CNS 42/2017

Dictamen en relació amb la consulta sobre la pràctica d'auditories consistent en un mostreig de diferents seus físiques del responsable seleccionades a l'atzar

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit d'una Administració pública, en relació amb una inspecció que s'hauria dut a terme, segons la consulta, a un Centre de recerca de l'àmbit de la salut (en endavant, el Centre).

Arran de la realització d'aquesta inspecció, la consulta sol·licita a aquesta Autoritat una avaluació de la legalitat del procediment emprat pel citat Centre, on la pràctica habitual de les auditories seria, segons exposa la consulta, *"fer un mostreig de les diferents seus físiques agafades a l'atzar".*

Segons la consulta, tenint en compte la previsió de l'article 96 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de l'LOPD (RLOPD), l'auditoria hauria d'abastar tots els centres, *"ja que segurament entre ells no existeix una identitat absoluta de sistemes, instal·lacions i emmagatzematge".*

Analitzada la petició, que no s'acompanya de cap altra documentació, vista la normativa vigent aplicable, i l'informe de l'Assessoria Jurídica, es dictamina el següent.

I

(...)

II

Per la informació aportada, les funcions que du a terme el Centre estarien relacionades, dins l'àmbit de l'atenció sanitària, amb la prestació de determinats tractaments mèdics (...) i amb la recerca mèdica.

En qualsevol cas, la informació personal (art. 3.a) Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD)) que el Centre pugui tractar per a dur a terme les seves funcions, es troba protegida pels principis i garanties de la normativa de protecció de dades de caràcter personal (LOPD i RLOPD). També cal tenir en compte el Reglament general de protecció de dades (UE) 2016/679 (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)).

En concret, per la informació de què es disposa, la informació personal que tracta el Centre podria ser, en bona mesura, informació de salut (art. 7.3 LOPD i arts. 4.15 i 9 RGPD), continguda en la història clínica dels pacients que atén el Centre, que es troba regulada i protegida per una regulació específica (Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica, i Llei 41/2002, de 14 de novembre, bàsica, reguladora de l'autonomia del pacient i de drets i obligacions en matèria d'informació i documentació clínica).

Als efectes que interessen, les dades de salut, entre d'altres categories de dades, requereixen una especial protecció (art. 7 LOPD i art. 9 RGPD) i, en conseqüència, han de protegir-se amb mesures que podem qualificar com de "nivell alt", tenint en compte els nivells de seguretat establerts en la normativa de protecció de dades –art. 9 LOPD i art. 81 i Títol VIII RLOPD-. Això, sens perjudici de les previsions sobre mesures de seguretat aplicables en cada cas, que puguin derivar-se del RGPD.

En aquest context, als efectes d'aquest informe cal tenir en compte que la normativa de protecció de dades preveu la realització d'auditories, en els termes de l'article 96 RLOPD, segons el qual:

> *"1. A partir del nivell mitjà,* ***els sistemes d'informació i instal·lacions de tractament i emmagatzematge de dades*** *s'han de sotmetre, almenys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol. Amb caràcter extraordinari, s'ha de realitzar l'auditoria esmentada sempre que es facin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades, amb l'objecte de verificar-ne l'adaptació, adequació i eficàcia. Aquesta auditoria inicia el còmput de dos anys assenyalat en el paràgraf anterior.*
> *2. L'informe d'auditoria ha de dictaminar sobre l'adequació de les mesures i controls a la Llei i el seu desplegament reglamentari, identificar les seves deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, fets i observacions en què es basin els dictàmens assolits i les recomanacions proposades.*
> *3. Els informes d'auditoria els ha d'analitzar el responsable de seguretat competent, que n'ha d'elevar les conclusions al responsable del fitxer o tractament perquè adopti les mesures correctores adequades, i han de quedar a disposició de l'Agència Espanyola de Protecció de Dades o, si s'escau, de les autoritats de control de les comunitats autònomes."*

Situat el context normatiu de la consulta, es sol·licita a aquesta Autoritat que avaluï si l'auditoria que, segons la consulta, hauria realitzat el dit Centre, *"on la pràctica habitual de les auditories és fer un mostreig de les diferents seus físiques agafades a l'atzar",* s'ajusta a la legalitat.

Cal fer avinent que el disseny, la planificació, l'avaluació o la revisió de les auditories internes o externes que, específicament, pugui dur a terme el responsable d'un determinat tractament de dades (art. 3.c) LOPD), com a *"persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, el contingut i l'ús del tractament"* (art. 3.d) LOPD), correspon al propi responsable, per bé que els resultats de les auditories realitzades hagin de quedar a disposició d'aquesta Autoritat, als efectes oportuns (art. 96.3 RLOPD).

En qualsevol cas, la informació aportada no permet avaluar, amb un abast general, si l'auditoria que hauria realitzat el Centre s'ajusta a les exigències de la normativa de protecció de dades de caràcter personal, ja que no es disposa d'informació completa sobre el programa d'auditoria del responsable (el Centre), entès com el document en el qual s'han de detallar i explicar els procediments d'auditoria que aplica el responsable, sinó que es coneix, només, un element concret d'aquesta auditoria, com és el fet que s'hauria dut a terme, segons la consulta, a través d'un mostreig de diferents seus físiques del responsable, triades de forma aleatòria.

Per tant, l'objecte d'aquest dictamen ha de ser únicament la valoració, en termes generals, de la possibilitat de realitzar una auditoria mitjançant un mostreig aleatori de

diferents seus físiques d'un únic responsable, des de la perspectiva de la normativa de protecció de dades de caràcter personal (art. 96 RLOPD).

III

Com ha quedat apuntat, la responsabilitat de realitzar les auditories dels sistemes d'informació (art. 96 RLOPD), recau en el responsable del tractament de dades i, si s'escau, en l'encarregat del tractament (art. 9.1 LOPD, art. 12 LOPD i arts. 20 a 22 RLOPD).

Per la informació de què es disposa, el Centre seria el responsable (art. 3.d) LOPD) del tractament sobre el que s'hauria dut a terme l'auditoria, el qual du a terme les seves tasques a través de diferents seus físiques, segons es desprèn de la consulta.

Els sistemes d'informació, que serien l'objecte de l'auditoria que, segons la consulta, hauria realitzat el Centre, podem considerar que són el conjunt organitzat d'elements que s'interrelacionen i que poden ser elements físics, lògics i organitzatius que comporten el tractament d'informació de tot tipus, sigui de caràcter personal o no.

Amb caràcter general, podem considerar que integren els sistemes d'informació d'una entitat o empresa (en el cas que ens ocupa, el Centre) el conjunt de persones o usuaris que integren l'organització i utilitzen o tracten la informació, així com la pròpia informació, es tracti o no d'informació personal, i també el conjunt d'activitats o processos realitzats dins l'organització en relació amb la informació tractada, els fluxos informatius que es generen, i també els recursos materials emprats en aquests processos.

Als efectes de la normativa de protecció de dades, i segons disposa l'article 5.2.m) del RLOPD, constitueix un sistema d'informació el conjunt de fitxers, tractaments, programes, suports i, si s'escau, equips utilitzats per al tractament de dades de caràcter personal. També haurem de tenir en compte que, segons el mateix article 5.2, apartat n) del RLOPD, constitueix un sistema de tractament la manera en què s'organitza o utilitza un sistema d'informació. És a dir, atenent al sistema de tractament, els sistemes d'informació poden ser automatitzats, no automatitzats o parcialment automatitzats.

La normativa (art. 96.2 RLOPD), preveu que l'auditoria s'ha de traduir en un informe que ha de tenir uns continguts mínims. En concret, l'informe d'auditoria ha de dictaminar sobre l'adequació de les mesures i controls a la normativa, ha d'identificar les deficiències que s'hagin detectat i proposar mesures correctores i recomanacions, incloent les dades, fets i observacions en què es basin aquestes recomanacions.

Ara bé, més enllà d'això, la normativa no estableix ni exigeix una metodologia determinada per a dur a terme l'auditora. A sensu contrari, cal entendre que la normativa tampoc no exclou amb caràcter general que es puguin utilitzar determinats mètodes d'anàlisi en el marc d'una auditoria, com podria ser el que és objecte de consulta.

En qualsevol cas, la normativa de protecció de dades no exigeix que necessàriament hagin de ser objecte d'auditoria totes i cadascuna de les instal·lacions de què disposa el responsable (i, si escau, l'encarregat del tractament), ni tampoc que cada auditoria que realitza un responsable (que, recordem, s'han de realitzat amb una periodicitat mínima bianual), hagi d'abastar, necessàriament, tots i cadascun dels fitxers, tractaments, programes, suports, equips, processos o instal·lacions de què disposa el responsable per a tractar la informació.

Per tant, a priori, no es pot descartar la validesa, com a metodologia d'auditoria, de fer una selecció prèvia de determinats fitxers, suports, equips, o instal·lacions del responsable, que hauran de ser l'objecte de l'auditoria, a través d'una selecció prèvia i aleatòria de determinats recursos del responsable, descartant-ne d'altres (sistema de mostreig aleatori).

La consulta apunta que no hi ha una *"identitat absoluta en els sistemes, instal·lacions i emmagatzematge"* del responsable.

Sobre això, cal fer notar que aquesta "identitat absoluta" difícilment es dona en el tractament de dades efectuat per un responsable que operi, com el Centre, a través de diferents seus, ja que el personal específicament adscrit a cada seu (usuaris), els fitxers, els equips i, en definitiva, els recursos humans i materials utilitzats en cada seu, no són, lògicament, idèntics.

Ara bé, certament, i amb caràcter general, sí es pot apuntar que el sistema d'auditoria consistent en un mostreig aleatori, com el que és objecte de consulta, pot ser un mecanisme vàlid sempre que els sistemes d'informació i el tractament de dades dut a terme a les diferents seus -en aquest cas, del Centre-, sigui mínimament homogeni, és a dir, que presenti unes característiques substancialment similars o equiparables.

Partint d'aquesta premissa, en qualsevol cas, el factor que resulta determinant a l'hora de valorar si el mostreig aleatori pot ser un mètode d'auditoria vàlid o no en un determinat cas, és que la mostra seleccionada (ja sigui de fitxers, de processos o, com en el cas plantejat, de les diferents seus físiques del Centre en les que es realitzarà l'auditoria), sigui suficientment representativa del tractament de dades que du a terme el responsable que es sotmet a l'auditoria.

A tall d'exemple, si en una determinada seu física el responsable du a terme un tractament de la informació que, qualitativament o quantitativament, és especialment significatiu (per exemple, en una seu del Centre es tracta el 80% de la informació dels pacients, mentre que en una altra seu només es du a terme un tractament de dades relacionat amb qüestions d'organització administrativa del Centre), això podria ser un element a tenir en compte per tal de fer la selecció de les seus del Centre que han de ser objecte de l'auditoria. En aquest cas, i sempre a títol d'exemple, podria no ser pertinent excloure de la selecció aleatòria la seu en la que es du a terme el tractament principal (el tractament més significatiu, qualitativa o quantitativament) de la informació.

També com a exemple, si els sistemes d'informació presenten unes característiques similars en les diferents seus d'un únic responsable (si no presenten diferències qualitatives o quantitatives significatives o substancials) i es realitzen auditories periòdiques en algunes seus, seleccionades a l'atzar, sempre que el sistema de mostreig es faci de forma rotatòria i de manera que totes les seus (tots els sistemes d'informació) acabin essent auditades en un període determinat de temps, el sistema de mostreig podria ser un sistema vàlid d'auditoria.

En qualsevol cas, i més enllà d'aquests o d'altres exemples il·lustratius, la utilització d'un mètode d'auditoria consistent en fer un mostreig aleatori, que pot ser vàlid en determinats casos, haurà d'estar previst en el corresponent programa d'auditoria del responsable, i haurà de justificar-se en base a les característiques dels sistemes d'informació i dels recursos humans i materials del responsable, al volum i tipologia d'informació personal tractada, i, en definitiva, en base a les particulars característiques del tractament de dades que es dugui a terme en cada cas.

En aquest punt, cal tenir en compte que el RGPD configura un sistema de seguretat que no es basa en els nivells de seguretat bàsic, mitjà i alt, previstos al RLOPD 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 i art. 24 RGPD).

El RGPD configura la protecció de dades des del disseny i per defecte (art. 25 RGPD), de manera que, als efectes que interessen, quan el responsable dissenya i planifica una auditoria a partir d'una selecció prèvia (mostreig aleatori) de sistemes d'informació, d'instal·lacions, etc, hauria de tenir en compte quin és el risc que pot comportar excloure determinats sistemes d'informació o determinades seus físiques d'aquesta auditoria.

En el cas plantejat, i seguint amb els exemples esmentats, probablement no suposaria el mateix risc excloure d'una auditoria una seu del Centre que dugui a terme el tractament principal –qualitativa o quantitativament- d'informació, que excloure una seu que fa un tractament d'informació menys rellevant, en els termes apuntats. En la mateixa línia, en la planificació d'auditories que utilitzen el mètode de mostreig aleatori, assegurar-se que, transcorregut un període determinat de temps, cap seu física del Centre haurà quedat sense auditar, resultaria una mesura adequada per mitigar possibles riscos, en els termes del RGPD.

Per tot l'exposat, atesa la informació disponible, no es pot descartar que l'elecció del mètode d'auditoria consistent en un mostreig aleatori de les seus físiques del Centre s'ajusti a les exigències de la normativa de protecció de dades (art. 96 RLOPD).

Ara bé, la validesa d'aquest mètode d'auditoria en relació amb els sistemes d'informació del Centre, dependrà de les característiques concretes dels dits sistemes d'informació i, en definitiva, del tractament d'informació que du a terme el Centre, tenint en compte la valoració de riscos esmentada, en els termes del RGPD, qüestions que haurien d'estar previstes i concretades en el corresponent programa d'auditoria.

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

Conclusions

Amb caràcter general, no es pot descartar que l'elecció del mètode d'auditoria consistent en un mostreig aleatori de diferents seus físiques d'un únic responsable (art. 3.d) LOPD) s'ajusti a les exigències de la normativa de protecció de dades (art. 96 RLOPD), en relació amb sistemes d'informació que presentin unes característiques substancialment homogènies.

La validesa del dit mètode d'auditoria en relació amb els sistemes d'informació del Centre, dependrà de les característiques concretes dels dits sistemes d'informació i, en definitiva, del tractament d'informació que du a terme el Centre, tenint en compte la valoració de riscos, en els termes del RGPD, qüestions que haurien d'estar previstes i concretades en el corresponent programa d'auditoria.

Barcelona, 15 de setembre de 2017