom que, com s'ha dit, no es pot descartar en el present cas-, la cessió només seria possible quan, a manca d'una llei que l'habilités, l'afectat hi consentís expressament o, segons el cas, expressament i també per escrit.

Així es desprèn de l'article 7 de l'LOPD, el qual disposa que:

> *"2. Només amb el consentiment exprés i per escrit de l'afectat poden ser objecte de tractament les dades de caràcter personal que revelin la ideologia, l'afiliació sindical, la religió i les creences. S'exceptuen els fitxers mantinguts pels partits polítics, els sindicats, les esglésies, les confessions o les comunitats religioses i associacions, les fundacions i altres entitats sense ànim de lucre, amb finalitat política, filosòfica, religiosa o sindical, quant a les dades relatives als seus associats o els seus membres, sens perjudici que la cessió d'aquestes dades requereix sempre el consentiment previ de l'afectat.*
> *3. Les dades de caràcter personal que facin referència a l'origen racial, a la salut i a la vida sexual només poden ser recollides, tractades i cedides quan, per raons d'interès general, així ho disposi una llei o l'afectat hi consenti expressament."*

Tenint en compte que en el cas plantejat no es comptaria amb el consentiment previ de l'afectat (o possibles afectats), caldria disposar d'una norma amb rang de llei que preveiés la comunicació d'aquestes dades a un tercer.

El Reial decret de 24 de juliol de 1889 pel qual es publica el Codi civil (en endavant, CC), a què es fa referència en l'escrit de consulta, estableix, en el seu article 615, que:

> *"El que encontrare una cosa mueble, que no sea tesoro, debe restituirla a su anterior poseedor. Si éste no fuere conocido, deberá consignarla inmediatamente en poder del Alcalde del pueblo donde se hubiese verificado el hallazgo.*
>
> *El Alcalde hará publicar éste, en la forma acostumbrada, dos domingos consecutivos.*
>
> *Si la cosa mueble no pudiere conservarse sin deterioro o sin hacer gastos que disminuyan notablemente su valor, se venderá en pública subasta luego que hubiesen pasado ocho días desde el segundo anuncio sin haberse presentado el dueño, y se depositará su precio.*
>
> *Pasados dos años, a contar desde el día de la segunda publicación, sin haberse presentando el dueño, se adjudicará la cosa encontrada o su valor al que la hubiese hallado.*
>
> *Tanto éste como el propietario estarán obligados, cada cual en su caso, a satisfacer los gastos."*

La Llei 5/2006, de 10 de maig, del llibre cinquè del Codi civil de Catalunya, relatiu als drets reals (en endavant, CCC), estableix, en relació amb la qüestió examinada, que:

> *"Article 542-22 Troballes*
>
> *1. (...)*
> *2. Si els propietaris són desconeguts, la troballa s'ha de notificar a l'ajuntament del lloc on s'ha fet, el qual l'ha de fer pública per mitjà d'un edicte, ha de dipositar*

la cosa durant el termini de sis mesos en l'establiment que determini i ho ha de notificar a les entitats públiques pertinents si les característiques de la troballa ho requereixen.
3. Si els propietaris es presenten dins del termini que estableix l'apartat 2:
a) Se'ls lliura l'objecte perdut una vegada han pagat les despeses ocasionades per la custòdia, la conservació i el lliurament.
b) Han de pagar als trobadors de bona fe el 10% del valor i, si aquest és igual o superior a sis vegades l'import del salari mínim interprofessional, el 4% del que n'excedeix.
4. (...)
5. Si ha transcorregut el termini que estableix l'apartat 2 i els propietaris no s'han presentat:
a) L'objecte es lliura a qui l'ha trobat, que prèviament ha de pagar les despeses causades per la custòdia, la conservació i el lliurament.
b) Si el valor en taxació de la cosa és superior a sis vegades el salari mínim interprofessional, es ven en subhasta pública, a càrrec de l'ajuntament, i els trobadors tenen dret a aquesta quantitat i, a més, a una quarta part de l'excés que s'obtingui en la subhasta. La resta queda a la disposició de l'ajuntament. Si en la subhasta no s'obté una quantitat equivalent a sis vegades el salari mínim interprofessional, els trobadors tenen l'opció de fer seva la cosa.
c) Els propietaris no tenen acció contra els trobadors de bona fe o els adjudicataris per a reivindicar la cosa perduda."

Malgrat que aquestes previsions legals legitimarien el lliurament del telèfon mòbil perdut i no reclamat pel seu propietari en el termini legal establert (6 mesos) al seu trobador, convé tenir en compte que aquestes no habilitarien la comunicació de la informació personal que pogués contenir l'aparell, especialment, si la dita informació comprengués dades sensibles o íntimes (articles 7 i 11 LOPD).

IV

Així doncs, per tal de trobar en el cas plantejat l'adequat equilibri entre el dret del trobador a quedar-se amb el telèfon mòbil (article 542.22 CC) i el dret fonamental a la protecció de dades de l'afectat (article 18.4 CE), es considera que l'entrega d'aquest aparell hauria d'efectuar-se previ esborrat definitiu de la informació personal que pogués conservar (tant en les memòries RAM i ROM com, si fos el cas, en la memòria externa).

Sobre això, tractant-se d'**informació continguda en la targeta SIM** de l'aparell **o**, si escau, en la **targeta de memòria externa**, es considera, atès el reduït cost material d'ambdues, que el mecanisme idoni per garantir aquest esborrat definitiu de les dades seria procedir a llur destrucció física.

Pel que fa a la **informació continguda en la memòria interna** de l'aparell, convé assenyalar, atesos els termes en què s'efectua la consulta, que procedir a formatar el dispositiu mòbil no és un mecanisme adient, des del punt de vista del dret a la protecció de dades, per garantir que la informació emmagatzemada no serà recuperable.

La seva finalitat és adaptar el suport d'emmagatzematge a un format determinat perquè el sistema hi pugui llegir i escriure dades. Això no implica l'esborrat de manera segura i permanent de la informació. El sistema operatiu podria no ser capaç de llegir-la de manera normal però la informació encara hi seria present (aquesta es guarda fins que el sistema operatiu necessita espai per als arxius eliminats més recentment), de tal manera que podria recuperar-se emprant qualsevol programa de recuperació de dades.

Tampoc, cal dir, seria un mecanisme adient procedir a la mera inicialització a l'estat de fàbrica (*reset)* del telèfon mòbil. Tot i que pugui semblar un procés diferent a l'anterior els efectes són els mateixos: els arxius amb la informació romanen invisibles per al sistema operatiu però aquesta continua sent recuperable.

La millor opció per garantir l'esborrat de manera segura i permanent de les dades emmagatzemades en el telèfon mòbil abans del seu lliurament seria, ara per ara, la realització acumulativa de les següents accions:

1. Iniciar el dispositiu en mode de recuperació ocult (*recovery mode*).

   Amb l'aparell apagat cal fer una sèrie de combinació o seqüència de tecles, predeterminada pel fabricant, en el moment d'encendre'l.

2. Emprar el menú que apareix a l'aparell per procedir a reiniciar-lo a l'estat de fàbrica (*reset*).

   Amb caràcter general, aquesta acció suprimeix tota la informació que pugui estar emmagatzemada al dispositiu, si bé, com s'ha dit, encara podria ser recuperable mitjançant eines i programari de recuperació de dades.

3. Xifrar el dispositiu mòbil.

   El reinici a l'estat de fàbrica elimina els mecanismes que pogués tenir l'aparell per protegir-ne l'accés (PIN, patró, empremta, etc.), de tal manera que és possible xifrar-lo mitjançant les eines de xifratge de què disposa (aquest xifratge no seria necessari si el propietari ja ho hagués fet o si el sistema operatiu del dispositiu l'incorporés per defecte, aspectes que es desconeixen en el present cas).

4. Reiterar la inicialització de l'aparell en mode de recuperació ocult (*recovery mode*) que permet procedir a reiniciar-lo a l'estat de fàbrica (*reset*).

5. Instal·lar en l'aparell una aplicació d'esborrat segur del seu contingut i executar-la.

Si bé, amb caràcter general, les accions descrites en anteriors punts 1 a 4 fan irrecuperable la informació del dispositiu mòbil, atès que en alguns aparells el procés de xifratge presenta vulnerabilitats, també és necessari emprar programes o aplicacions que permeten sobreescriure les dades amb bits a l'atzar diverses vegades, de tal manera que aquestes no siguin recuperables (punt 5). Tot això en el benentès que el caràcter canviant de la tecnologia no permet descartar l'aparició en un futur de noves vulnerabilitats que puguin afectar alguna de les operacions a què s'ha fet referència.

En aquest punt, convé tornar a fer referència a l'article 542.22 de l'CCC. Aquest article estableix, en el seu apartat 5.a), que, transcorregut el termini de 6 mesos sense que el propietari reclami l'objecte perdut, aquest es lliura a qui l'ha trobat, *"que prèviament ha de pagar les despeses causades per la custòdia, la conservació i el lliurament".*

Això, traslladat al cas que ara ens ocupa, legitimaria l'Ajuntament per condicionar l'entrega del telèfon mòbil al pagament previ, per part de la persona que el va trobar, de les despeses que originin les tasques d'esborrat definitiu de les dades personals que s'hi contenen.

Ara bé, malgrat que es duguin a terme aquestes tasques, l'Ajuntament ha de tenir en compte que, en funció de les aplicacions que pogués tenir instal·lades el telèfon mòbil objecte de lliurament, cab l'opció que determinades dades personals del propietari siguin encara accessibles.

Ens referim, en concret, a aquella **informació emmagatzemada fora del dispositiu mòbil** (serveis *cloud*) però accessible des de les aplicacions que té instal·lades i, particularment, quan aquestes aplicacions empren, com a mecanisme d'autenticació o d'accés al servei remot d'emmagatzematge d'informació de què es tracti, el número IMEI de l'aparell.

La utilització d'aquest número permet limitar l'accés a la informació d'un dispositiu mòbil concret. Es tracta d'una bona mesura de seguretat en l'accés sempre, és clar, que

l'aparell segueixi en poder del seu propietari. Quan aquest decideix, per exemple, substituir el seu telèfon mòbil per un altre és necessari, als efectes d'evitar que un tercer no autoritzat accedeixi a la informació, desvincular el dispositiu de tots els serveis emprats i modificar-ne les credencials d'accés (contrasenyes) que puguin arribar a combinar-se amb l'ús del número IMEI.

En el present cas es desconeix si el propietari del telèfon mòbil es valia d'aquest tipus de serveis, així com, d'emprar-los, si hauria procedit o no a realitzar aquesta acció de desvinculació i modificació de contrasenyes en el moment en què es va adonar de la pèrdua de l'aparell.

Per tant, no es pot descartar que, d'entregar-se el telèfon mòbil a la persona que el va trobar, es doni la circumstància que aquesta instal·li una nova aplicació –coincident amb una aplicació o servei utilitzat pel seu propietari anterior- i tingui accés a la informació emmagatzemada remotament per aquest.

El fet de no poder garantir que en el present cas la persona que va trobar el telèfon mòbil no podrà accedir a informació personal de l'antic propietari porta a concloure que, des del punt de vista de la protecció de dades, el lliurament de l'aparell podria comportar una comunicació de dades contraria a l'LOPD.

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

Conclusions

El lliurament d'un telèfon mòbil que contingui dades de caràcter personal a la persona que el va trobar un cop transcorregut el termini legal establert per a que el seu propietari el reclami només podria efectuar-se previ esborrat definitiu de les dades que pogués conservar (tant en la memòria interna de l'aparell com en la targeta SIM o, si fos el cas, en la targeta de memòria externa) i sempre que es garantís que no és possible accedir a les dades emmagatzemades remotament per aquest (serveis *cloud*), circumstàncies que, per la informació de què es disposa, no semblarien donar-se en el supòsit examinat.

Barcelona, 21 d'abril de 2016