CNS-34/2011

Dictamen en relació amb la consulta formulada per una entitat privada sobre el termini durant el qual s'ha de conservar la documentació relativa a les auditories realitzades

Es presenta davant l'Autoritat Catalana de Protecció de Dades un escrit emès per una entitat privada, en què se sol·licita el parer de l'Autoritat sobre el termini durant el qual han de conservar la documentació relativa a les auditories de protecció de dades personals que hagin realitzat.

Analitzada la consulta, i vist l'informe de l'Assessoria Jurídica, es dictamina el següent:

I

(...)

II

El dictamen CNS 12/2010, a què fa referència l'entitat consultant en el seu escrit de consulta, va ser emès per aquesta Autoritat en resposta a una consulta plantejada en relació amb el termini en què les entitats, incloses dins l'àmbit d'actuació de l'Autoritat, resten obligades a conservar la documentació relativa a les auditories de seguretat.

Tal i com es deixava palès en aquell dictamen, ni l'article 96 del Reglament de desplegament de la Llei orgànica de protecció de dades (RLOPD), aprovat pel Reial decret 1720/2007, de 21 de desembre, relatiu a l'auditoria de verificació del compliment de les mesures de seguretat a implantar en relació amb el tractament de determinades dades personals, ni cap altra disposició vigent en matèria de protecció de dades, estableix de forma expressa el termini de conservació de la documentació que integra l'auditoria, per la qual cosa la seva determinació s'ha de realitzar a partir de l'anàlisi de les obligacions que aquesta normativa imposa al responsable del fitxer i, en especial, del règim de responsabilitats que li pot resultar aplicable.

Aquest anàlisi es recull en l'apartat II del dictamen CNS 12/2010, que reproduïm a continuació:

> *"Un primer criteri obvi, però vàlid com a punt de partida, pot ser que en la mesura que un informe d'auditoria no és un document aïllat sinó que forma part d'un procés continuat d'implantació i avaluació de mesures de seguretat, s'haurà de conservar, com a mínim, fins que no existeixi un ulterior informe d'auditoria, amb independència de que hagi passat el termini de 2 anys des que va ser redactat. Ara bé, com veurem a continuació, l'existència d'un informe d'auditoria posterior, ja sigui l'auditoria bianual o per modificació substancial del sistema d'informació, no implica sense més que hagi cessat l'obligació de conservar l'auditoria anterior.*
>
> *Al marge del que direm a continuació, des d'un punt de vista estricte d'auditoria, resulta coherent mantenir tota la documentació de l'auditoria mentre es mantingui un determinat sistema d'informació. Disposar d'aquesta documentació pot aportar informació valuosa a processos d'auditoria posteriors per tal de seguir l'evolució de mesures de seguretat aplicades. I encara resulta més recomanable, quan es tracta d'àmbits, com el sanitari, en que l'ordenament vigent obliga a la conservació de determinada informació, en concret la informació que forma part de la història clínica durant períodes molt llargs de temps.*

Però més enllà d'això, a l'hora de determinar el termini de conservació cal atenir-se al règim de responsabilitats establert a la LOPD i a la resta de l'ordenament jurídic. És en aquest sentit que l'apartat tercer de l'article 96 requereix que la documentació que forma part de l'auditoria estigui a disposició de l'autoritat de control. I no només com a mitjà que permeti aportar informació sobre determinats incompliments, sinó també des del punt de vista de l'entitat responsable del fitxer, com a mitjà per acreditar el compliment de la normativa vigent.

Des del punt de vista del règim sancionador previst a la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), l'obligació de dur a terme les auditories és una mesura de seguretat i per tant la manca de la seva realització pot ser sancionada com a falta greu, a tenor del que disposa l'article 44.3.h de la LOPD. D'acord amb l'article 47.1 de la mateixa LOPD el termini de prescripció per a les infraccions greus és de dos anys. Termini de dos anys que caldria comptar des de la data en que es realitza l'auditoria. Per tant aquest seria un primer termini a tenir en compte des del punt de vista de les responsabilitats. Ara bé, no es pot descartar que l'auditoria, igual que ho pot ser, per altres motius, el registre d'incidències, pot ser un valuós element probatori en la investigació d'altres tipus d'infraccions que tenen atribuït un termini de prescripció més llarg, com és el cas de la infracció molt greu prevista l'article 44.4.f) de la LOPD, que tindria un termini de prescripció de tres anys.

Cal fer però un aclariment, perquè el termini de conservació, en aquests casos no abastaria només el termini de prescripció, sinó també el termini necessari per a la conclusió dels procediments sancionadors que s'hagin pogut incoar abans que transcorri aquest termini.

Però el règim de responsabilitats previst a la LOPD no s'esgota amb el règim sancionador, sinó que l'article 19 de la LOPD preveu també la responsabilitat pels danys o lesions que les persones afectades pateixin en els seus béns o drets, ja sigui mitjançant la reclamació de la responsabilitat de l'administració, quan el dany sigui imputable a una administració pública, o mitjançant el sistema de responsabilitat extracontractual previst al dret civil. En aquest sentit, disposar de la documentació relativa a les auditories pot ser un element probatori important per a l'acreditació de la diligència del responsable en el compliment de les mesures de seguretat exigibles. Al respecte cal recordar que la lletra d) de l'article 121-21 del Llibre primer del Codi civil de Catalunya estableix que prescriuen al cap de tres anys les pretensions derivades de responsabilitat extracontractual i la resta de pretensions al cap de 10 anys, llevat de la recuperació de la possessió (arts. 121-20 i 121-22)".

Per tot plegat es va concloure, tal i com apunta l'entitat consultant en el seu escrit, que *"la documentació que forma part de les auditories de seguretat requerides per aquesta normativa, ha de conservar-se per un període mínim de tres anys, o bé fins que es realitzi l'auditoria de seguretat següent si aquesta no s'ha realitzat dins el termini de dos anys exigible"*.

A això hauríem d'afegir que, arran la modificació de la LOPD introduïda per la Llei 2/2011, de 4 de març, d'economia sostenible, la conservació de la documentació relativa a l'auditoria externa per part de l'entitat responsable del fitxer pot adquirir especial rellevança a l'hora de graduar la sanció, pel que fa a la circumstància prevista a la lletra i) de l'article 45.4 LOPD, això és, "*l'acreditació que abans dels fets constitutius d'infracció l'entitat imputada tenia implantats procediments adequats d'actuació en la recollida i el tractament de les dades de caràcter personal, i que la infracció és conseqüència d'una anomalia en el funcionament d'aquests procediments no deguda a una falta de diligència exigible a l'infractor.*".

D'altra banda, també es va considerar, en aquell dictamen, que *"la conservació d'aquesta documentació pot resultar convenient per un termini més ampli als efectes de disposar d'una informació completa que permeti avaluar l'evolució de les mesures de seguretat aplicades, i també als efectes de disposar d'elements probatoris del compliment de la normativa vigent en matèria de protecció de dades, mentre no hagi prescrit les responsabilitats pels danys que s'hagi pogut ocasionar amb el tractament de dades".*

III

Sens perjudici de les consideracions anteriors, cal tenir en compte que el criteri sostingut en el dictamen CNS 12/2010, i reproduït en l'apartat anterior d'aquest dictamen, s'estableix sempre en relació amb la figura del responsable del fitxer o tractament (article 3.d) de la LOPD), atès que és sobre aquest que recau l'obligació de realitzar, sempre que siguin d'aplicació com a mínim les mesures de seguretat de nivell mitjà, una auditoria de seguretat interna o externa biennal o bé una d'extraordinària (quan es facin modificacions substancials del sistema d'informació que puguin repercutir en les mesures de seguretat implantades), així com el deure de mantenir aquesta documentació sempre a disposició de l'autoritat de control (articles 79 i 96 del RLOPD).

És en aquest sentit que la conservació de la documentació que forma part de l'auditoria es configura com element indispensable perquè el responsable del fitxer o tractament pugui acreditar el compliment de la normativa vigent en matèria de protecció de dades davant les autoritats de control de protecció de dades.

En aquest cas però, la consulta adreçada a l'Autoritat es planteja en relació amb el termini durant el qual l'auditor extern, i no així el responsable, ha de conservar la documentació de l'auditoria que aquest hagi realitzat.

En concret, l'entitat consultant planteja si el criteri aplicable en aquest cas és o no el mateix que el defensat en el dictamen citat, això és, la conservació de la documentació durant un període mínim de 3 anys o fins que es realitzi l'auditoria de seguretat següent en cas de no haver-se realitzat dins el termini de 2 anys exigible.

En aquest sentit, cal posar de manifest que quan es tracta d'auditories realitzades per entitats externes a la pròpia organització auditada l'obligació de conservació a què es fa referència continua recaient en el responsable del fitxer o tractament que ha encarregat la seva realització.

És a dir, en el cas que el responsable decideixi realitzar l'auditoria de seguretat mitjançant un auditor extern, aquest, un cop finalitzats els treballs encomanats, haurà de retornar la documentació de l'auditoria al responsable, segons allò establert en l'acord inicial signat en el marc de la seva relació contractual.

Com s'ha apuntat abans, el responsable del fitxer o tractament és qui ha de vetllar per conservar aquesta documentació, atès que podria ser-li requerida per l'Autoritat de control per tal de comprovar el compliment de les obligacions establertes a la normativa vigent de protecció de dades (article 96.3 del RLOPD).

Ara bé, és possible que l'auditor extern consideri necessari conservar aquesta documentació tot i que des de la vessant de la protecció de dades no hi estigui obligat. En el cas que sigui així, haurà de tenir en compte que, en la mesura que en aquesta documentació constin dades personals, la seva conservació no resultaria justificada

(article 4.5 LOPD), tret que les dades es mantinguin bloquejades per tal d'atendre les possibles responsabilitats derivades del seu tractament, durant el termini en què aquestes responsabilitats no hagin prescrit (article 22.2 RLOPD), o bé que sigui necessària per a la realització d'un nou encàrrec per compte de l'entitat auditada.

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

Conclusions

D'acord amb la normativa vigent en matèria de protecció de dades personals, en el cas que l'auditoria de seguretat es dugui a terme per una entitat externa a l'entitat auditada, aquesta no està obligada a conservar la documentació de l'auditoria més enllà del seu lliurament al responsable del fitxer o tractament.

Barcelona, 21 d'octubre de 2011