CNS 49/2015

Dictamen en relació amb la consulta formulada per una empresa pública en relació amb els Protocols de pagament de factures

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una empresa que presta un servei públic (en endavant l'empresa) en el qual es demana que l'Autoritat emeti un dictamen per tal de validar l'adequació a la normativa de protecció de dades dels Protocols relatius als tràmits d'atenció als clients.

En concret, la consulta es refereix al Protocol de pagament telefònic mitjançant targeta de crèdit, i al Protocol de procediment telefònic per al canvi de compte de pagament per domiciliació bancària, que s'adjunten a la consulta formulada.

Analitzada la consulta, vista la normativa 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'empresa explica que treballa en un procés de millora en l'atenció als seus clients, que passa per la simplificació de tràmits i per evitar que els clients s'hagin de desplaçar a les oficines de l'empresa.

La consulta es refereix a dos tipus de gestions que, segons l'empresa, actualment requereixen de la presència dels clients, en concret:

- Pagament extraordinari. L'empresa posa com a exemple reposar fons de rebuts impagats després que, superats els terminis per poder fer-ho per mitjans habituals (domiciliació bancària), s'interromp el subministrament del servei. Com a opció alternativa al pagament presencial, l'empresa planteja el pagament per via telefònica mitjançant targeta de crèdit. S'afegeix que, pel que fa als mitjans informàtics segurs per a la validació de targetes, aquest és un servei que poden proveir diverses entitats. A efectes de preservació de la seguretat i la privacitat de les dades, l'empresa remet al "Protocol de pagament telefònic mitjançant targeta de crèdit", que s'adjunta.

- Canvi del número de compte bancari sobre el que es giren les factures. L'empresa considera que el titular del compte ha de comparèixer presencialment i acreditar documentalment la titularitat del compte. Afegeix que altres empreses prestadores de serveis eviten la presència física i tramiten el canvi per via telefònica. L'empresa adjunta el "Protocol de procediment telefònic per al canvi de compte de pagament per domiciliació bancària" que s'ha previst per a aquest tràmit.

L'empresa demana a l'Autoritat la validació sobre l'adequació a la normativa de protecció de dades de les qüestions plantejades, en els termes previstos en els dos Protocols aportats.

Cal fer avinent que l'objecte d'aquest informe no consisteix en "validar" el contingut dels protocols aportats, especialment en relació amb la seguretat en el tractament de les dades en relació amb els tràmits que l'empresa vol gestionar per via telefònica, validació que no resulta possible, atesa la manca de previsió o concreció en els protocols de qüestions referides a les mesures de seguretat a aplicar en relació amb el dit tractament. Estrictament, la validació d'un determinat procediment o sistema de seguretat en relació amb el tractament de dades personals només es pot realitzar després d'un procediment d'auditoria que s'ha de realitzar, per definició, un cop un determinat tractament de dades es troba implementat.

Tenint en compte això, en aquest informe s'atendrà la consulta formulada tenint en compte els Protocols aportats, posant de manifest aquelles qüestions que siguin rellevants des de la perspectiva de la protecció de dades personals.

Situada la consulta en aquests termes, cal partir de la base que l'article 3.*a)* de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD) defineix les dades personals com qualsevol informació referent a persones físiques identificades o identificables (article 5.1.*o)* del Reial decret 1720/2007, de 21 de desembre, que aprova el Reglament de desenvolupament de la LOPD (RLOPD)).

Segons l'article 3.c) de l'LOPD, es considera tractament de dades el conjunt de les operacions i els procediments tècnics de caràcter automatitzat o no, que permetin recollir, gravar, conservar, elaborar, modificar, bloquejar i cancel·lar, així com les cessions de dades que derivin de comunicacions, consultes, interconnexions i transferències.

Qualsevol tractament que faci l'empresa de les dades dels seus clients, com ara dades identificatives (nom i cognoms, DNI, adreça postal o electrònica, número de telèfon, així com la veu de les persones -en el cas que l'empresa enregistrés la conversa telefònica-), o les dades economicofinanceres (dades bancàries o de targetes de crèdit), entre d'altres, s'ha de sotmetre a la normativa de protecció de dades, independentment del sistema concret que s'articuli per a la recollida de dades i tractament d'aquestes dades (a través de formularis, de forma presencial, telefònicament, etc).

D'acord amb la normativa de protecció de dades, el tractament de dades ha de comptar amb el consentiment inequívoc de l'afectat, llevat que una llei disposi una altra cosa (article 6.1 LOPD). Segons el mateix article 6, apartat 2, no cal el consentiment, entre d'altres, quan les dades es refereixin a les parts d'un contracte o un precontracte d'una relació de negoci, laboral o administrativa, i siguin necessàries per al seu manteniment o compliment.

Per tant, la recollida i el tractament de les dades que resultin necessàries per al manteniment de la relació contractual prèviament establerta entre l'empresa i els seus clients, no requerirà el consentiment dels afectats (article 3.e) LOPD).

Dit això, a continuació es fa referència al tractament de dades a través del servei telefònic previst als Protocols que s'adjunten.

III

Protocol de pagament telefònic mitjançant targeta de crèdit.

Segons la informació aportada, l'operador de l'empresa ha de preguntar a l'abonat les següents dades, per tal d'identificar-lo:

- El nom del titular de la pòlissa objecte del pagament
- El DNI del titular de la pòlissa objecte del pagament
- El número de pòlissa objecte del pagament.

L'empresa pot tractar legítimament les dades dels seus clients (article 6.2 LOPD), sempre que aquestes resultin necessàries, en atenció al principi de qualitat (article 4.1 LOPD), segons el qual:

> *"Les dades de caràcter personal només es poden recollir per ser tractades, així com sotmetre-les a aquest tractament, quan siguin adequades, pertinents i no excessives en relació amb l'àmbit i les finalitats determinades, explícites i legítimes per a les quals s'han obtingut."*

La sol·licitud d'aquestes dades per part de l'operador quan atén un client per via telefònica, es considera ajustat al principi de qualitat, ja que no resulta excessiu demanar el nom i DNI per identificar un usuari d'una determinada pòlissa, en relació amb la que es vol realitzar un tràmit (en aquest cas, el pagament per via telefònica mitjançant targeta de crèdit).

Des de la perspectiva del principi de finalitat, les dades de caràcter personal objecte de tractament no es poden utilitzar per a finalitats incompatibles amb aquelles per a les quals les dades han estat recollides (article 4.2 LOPD).

Partim de la premissa que l'empresa ja disposa d'aquestes dades (nom i DNI del titular de la pòlissa), ja que en el seu moment s'haurien recollit per a l'establiment de la relació contractual amb el client (subministrament del servei públic).

Respecte d'això, consta inscrit en el Registre de Protecció de Dades de Catalunya (RPDC), el fitxer *"Dades dels abonats",* del qual és responsable l'empresa (article 3.d) LOPD). Aquest fitxer té per finalitat la creació de l'oficina virtual a la web de l'empresa, on es posen dades dels abonats (consums, lectures, factures...), segons la informació que consta al RPDC. Entre les dades tractades en aquest fitxer, consten el nom i cognoms i DNI dels usuaris.

Pel que fa al "número de pòlissa objecte de pagament" que, segons el Protocol, l'operador també ha de sol·licitar al client en el tràmit telefònic, sembla que seria una dada que la pròpia empresa facilita al client. Atès que, segons es desprèn de la informació aportada, el tràmit al que es refereix el Protocol consisteix en fer un pagament relacionat amb el servei que rep l'usuari en relació amb una pòlissa determinada, resulta adequat que l'operador sol·liciti la confirmació d'aquest número de pòlissa, per a identificar el titular i el tràmit que es vol realitzar telefònicament.

Per tant, el fet que, quan el client o usuari es comunica amb l'empresa per via telefònica se li demanin les dades esmentades en el Protocol a efectes d'identificar-lo, resulta legítim i ajustat als principis de qualitat i de finalitat.

Cal fer notar que la sol·licitud de les dades indicades en el Protocol (nom i DNI del titular de la pòlissa i el número de pòlissa), no implica necessàriament que la persona que truca

per telèfon sigui el titular de la pòlissa, ja que podria ser una altra persona, diferent del titular, que amb consentiment d'aquest -o fins i tot sense el seu consentiment, ja que així ho permet l'article 1158 del Codi Civil-, truca a l'empresa per realitzar el tràmit en nom del titular, facilitant les dades d'aquest. En aquest cas, si l'empresa recull el nom o altres dades d'aquest tercer que truca per realitzar el tràmit en nom del titular de la pòlissa, com ara la vinculació o relació familiar amb el titular, haurà d'aplicar, respecte d'aquestes dades, els mateixos principis i garanties de la normativa de protecció de dades que ha d'aplicar a les dades dels usuaris o abonats.

El Protocol preveu que, un cop identificat el titular i la pòlissa respecte la qual es vol fer el pagament, l'operador sol·liciti informació de la targeta de crèdit amb la que es realitzarà el pagament, en concret:

- *Titular de la targeta de crèdit o dèbit*
- *Tipus de targeta*
- *Nº de targeta de crèdit*
- *Caducitat*
- *Codi de seguretat (segons tipus de targeta)*

Tenint en compte que l'únic tràmit que es pot realitzar en el cas que ens ocupa és un pagament respecte un deute relacionat amb una pòlissa concreta, i no al contrari (obtenció de diners o d'altres prestacions), d'entrada, el risc que algun tercer realitzi una suplantació fraudulenta del client per realitzar aquest tràmit, és baix.

Tot i així, cal apuntar que les dades previstes en el Protocol (nom i DNI del titular de la pòlissa i número de la pòlissa) es poden aconseguir de qualsevol de les factures que arriben a l'abonat, de manera que, al menys hipotèticament, podria donar-se el cas que un tercer que accedeixi a la factura sense el consentiment i coneixement del titular, es comuniqui per telèfon amb l'empresa i intenti aconseguir dades del client (en concret, les dades de la targeta de crèdit), és a dir, que suplanti el client per tal d'obtenir-ne informació.

Aquest és un risc que cal evitar, des del punt de vista de la seguretat, ja que implicaria una comunicació indeguda d'informació sobre un client, susceptible de ser utilitzada de forma fraudulenta.

Per una banda, el Protocol pot preveure que l'operador demani alguna dada complementària, que només aparegui en la comunicació de requeriment de pagament extraordinari que l'empresa envia al client, com ara un número de referència específic o fins i tot la quantitat a abonar, per tal d'identificar amb major seguretat al client o abonat i assegurar que és aquest –o un tercer amb autorització d'aquest-, el qui realitza el tràmit de forma legítima.

Per altra banda, el Protocol ha d'explicitar que el flux informatiu que s'ha de produir entre l'interlocutor i l'operador de l'empresa, amb la única finalitat de realitzar el pagament, haurà de ser sempre unidireccional, en el sentit que l'operador recollirà les dades de l'interlocutor, i en cap cas a la inversa. Cal assegurar que l'operador no facilitarà cap dada personal del client (ni les indicades en el Protocol ni cap altra dada personal, com ara adreces, telèfons de contacte, etc) a l'interlocutor que realitza la gestió per telèfon.

En aquests termes, que s'haurien de reflectir en el Protocol, es pot considerar que el flux informatiu previst compliria uns paràmetres adequats des del punt de vista de la seguretat i la protecció de les dades personals.

IV

El Protocol de pagament telefònic mitjançant targeta de crèdit, estableix que:

"L'operador procedirà a sol·licitar les dades i apuntarà les respostes directament en el programa de pagament segur de l'entitat financera sense prendre anotació en cap altra mitjà ni escrit ni informàtic:

- Titular de la targeta de crèdit o dèbit
- Tipus de targeta
- Nº de targeta de crèdit
- Caducitat
- Codi de seguretat (segons tipus de targeta)

Un cop validats els valors, es preguntarà a l'abonat si està d'acord en fer el pagament i si la resposta és afirmativa es validarà el pagament i guardarà les dades de manera segura".

La consulta explica que, respecte la gestió del pagament per via telefònica mitjançant targeta de crèdit, pel que fa als mitjans informàtics segurs per a la validació de targetes, *"aquest és un servei que poden proveir diverses entitats",* sense afegir més informació. La consulta no concreta quines són aquestes entitats, ni els mitjans segurs, ni les característiques d'aquests mitjans a efectes de la preservació de la seguretat de la informació, sinó que remet a les previsions del Protocol, en les que tampoc no es detallen aquests extrems.

Pel que fa a les dades de la targeta de crèdit, citades, que el Protocol preveu comunicar al programa de pagament segur de l'entitat financera, es considera que la seva comunicació s'ajusta a les exigències dels principis de qualitat i de finalitat, als que s'ha fet esment, ja que poden resultar necessàries per a la finalitat prevista, que és fer un pagament amb una determinada targeta de crèdit.

En qualsevol cas, i tenint en compte la informació aportada, cal fer avinent que l'empresa, en recollir les dades relatives al titular de la targeta de crèdit i altra informació de la targeta, està realitzant un tractament de dades com a responsable, als efectes de l'LOPD, per bé que aquest tractament consisteixi en introduir les dades en un programa informàtic d'un tercer (una entitat financera).

Això suposa una comunicació de dades (article 3.i) LOPD), que ha d'estar sotmesa al règim general previst en l'article 11 de l'LOPD, segons el qual les dades objecte de 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"* (article 11.1 LOPD).

Aquesta regla general troba però determinades excepcions, entre les quals, que la comunicació estigui autoritzada en una llei o norma amb rang de llei (article 11.2.a) LOPD), o *"quan el tractament respongui a la lliure i legítima acceptació d'una relació jurídica el desenvolupament, el compliment i el control de la qual impliqui necessàriament la connexió del tractament esmentat amb fitxers de tercers. En aquest cas, la comunicació només és legítima quan es limiti a la finalitat que la justifiqui"* (art. 11.2.c) LOPD).

En el cas plantejat, l'empresa habilita per als seus clients la possibilitat de realitzar determinats pagaments mitjançant targeta de crèdit per via telefònica, a través d'un programa informàtic d'una entitat financera. Aquest flux informatiu suposa una cessió de dades, en la que el cessionari final seria una entitat financera, és a dir, un tercer diferent

de l'afectat –el client- (art. 3.e) LOPD), i de l'empresa. Aquesta cessió de les dades dels clients de l'empresa, s'emmarcaria en la relació jurídica contractual entre l'empresa i aquests.

En aquests termes, i pel que fa a la gestió prevista en el Protocol, es pot considerar que el propi desenvolupament de la dita relació jurídica entre l'afectat i l'empresa requereix la comunicació de determinades dades a l'entitat financera.

Des d'aquesta perspectiva, l'article 11.2.c) de l'LOPD pot habilitar la comunicació de determinades dades que l'empresa sol·licita al client, a l'entitat financera, per tal que es pugui dur a terme el pagament corresponent.

V

En atenció a la normativa de protecció de dades, cal fer especial atenció a la seguretat de la informació personal objecte de tractament per part de l'empresa i de comunicació a l'entitat financera.

Segons disposa l'article 9.1 de l'LOPD:

> *"El responsable del fitxer i, si s'escau, l'encarregat del tractament han d'adoptar les mesures de caràcter tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, tant si provenen de l'acció humana o del medi físic o natural."*

Com ha quedat dit, l'empresa és la responsable, als efectes de l'LOPD, de les dades dels seus clients i abonats, incloses les necessàries per realitzar els cobraments per via telefònica mitjançant targeta de crèdit.

El Protocol explicita que l'operador no fa cap anotació per mitjà escrit o informàtic de les dades. Sembla que, segons el Protocol, l'empresa no conservaria les dades de la targeta de crèdit i del seu titular, sinó que únicament les introdueix en un programa de pagament segur d'una entitat financera (un tercer).

Ara bé, el propi Protocol explica que l'operador preguntarà a l'abonat si està d'acord en fer el pagament, i si és així, un cop validat el pagament, *"guardarà les dades de manera segura".* Això dóna a entendre que l'empresa sí conservarà les dades referents a la targeta de crèdit i al seu titular, cosa que resulta contradictòria amb l'afirmació anterior del Protocol, en el sentit que l'operador (l'empresa, en definitiva), no fa cap "anotació".

Cal considerar que l'empresa podria conservar, al menys, el número de la targeta de crèdit amb la que s'ha realitzat el pagament, a efectes de possibles reclamacions o comprovacions posteriors, tant a instàncies de l'empresa com del propi interessat.

En qualsevol cas, el Protocol hauria d'aclarir aquesta qüestió, relativa a la conservació de les dades en qüestió, i a quins efectes es conserven.

Des de la perspectiva de la seguretat del flux informatiu previst i de les dades objecte de tractament, resultaria necessari afegir en el Protocol una mesura específica que limiti el possible mal ús de les dades de la targeta de crèdit de l'abonat, com és identificar l'operador que fa la transacció amb la passarel.la de pagament bancària.

En definitiva, el Protocol hauria de preveure que l'empresa conservarà unes mínimes dades necessàries del fet que s'ha produït la transacció (data, operador que la realitza, en relació amb quin pagament, així com el número de la targeta amb el que s'ha efectuat el pagament), als efectes de comprovació posterior que l'operació s'ha realitzat.

La normativa de protecció de dades estableix diferents nivells de seguretat (art. 80 RLOPD). Pel que fa a les dades que es tracten en el cas que ens ocupa, resultarien d'aplicació les mesures de seguretat de nivell bàsic, atès el que disposa l'article 81.1 LOPD. Això, sens perjudici que l'empresa pot aplicar altres mesures de seguretat, més enllà de les exigibles de nivell bàsic.

No comportaria necessàriament l'aplicabilitat d'un nivell mitjà de seguretat, perquè tot i que es tracta d'informació economicofinancera, no es tracta d'un fitxer d'una entitat financera per finalitats relacionades amb la prestació de serveis financers. En aquest sentit, l'article 81.2.d) RLOPD disposa que:

> *"2. S'han d'implantar, a més de les mesures de seguretat de nivell bàsic, les mesures de nivell mitjà, en els següents fitxers o tractaments de dades de caràcter personal:*
> *(...)*
> *d) Aquells els responsables dels quals siguin les entitats financeres per a finalitats relacionades amb la prestació de serveis financers.*
> *(...)".*

En canvi, pel que fa al tractament de les dades dels clients que farà l'entitat financera a través del seu programa informàtic, en aquest cas sí es tractaria d'un fitxer o tractament responsabilitat d'una entitat financera per a la "prestació de serveis financers". Per tant, pel que fa a l'entitat financera, en aquest cas correspondria l'aplicació del nivell mitjà de mesures de seguretat, segons el que disposa el RLOPD.

Sobre això, val a dir que la Llei 22/2007, d'11 de juliol, de comercialització a distància de serveis financers, preveu en el seu article 4 que:

> *"2. A los efectos de la presente Ley,* ***se entenderán por servicios financieros los servicios bancarios, de crédito o de pago,*** *los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros. (...)".*

VI

Protocol de procediment telefònic per al canvi de compte de pagament per domiciliació bancària

El Protocol preveu que l'operador s'ha d'assegurar que l'interlocutor és l'abonat titular de la pòlissa i titular del nou compte bancari i que, si no és així, la gestió s'ha de fer de forma presencial. S'ha de valorar positivament, des del punt de vista de la seguretat, que la gestió telefònica es limiti als casos en que es pugui assegurar que l'interlocutor és l'abonat i titular del compte.

Segons el Protocol, l'operador confirmarà el nom i el DNI del titular de la pòlissa objecte de canvi de compte de domiciliació bancària, així com els darrers quatre números de l'actual compte de domiciliació bancària.

L'empresa ja disposa d'aquestes dades, atesa la relació contractual amb el client (art. 6.2 LOPD), en el fitxer *"Dades dels abonats",* responsabilitat de l'empresa, i per tant pot dur a terme la comprovació.

Ara bé, cal tenir en compte que un mateix titular podria tenir diverses pòlisses contractades al seu nom amb l'empresa. Els pagaments corresponents a aquestes diverses pòlisses, poden estar associades a un mateix compte bancari de pagament, o bé a diferents comptes. Tenint en compte això, resulta necessari complementar la informació que l'operador sol·licita a l'abonat. Concretament, l'operador hauria de sol·licitar al client el número de pòlissa en relació amb la qual es vol efectuar un canvi de compte de pagament per domiciliació bancària. D'aquesta manera, s'evita el risc de modificar el compte de pagament en relació amb una pòlissa que no correspon i, per tant, modificar de forma errònia determinades dades personals del titular.

Caldria, doncs, fer constar en el Protocol que l'operador confirmarà, a més del nom i DNI del titular i els darrers quatre números de l'actual compte, el número de pòlissa –o de pòlisses- que el titular vol assignar a un nou número de compte de pagament.

VII

El Protocol preveu que l'operador *"apuntarà les respostes directament en el programa d'abonats",* sense afegir més informació al respecte.

Atesa la informació que s'aporta, partim de la base que el "programa d'abonats" és un programa responsabilitat de la pròpia empresa, que aquesta utilitza per domiciliar els pagaments dels seus clients, a través de les entitats financeres corresponents.

Que l'operador apunti les dades que li comunica el client en un programa d'abonats de l'empresa a efectes d'actualitzar les dades bancàries (compte corrent) per poder efectuar els cobraments corresponents, no resulta problemàtic des de la perspectiva de la protecció de dades personals, ja que la finalitat d'aquest tràmit consisteix en què l'empresa tingui actualitzades les dades del client, i pugui cobrar els pagaments que el client domicilia en la seva entitat financera.

Fem notar que el Protocol de procediment telefònic per al canvi de compte de pagament per domiciliació bancària, preveu que s'informarà l'abonat, entre d'altres, que *"és de la seva responsabilitat la validesa i correcció de les dades que ha donat".*

Segons disposa l'article 4.3 de l'LOPD, *"les dades de caràcter personal han de ser exactes i posades al dia de manera que responguin amb veracitat a la situació actual de l'afectat."*

Per tant, l'empresa, com a responsable del tractament de les dades dels seus abonats, té un deure de mantenir actualitzada i veraç la informació personal d'aquests.

En relació amb el Protocol examinat, l'empresa haurà d'aplicar al programa d'abonats, i a les dades que s'hi contenen (a les que es refereix el Protocol) les mesures de seguretat corresponents, com a mínim, de nivell bàsic (article 9 LOPD i Títol VIII RLOPD).

En el Protocol s'indica que aquest servei l'atendrà un nombre reduït i delimitat de treballadors, que estaran específicament formats per a aquesta funció.

L'article 91 del RLOPD preveu el control d'accessos com a mesura de seguretat de nivell bàsic (articles 89 a 94 RLOPD) i, per tant, aplicable a qualsevol fitxer o tractament de dades, en els següents termes:

> *"1. Els usuaris han de tenir accés només als recursos que necessitin per a l'exercici de les seves funcions.*
> *2. El responsable del fitxer s'ha d'encarregar que hi hagi una relació actualitzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.*
> *3. El responsable del fitxer ha d'establir mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.*
> *(...)".*

El fet que el Protocol prevegi que només un nombre reduït i delimitat de treballadors accediran i tractaran les dades especificades en el Protocol, s'ha de valorar positivament des de la perspectiva de la seguretat de la informació, ja que resulta coherent amb l'exigència de l'article 91 del RLOPD, citat, i permet minimitzar el risc d'un tractament inadequat de la informació dels clients. Això, amb més motiu, tenint en compte que el Protocol preveu que aquests treballadors rebran una formació específica.

Fem extensible aquesta consideració i valoració positiva en relació amb l'anterior Protocol, que inclou la mateixa previsió respecte el personal que atendrà el servei.

Sens perjudici d'això, el Protocol hauria d'incloure algunes previsions més, que s'apunten a continuació, des de la perspectiva de la seguretat en el tractament de la informació personal dels afectats (article 3.e) LOPD).

Cal tenir en compte el risc que el titular del compte, o un tercer que hagi pogut accedir a la informació sol·licitada per fer el canvi, en realitzar la gestió prevista en el Protocol, faciliti com a nou compte de pagament, el d'una tercera persona que posteriorment no vol assumir el pagament, que faciliti un compte que no és operatiu, etc.

Per minimitzar aquest risc, el Protocol hauria de preveure que, un cop realitzat el canvi de compte corrent en el programa d'abonats de l'empresa, es comunicarà al titular del compte que s'ha produït el canvi de número de compte corrent, en relació amb una pòlissa determinada. Això es podria fer, per exemple, a través d'una trucada telefònica de confirmació al número de telèfon associat a la pòlissa efectuada per l'empresa, per escrit, a través d'un missatge de correu electrònic o d'un missatge de text al número de mòbil de contacte que el titular hagi facilitat a l'empresa, etc.

Amb aquest enviament de la confirmació de la gestió, l'empresa s'assegura que el titular rep informació suficient de l'operació realitzada, de manera que aquest titular no podria al·legar, posteriorment, per exemple, desconeixement o confusió respecte el nou número de compte facilitat a l'empresa.

Finalment, el programa d'abonats hauria d'identificar l'operador que fa la transacció de canvi de compte bancari, als mateixos efectes indicats per a l'anterior Protocol.

VIII

Els dos Protocols examinats no especifiquen si les trucades telefòniques relacionades amb la gestió del pagament extraordinari i amb la gestió del canvi de número de compte corrent, seran enregistrades.

En principi no sembla que l'empresa hagi previst l'enregistrament de trucades, ja que el fitxer *"Dades dels abonats",* citat, no preveu el tractament de la veu, ni se'n fa esment en els Protocols.

En qualsevol cas, cal fer avinent que la recollida de dades personals a través d'un servei de telefonia ha de ser considerada, en sí mateixa, com una operació de tractament de dades (art. 3.a) LOPD i article 5.1.f) RLOPD).

No s'ha de descartar la possibilitat o fins i tot la conveniència que l'empresa enregistri les trucades, per acreditar tècnicament evidències que permetin investigar qualsevol incident de seguretat amb les dades de l'abonat.

En qualsevol cas, si l'empresa considera adequat (tenint en compte les exigències dels principis de qualitat i de finalitat) l'enregistrament de les trucades en els casos a què es refereixen els Protocols, a banda d'adequar el fitxer corresponent, l'empresa haurà d'informar els clients del fet que s'està enregistrant la trucada.

L'article 5.1 de l'LOPD regula el deure d'informació en la recollida d'informació provinent de les mateixes persones afectades, en els termes següents:

> *"Els interessats als quals se sol·licitin dades personals han de ser prèviament informats de manera expressa, precisa i inequívoca:*
> *a) De l'existència d'un fitxer o un tractament de dades de caràcter personal, de la finalitat de la recollida de les dades i dels destinataris de la informació.*
> *b) Del caràcter obligatori o facultatiu de la resposta a les preguntes que els siguin plantejades.*
> *c) De les conseqüències de l'obtenció de les dades o de la negativa a subministrar-les.*
> *d) De la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.*
> *e) De la identitat i la direcció del responsable del tractament o, si s'escau, del seu representant.*
> *Quan el responsable del tractament no estigui establert en el territori de la Unió Europea i utilitzi en el tractament de dades mitjans situats en territori espanyol, ha de designar, llevat que aquests mitjans s'utilitzin amb finalitats de tràmit, un representant a Espanya, sens perjudici de les accions que es puguin emprendre contra el mateix responsable del tractament."*

El compliment del deure d'informació resulta especialment important, ja que permet als afectats (article 3.e) LOPD), en aquest cas, els clients de l'empresa, tenir informació adequada sobre el tractament que es realitza de les seves dades personals, i per tant és d'especial importància per a poder exercir els drets que l'LOPD atorga, i que conformen el dret d'autodeterminació informativa (drets d'accés, rectificació, cancel·lació i oposició, o drets ARCO).

En el cas que ens ocupa, això es pot dur a terme, per exemple, amb la reproducció d'un missatge enregistrat prèviament, a l'inici de la conversa de l'operador amb el client.

D'acord amb les consideracions fetes en relació amb la consulta formulada, i vist el contingut dels dos Protocols previstos per l'empresa, d'acord amb la legislació de protecció de dades personals, es fan les següents,

Conclusions

1) Pel que fa al Protocol de pagament telefònic mitjançant targeta de crèdit:

Caldria assegurar en el Protocol que l'operador no facilitarà cap dada personal del client (ni les indicades en el Protocol ni cap altra dada personal) a l'interlocutor que realitza la gestió per telèfon.

El Protocol hauria de preveure la conservació d'unes mínimes dades necessàries del fet que s'ha produït la transacció (data, identificació de l'operador que la realitza, en relació amb quin pagament, així com el número de la targeta amb el que s'ha efectuat el pagament), als efectes de comprovació posterior.

2) Pel que fa al Protocol de procediment telefònic per al canvi de compte de pagament per domiciliació bancària:

El Protocol hauria de preveure que l'operador confirmarà, a més del nom i DNI del titular i els darrers quatre números de l'actual compte, el número de pòlissa –o de pòlisses- a les quals el titular vol assignar el nou número de compte de pagament.

El Protocol hauria de preveure que, un cop realitzat el canvi de compte corrent en el programa d'abonats de l'empresa, es comunicarà al titular del compte que s'ha produït el canvi de número de compte corrent, en relació amb una pòlissa determinada.

El programa d'abonats hauria d'identificar l'operador que fa la transacció de canvi de compte bancari.

3) Si l'empresa enregistra les trucades a què es refereixen els Protocols, haurà d'informar els clients del fet que s'està enregistrant la trucada (article 5 LOPD).

Barcelona, 21 d'octubre de 2015