RESOLUCIÓ del procediment sancionador núm. 5/2008 referent a la Secretaria de Relacions amb l'Administració de Justícia del Departament de Justícia de la Generalitat de Catalunya.

Antecedents

Primer.- El dia 18/06/2007 va tenir entrada a l'Agència Catalana de Protecció de Dades l'escrit del director de l'*Agencia Española de Protección de Datos* mitjançant el qual donava trasllat de la denúncia formulada per la Policia Local d'Ourense, que informava del resultat d'unes investigacions realitzades a la xarxa punt a punt d'Internet a la qual s'accedia amb els programes d'intercanvi d'arxius EMULE i LPHANT, i que havien portat a detectar un presumpte incompliment de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant LOPD).

La denúncia es concretava en que el dia 11/03/2007 es va detectar que s'havien difós a través d'Internet una sèrie d'arxius aparentment relacionats amb l'Institut de Medicina Legal de Catalunya (en endavant, IMELEC) que contenien dades de caràcter personal relatives a funcionaris o personal de la Generalitat de Catalunya i a persones que havien rebut algun dels serveis que presta aquest organisme. Juntament amb la denúncia es varen trametre electrònicament els arxius trobats a Internet, així com impressions de pantalla de l'EMULE i LPHANT en les quals apareixien els fitxers d'aquests arxius.

Segon.- L'Agència va obrir una fase d'informació prèvia (núm. 45/2007) d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment d'aplicació als àmbits de competència de la Generalitat, en relació amb l'article 17 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades, per tal de comprovar la realitat dels fets denunciats, i a fi d'obtenir més informació sobre les circumstàncies dels fets i els subjectes responsables.

En el si d'aquesta fase d'investigació, l'Àrea d'Inspecció de l'Agència va realitzar les actuacions següents:

1. El dia 18/07/2007 va sol·licitar al coordinador d'Auditoria i Seguretat de la Informació de l'Agència un informe sobre aspectes tècnics relacionats amb els fets objecte de denúncia, que va ser lliurat el dia 9/10/2007.

2. El dia 11/02/2008 el personal de l'Agència va realitzar una inspecció a la seu de l'IMELEC.

3. El dia 15/02/2008 va rebre en declaració al sr. XXX, qui presta serveis a l'IMELEC, en règim de personal laboral.

4. El dia 18/02/2008 es va requerir a la Secretaria de Relacions amb l'Administració de Justícia del Departament de Justícia per tal que informés sobre una sèrie d'extrems relacionats amb els fitxers de l'IMELEC, i trametés una còpia del document de seguretat relatiu als fitxers o tractaments de dades relacionats amb els informes de malapraxis mèdica, autòpsies i control de sales i tècnics. La Secretaria va complimentar aquest requeriment el dia 5/03/2008.

C. Llacuna, 166, 7a planta
08018 Barcelona
Tel. 93 552 78 00
Fax 93 552 78 30

5. A l'últim, el dia 13/03/2008 es va demanar al Coordinador d'Auditoria i Seguretat de la Informació de l'Agència un informe sobre el document de seguretat aportat per la Secretaria de Relacions amb l'Administració de Justícia, que va ser elaborat i lliurat el mateix dia.

Tercer.- En data 9/05/08, la directora de l'Agència Catalana de Protecció de Dades va acordar iniciar procediment sancionador per una presumpta infracció lleu de l'article 44.2.e) i una presumpta infracció molt greu prevista a l'article 44.4.g) de la LOPD, ambdues relacionades amb el deure de secret previst a l'article 10 de la mateixa LOPD; una infracció greu prevista a l'article 44.3.h) de la LOPD en relació amb l'article 9 de la LOPD i les obligacions derivades de l'aplicació del Reial decret 994/1999, d'11 de juny, pel qual s'aprova el Reglament de seguretat dels fitxers automatitzats que continguin dades de caràcter personal; i una altra infracció greu prevista a l'article 44.3.a) de la LOPD en relació amb l'article 20 de la LOPD, sens perjudici de les que es poguessin determinar durant la instrucció del present procediment sancionador.

Així mateix, va nomenar instructora de l'expedient a la funcionària de l'Agència Catalana de Protecció de Dades, XXX. Aquesta resolució es va notificar a la Secretaria de Relacions amb la Justícia juntament amb el plec de càrrecs, i a la Policia Local d'Ourense,.

Cinquè.- La Secretaria de Relacions amb la Justícia va formular al·legacions a l'Acord d'Inici i al plec de càrrecs, que van tenir entrada al registre de l'Agència el dia 3/06/08. Aquestes al·legacions s'analitzen a l'apartat segon dels Fonaments de Dret d'aquesta proposta de resolució.

Sisè.- El dia 18/09/2008 es va formular la proposta de resolució corresponent per part de la instructora d'aquest expedient. Aquesta proposta va ser notificada a Secretaria de Relacions amb la Justícia, per tal que en el termini de 10 dies poguessin presentar les al·legacions que consideressin adients.

El dia 8/10/2008 va tenir entrada l'escrit d'al·legacions formulat per la Secretaria de Relacions amb l'Administració de Justícia, les quals es resolen de forma motivada en l'apartat de Fonaments de Dret d'aquesta resolució.

Fets Provats

Primer.- El dia 11/03/2007, la Policia Local d'Ourense va enviar a l'*Agencia Española de Protección de Datos* un escrit pel qual posava en coneixement d'aquesta entitat que amb motiu d'unes investigacions realitzades a Internet, va detectar que en una xarxa pública punt a punt ("*peer to peer" o* "P2P" EDONKEY/EMULE), hi havia dos usuaris, que operaven sota els pseudònims de (...)", que tenien a disposició de la resta d'usuaris de la xarxa arxius que contenien dades de caràcter personal.

En concret, l'usuari identificat com a "*(...)*" compartia a Internet mitjançant el programari de connexió a la xarxa P2P (d'intercanvi d'arxius) "*LPHANT*", dos arxius d'extensió "*.mdb*" (base de dades de Microsoft Access), anomenats "*Control_Salas_y_Tecnicos_Access2003.mdb*" i "*Malpraxis20041210 Access 2000.mdb*". Una vegada analitzat el contingut d'aquests arxius, la policia local va detectar que contenien dades de caràcter personal de 183 metges forenses i 50 tècnics de jutjats de Catalunya. La policia local d'Ourense va identificar l'adreça IP d'aquest usuari (IP xxxx a les 9:58 hores del dia 11/03/2007).

Així mateix, l'usuari identificat com a "*(...)*" compartia a Internet un arxiu mitjançant el programari de connexió a la xarxa P2P (d'intercanvi d'arxius) "*EMULE*", d'extensió ".*mdb*" (base de dades de MICROSOFT ACCESS), anomenat "*Llibre Registre Autopsies.mdb*". La policia local d'Ourense va identificar l'adreça IP d'aquest usuari (IP xxxx).

Els programes "*EMULE*" i "*LPHANT*" s'utilitzen a Internet amb la finalitat de compartir fitxers o arxius entre els ordinadors que es troben connectats a la xarxa P2P. Qualsevol persona que tingui instal·lat algun d'aquests programes té accés als arxius que la resta d'usuaris tenen per compartir dins la xarxa.

La Policia Local d'Ourense va trametre electrònicament juntament amb la denúncia, els arxius als quals es fa referència, tot i que hi havia més arxius de nomenclatura similar que es trobaven en aquesta xarxa P2P d'Internet, segons s'acredita de les captures de pantalla referides a l'usuari "*(...)*". Així mateix, també va trametre còpia d'algunes de les extraccions de dades realitzades d'aquests fitxers, en les quals apareixien dades personals de metges forenses i d'altres persones, relacionades amb el fitxer de malpraxis. En les captures de pantalla aportades també consten les adreces IP dels usuaris "*(...)*".

L'*Agencia Española de Protección de Datos* va trametre aquesta denúncia amb els arxius esmentats a l'Agència Catalana de Protecció de Dades el dia 5/06/2007, atès que constaven com a titulars dels fitxers el Departament de Justícia i la Generalitat de Catalunya.

Segon.- Una vegada es va rebre la denúncia amb la documentació i arxius esmentats, es van realitzar comprovacions sobre l'existència de dades personals als arxius, una vegada oberts amb el programari MS ACCESS.

1. Es va comprovar que la base de dades anomenada "*Control_Salas_y_Tecnicos_Access2003.mdb*", presenta un llistat de Taules, algunes de les quals contenen dades personals:

"Contactos"
"dbo_Forenses"
"dbo_Incidencias_Salas"
"dbo_Sala_autopsies"
"dbo_Sala_autopsies Copia"
"Incidencias Tecnicos"
"Incidencias Tecnicos Copia"
"Llamadas"
"Salas dautopsies"
"TECNICS"
"TECNICS Copia"

Només per citar alguns exemples respecte les dades personals que conté aquesta base de dades, s'ha constatat que:

a) La Taula "*TECNICS*" conté 50 registres amb dades del personal de l'Institut de Medicina Legal de Catalunya (en endavant, IMELEC). Aquestes dades fan referència a nom i cognoms, data de naixement, DNI, adreça personal i professional i telèfons personals i professionals.

b) La taula "*dbo_Forenses*" conté 50 registres corresponents a metges forenses i altres càrrecs de l'IMELEC, amb dades relatives a nom i cognoms del metge forense, adreça particular, adreça professional, telèfon, destí, cos, login i password, entre altres.

c) La taula de "*Contactos*" té 2 registres de personal de l'IMELEC, on consten complimentats camps amb dades personals tals com: nom i cognoms, entitat, adreça, telèfon del domicili i del lloc de treball, correu electrònic i número d'identificació del tècnic.

d) La taula "*Incidencias técnicos*" té 129 registres, que contenen dades personals com ara el número d'identificació del tècnic (que es pot relacionar amb la persona física a través de la Taula "*TECNICS*"), incidències (vacances, baixa, permís...), persona que el substitueix, etc..

2. La base de dades anomenada "*Llibre Registre Autopsies.mdb*", presenta un llistat de Taules, algunes de les quals contenen dades personals:

"Gavà"
"Rubí"
"Sardañola"
"T_S_Feliu"

Aquestes taules, contenen 169 registres, i recullen dades relacionades amb persones difuntes i les dades personals (nom i cognoms) dels metges forenses i tècnics que han intervingut en les autòpsies.

3. La base de dades anomenada "*Malpraxis20041210 Access 2000.mdb*", presenta un formulari mitjançant el qual es poden visualitzar 148 registres amb dades personals tals com: nom del pacient –suposadament-, jutjat i diligències penals, nom i cognoms del metge forense, resultat de l'informe i especialitat mèdica, entre altres

4. Així mateix, es va procedir a obrir les bases de dades amb el programari UltraEdit destinat a visualitzar les dades en format ASCII i Hexadecimal amb la finalitat de trobar indicis dins d'aquests arxius que permetessin trobar l'origen d'aquests fitxers, mitjançant rutes o dispositius utilitzats.

Mitjançant l'anàlisi de la base de dades "*Control_Salas_y_Tecnicos_Access2003.mdb"* es va trobar la ruta "*D:\Trabajo\YYY\Access\A\Flechas\Arrow10Cx.IC",* en la que destaca el nom "YYY"; i la ruta "*f:\Mis documentos\Delia Software\Iconos\Castellano.ICO*", en la que destaca "*Delia Software*". De l'anàlisi hexadecimal de "*Llibre Registre autopsies.mdb*" es va trobar la ruta "*C:\Llibre Registre AF:\Trabajo\Collserola\Llibre Registre Autopsies\NECROS.XLS",* on apareix la referència a la localitat de "*Collserola*".

5. El dia 11/02/2008 es va realitzar un acte d'inspecció a la seu de l'IMELEC en el si del qual es va constatar que els informes d'autòpsies es gestionen mitjançant un fitxer que està fet en el programari MSACCESS, on existeix un Llibre registre d'autòpsies amb camps de dades del cadàver, del metge forense, procediment judicial, etc.

El fitxer d'autòpsies de Barcelona està ubicat a un servidor de fitxers al Servei de Patologia que es troba al carrer Villarroel al recinte de l'Hospital Clínic-Facultat de Medicina o bé a la Clínica Forense, connectat a la xarxa judicial. Es pot accedir a aquesta informació a través d'altres edificis de la xarxa judicial, els accessos a aquesta informació depenen dels perfils d'usuari d'accés a la xarxa.

Els serveis fora de Barcelona estan en un fitxer Excel (Collserola i L'Hospitalet), mentre que la resta de serveis gestiona aquesta informació en suport paper.

Els informes de malpraxis es gestionen mitjançant una base de dades creada en MSACCESS. Recull la informació dels informes fets pels metges forenses a Barcelona ciutat i els que són de fora, una vegada arriba l'informe a l'IMELEC, s'introdueix aquesta informació a la base de dades. Només a Barcelona ciutat s'enregistren les dades bàsiques de cada informe.

Les dades derivades dels informes de malpraxis que es fan des de la Clínica Médico Forense de Barcelona s'introdueixen a la base de dades que es troba a un servidor ubicat a la Clínica, i segueix el mateix esquema d'accessibilitat que el fitxer d'autòpsies.

Per al control de sales els responsables de l'IMELEC van manifestar que podia ser que existís un full d'Excel d'ús intern, amb les dades dels forenses i de localització del personal de guàrdia. A Collserola s'han centralitzat partits judicials i el mateix ha succeït amb altres serveis.

Els coordinadors de tècnics fan un calendari anual amb els dies que treballen a l'any, els torns de vacances, els telèfons de contacte, etc. La gestió es fa de forma individual per a cada servei, es tracta d'un fitxer de gestió, en els casos en què existeix, doncs hi ha serveis que potser no en tenen. No es va poder concretar com es porta a terme el control d'accés a aquests fitxers perquè depèn de com s'organitza cada servei. En tot cas, l'accés a aquesta informació es fa des d'edificis connectats a la xarxa judicial i per persones degudament autoritzades.

El control d'accés en el cas de Llibre d'autòpsies i de malpraxis es realitza mitjançant un usuari i contrasenya afegit al d'accés a la xarxa. És tracta d'un usuari específic per accedir a la base de dades d'ACCESS, en principi, només hi podria accedir el cap de Servei de Clínica i Patologia Forense i l'administratiu que dóna suport a cada servei.

L'Àrea de Tecnologies de la Informació i Comunicacions del Departament de Justícia gestiona tota la informació de l'IMELEC des de l'any 2004 aproximadament. La referència que es feia en una de les rutes trobades a "*Delia Software*" obeeix al fet que un metge forense que presta serveis a l'IMELEC, el Dr. ZZZ, dóna suport puntual de tipus informàtic, i alhora és el responsable de l'empresa Delia Software.

El Dr. ZZZ va manifestar durant l'acte d'inspecció que en un servidor del Servei de Patologia de l'IMELEC que es troba ubicat a l'Hospital Clínic té un directori amb el nom Delia Software, que és el nom que ha utilitzat per desenvolupar alguns programes ja siguin per ús propi o per coneguts, i també l'utilitza a l'hora d'instal·lar i configurar alguns equips. Aquesta empresa no ha tingut relació contractual o comercial amb l'IMELEC, ja que els programes que ha desenvolupat el Dr. ZZZ ho ha fet a títol gratuït, en el marc de la relació de servei que manté amb l'IMELEC, en la seva qualitat de metge forense adscrit a aquest organisme.

El Dr. ZZZ s'encarrega de la coordinació de qüestions informàtiques de l'IMELEC, i d'aquest amb el Gabinet Tècnic del Departament de Justícia. Fa anys va desenvolupar per a l'IMELEC un programa informàtic de gestió de les bases de dades d'autòpsies.

En el registre d'incidències relacionades amb els sistemes d'informació no tenen registrat cap incident de seguretat a partir de l'any 2004 relacionat amb alguna pèrdua d'informació o accessos no autoritzats.

No existeix cap relació formal entre el Sr. YYY, que era el nom que apareixia a una de les rutes trobades mitjançant l'examen dels fitxers, i l'IMELEC, ni consta que aquesta persona formi part del personal de la Generalitat de Catalunya, si bé es va esbrinar que aquesta persona és un conegut d'un dels treballadors de l'IMELEC, el senyor XXX, tal com s'exposa més endavant.

Les funcions del responsable de seguretat recauen sobre el Cap del Gabinet Tècnic del Departament de Justícia. El document de seguretat general del Departament de Justícia inclou els tractament de dades de caràcter personal que tracta l'IMELEC.

Tercer.- Les actuacions realitzades denoten que no s'han implementat mesures de seguretat adequades dirigides a protegir les dades objecte de tractament i evitar-ne accessos no autoritzats, tota vegada que els fitxers esmentats han aparegut a una xarxa P2P d'Internet, on resultaven accessibles per a qualsevol usuari de la xarxa. No consta que s'hagin adoptat mesures concretes respecte de la sortida de suports amb informació, ni que s'enregistrin aquestes sortides, ni que es compleixin les previsions del document de seguretat del Departament de Justícia pel què fa a la seguretat física i lògica. És més, la manca de control sobre el compliment de les mesures de seguretat, juntament amb l'organització operativa del personal de l'IMELEC per accedir als fitxers amb dades personals, afavoreix situacions de risc pel que fa a la seguretat de les dades. Tampoc consta que s'hagin donat instruccions concretes al personal sobre el tractament de les dades de caràcter personal i les precaucions que s'han d'adoptar a l'hora de treure suports amb informació de caràcter personal fora de les dependències de l'IMELEC, ja siguin de la seva seu central o d'altres dependències.

Tampoc consta que el responsable del fitxer hagi realitzat les auditories de caràcter bianual que preveu la LOPD i les normes que la desenvolupen, respecte del fitxer que consta declarat de l'Institut de Medicina Legal de Catalunya "*Arxiu d'informes mèdics de l'Institut de Medicina Legal de Catalunya".*

Quart.- Respecte dels fitxers que es van trobar a Internet, escau assenyalar que el fitxer de malpraxis consta declarat com a "*Arxiu d'informes mèdics de l'Institut de Medicina Legal de Catalunya"*, que donaria cobertura a tots els informes forenses que es realitzen, segons l'Ordre JUS/86/2007, de 10 d'abril, per la qual es regulen els fitxers que contenen dades de caràcter personal gestionats pel Departament de Justícia. El fitxer d'autòpsies no consta declarat, tot i que recull les dades identificatives dels metges forenses que les practiquen, amb la qual cosa quedarien subjectes a la LOPD.

Finalment, pel que fa al fitxer de "*Control de Sales i Tècnics*", durant l'acte d'inspecció es va manifestar que "*per la informació que conté, es considera inclòs dins el fitxer de GIP-SIP del Departament de Governació i Administracions Públiques*."

El fitxer conegut com a GIP-SIP es correspon amb el fitxer "Gestió Integrada de Personal", creat mitjançant l'Ordre GRI/371/2003, de 18 d'agost, per la qual es regulen els fitxers que contenen dades de caràcter personal gestionats pel Departament de Governació i Relacions Institucionals. Aquest fitxer té com a finalitat gestionar les dades personals, econòmiques i laborals de tot el personal que presta els seus serveis a la Generalitat.

El fitxer "*Control de Sales i Tècnics"* és un fitxer de titularitat de l'IMELEC, amb una finalitat organitzativa tan del personal de l'IMELEC com de les sales on es desenvolupen les funcions del personal, per tal de garantir la seva disponibilitat i localització en tot moment. Així es recullen dades relatives a la identificació d'aquest personal, els telèfons de contacte (professionals, personals, de l'IMELEC), incidències relacionades amb la prestació del servei, substitucions, persones de contacte dels diferents tanatoris de Catalunya, etc.

Cinquè.- Durant l'acte d'inspecció es van obrir els tres fitxers i es va mostrar el seu contingut als representants de l'entitat inspeccionada, els quals van manifestar que reconeixien la informació com a pròpia, és a dir, com la informació que tracta l'IMELEC. Però van realitzar uns aclariments:

a) Del fitxer control de sales i tècnics, tot i que es reconeixien les dades com a reals així com la informació continguda al fitxer, no es reconeixia el format en què es presentava la informació.

b) Del fitxer que gestiona els informes de malpraxis, es reconeixien les dades com a reals, algunes d'històriques i també el format en què es mostrava la informació. Aquesta informació és la que gestionen els serveis de l'IMELEC.

c) Del fitxer Llibre registre d'autòpsies tampoc no es reconeixia el format com es presentava la informació, i en relació amb els camps d'informació, van manifestar que aproximadament coincidien amb els que gestionaven en aquell moment. El conjunt de taules del Llibre registre d'autòpsies sí que el reconeixen com una estructura de fitxers utilitzada per a les autòpsies realitzades al Tanatori de L'Hospitalet.

Respecte l'alias "*(...)*" tant el Dr. ZZZ com el gerent de l'IMELEC el van relacionar, per la coincidència amb el nom de l'adreça personal de correu electrònic, amb el Sr. XXX, tècnic d'autòpsies i coordinador d'altres tècnics, que treballa a l'IMELEC, habitualment a la seu central de l'IMELEC, així com a la seu de Collserola i a altres dependències. Abans de ser coordinador, fins fa uns dos anys aproximadament, havia estat tècnic a L'Hospitalet de Llobregat. El Sr. XXX comparteix l'ordinador amb la Sra. AAA, que és una tècnica que treballa a la seu central de l'IMELEC i l'única que té accés a la base de dades de malpraxis. Durant l'acte d'inspecció es va verificar que des d'aquesta estació de treball es podia accedir a uns fitxers en format ACCESS que tenien la mateixa informació que el fitxer de malpraxis trobat a la xarxa P2P d'Internet.

Sisè.- El dia 15/02/2008 es va rebre en declaració al Sr. XXX, que presta serveis a la Generalitat com a personal laboral des de l'any 1992 aproximadament. Les seves funcions actualment consisteixen en la coordinació de tots els tècnics forenses de Catalunya i també és el responsable del Servei de Patologia Forense de la zona nord (Collserola) pel què fa a les necessitats internes del servei. Escau assenyalar que una de les rutes trobades en els arxius feia referència a Collserola.

El Sr. XXX va declarar que els fitxers "*autòpsies*", "*control de sales i tècnics*" i "*malpraxis*" els ha fet ell. Els dos primers els va fer ell exclusivament, mentre que el de "*malpraxis*" el va iniciar el Dr. ZZZ, i posteriorment el Sr. XXX va continuar el projecte. Actualment continua fent el manteniment i millora d'aquests tres fitxers.

El Sr. YYY és amic personal del Sr. XXX. En una ocasió, el senyor YYY li va demanar ajuda per desenvolupar una base de dades per gestionar les visites a metges que volia utilitzar per a ús personal, aquesta base de dades la va desenvolupar en ACCESS. A l'ordinador que utilitza a l'IMELEC té un directori amb carpetes personals entre les quals es troba una carpeta anomenada "*YYY*". En aquest ordinador té instal·lats els tres fitxers esmentats anteriorment. També té una còpia dels fitxers de l'IMELEC, per poder treballar tan des del seu ordinador personal portàtil com des de l'ordinador fix que té a casa seva. El motiu de tenir còpia d'aquests arxius és per gestionar des de casa seva les incidències que es produeixen a la feina.

El Sr. XXX utilitza l'àlies "*(...)*" per connectar-se a la xarxa pública P2P en la que es van trobar els fitxers, mitjançant els programes EMULE i LPHANT, des de l'ordinador fix que té a casa seva. Per a la connexió a Internet fins fa un any i mig utilitzava MENTA com a proveïdor de serveis d'Internet (ISP) i després ONO quan va canviar de nom. En algun cas va detectar l'existència d'intrusos que volien entrar al seu ordinador, fet que va posar en coneixement de l'ISP per solucionar el problema.

Pel personal de l'Àrea d'Inspecció es van fer comprovacions respecte del número d'IP utilitzat per l'usuari "*(...)*" (núm. xxxx) i es va constatar que era de MENTA-CABLEMODEMS, connexió que avui en dia correspon a ONO.

El Sr. XXX també va informar que als ordinadors de casa seva, tan el fix com el portàtil, tenen una carpeta que s'anomena TRABAJO, dins de la qual es troba una carpeta anomenada IMELEC, i una altra YYY, entre altres. També va reconèixer la ruta "*D:\Trabajo\PYYY\Access\A\Flechas\ARROW10Cx.IC*", que és una de les trobades en l'anàlisi hexadecimal dels fitxers.

Setè.- El Departament de Justícia té un protocol específic que disposa que per raons de seguretat els usuaris no es poden instal·lar programes Peer to Peer. Ni el Sr. XXX ni el Dr. ZZZ van poder donar cap explicació al fet que aquests tres arxius apareguessin a una xarxa Peer to Peer, però es va constatar que l'usuari utilitzat pel Sr. XXX per connectar-se a la xarxa punt a punt d'Internet mitjançant el programa "*LPHANT*" és "*(...)*", que és el mateix usuari que compartia a Internet els dos arxius d'extensió "*.mdb*" (base de dades de MICROSOFT ACCESS), anomenats "*Control_Salas_y_Tecnicos_Access2003.mdb*" i "*Malpraxis20041210 Access 2000.mdb".* El proveïdor d'accés a Internet que utilitza el Sr. XXX és el mateix que va utilitzar "*(...)*" quan es van detectar els arxiu.

Vuitè.- L'IMELEC és un organisme tècnic al servei de l'Administració de justícia, adscrit al Departament de Justícia i que depèn de la Secretaria de Relacions amb l'Administració Justícia, d'acord amb el que preveu el Decret 12/2007, de 16 de gener, reestructuració del Departament de Justícia. El responsable de seguretat dels fitxers que gestiona l'IMELEC és el Gabinet Tècnic de la Secretaria General de Justícia segons consta al Document de Seguretat del Departament de Justícia.

Novè.- Segons l'Ordre JUS/86/2007, de 10 d'abril, per la qual es regulen els fitxers que contenen dades de caràcter personal gestionats pel Departament de Justícia, la Secretaria de Relacions amb l'Administració de Justícia és la responsable del fitxer anomenat "*Arxiu d'informes mèdics de l'Institut de Medicina Legal de Catalunya*" que té com a finalitat "... *arxivar els informes medicoforenses emesos pels metges de l'Institut de Medicina Legal de Catalunya en el marc d'un procediment judicial*", i les persones afectades o obligades a subministrar les dades són els "*Ciutadans i ciutadanes atesos al Servei de Clínica Medicoforense per ordre judicial".*

No consta publicada cap altre disposició de creació de fitxers relacionada amb els fitxers gestionats o de titularitat de l'IMELEC.

Fonaments de Dret

Primer.- És d'aplicació al present procediment el previst al Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat d'acord amb l'article 17 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades i el Títol VII de la LOPD. Aquesta proposta de resolució es formula de conformitat amb l'article 13 del Decret 278/1993, que atribueix tal facultat a la instructora del procediment. Pel que fa a la competència per dictar la resolució del procediment sancionador, correspon a la directora d'aquesta Agència, d'acord amb l'article 5 de la Llei 5/2002, de 19/04, de l'Agència Catalana de Protecció de Dades, i l'article 15 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades.

Segon.- En el curs del procediment sancionador, i concretament davant la notificació del plec de càrrecs, la Secretaria de relacions amb l'Administració de Justícia va formular al·legacions mitjançant escrit presentat a l'Agència el 03/06/2008. Tot seguit s'aborden aquestes al·legacions, i s'exposen els motius en base als quals no poden reeixir.

A) Al·legació Primera: la Secretaria exposava que en relació amb la falta imputada relativa a la vulneració del deure de secret, s'ha de distingir entre la responsabilitat de l'Administració d'instruir el seu personal en l'ús que ha de fer de la informació, i una altra qüestió és que aquest personal en faci un bon o mal ús. Al respecte, la Secretaria afegia que tot el personal al servei de l'Administració de Justícia que depèn del Departament està informat de les obligacions derivades del tractament de dades personals.

   Respecte aquesta al·legació, en primer lloc, escau assenyalar que certament el document de seguretat del Departament de Justícia conté un apartat 6 anomenat "Funcions, Comunicacions, Obligacions dels Usuaris i Conseqüències del Mal Ús", a banda d'altres obligacions legals que puguin afectar als treballadors públics. Però tot i aquestes previsions, l'aparició dels fitxers de l'IMELEC a Internet i la pròpia organització de l'IMELEC pel que fa als sistemes d'informació i les persones que tracten dades, evidencien que tot i que el Departament de Justícia disposa d'un document de seguretat, les mesures per garantir la seguretat de les dades no s'han implementat de forma efectiva. En aquest cas, la responsabilitat és del responsable del fitxer, doncs a ell li incumbeix garantir la seguretat de les dades, sens perjudici de la responsabilitat en què haguessin pogut incórrer les persones que tracten les dades. Els fets provats acrediten que com a mínim fins el dia 11/03/2007 -data en la que va accedir la policia local d'Ourense als esmentats arxius-, tres fitxers de l'IMELEC que contenien dades personals van estar accessibles a tercers a la xarxa d'Internet. No

consta que s'haguessin implementat les mesures de gestió de suports que preveu el document de seguretat, tampoc no consta que s'hagués informat als usuaris dels sistemes d'informació sobre les obligacions concretes respecte el tractament de les dades. En definitiva, l'existència d'un document de seguretat resulta inútil si no s'implementen les mesures de forma efectiva, i aquesta responsabilitat recau en el responsable del fitxer, i, en el seu cas, en el responsable de seguretat.

Per tant, per les raons exposades i els arguments que es recullen al Fonament de Dret Quart d'aquesta proposta, aquesta al·legació es va desestimar.

B) Al·legació Segona: la Secretaria manifestava que el fitxer d'autòpsies és una tractament que queda inclòs en el fitxer anomenat "Arxiu d'informes mèdics de l'Institut de Medicina Legal de Catalunya" regulat a l'Ordre JUS/86/2007, de 10 d'abril.

Segons l'Ordre JUS/86/2007, de 10 d'abril, per la qual es regulen els fitxers que contenen dades de caràcter personal gestionats pel Departament de Justícia, el fitxer "*Arxiu d'informes mèdics de l'Institut de Medicina Legal de Catalunya*" té com a finalitat "*... arxivar els informes medicoforenses emesos pels metges de l'Institut de Medicina Legal de Catalunya en el marc d'un procediment judicial*", i les persones afectades o obligades a subministrar les dades són els "*Ciutadans i ciutadanes atesos al Servei de Clínica Medicoforense per ordre judicial".* El tipus de dades objecte de tractament són: "*Dades identificatives (DNI/NIF, nom i cognoms i ordre judicial que motiva l'informe),dades de característiques personals (estat civil, dades familiars, lloc i data de naixement, sexe, edat i nacionalitat, característiques físiques i llengua materna), dades de salut (històries clíniques derivades dels informes mèdics), origen racial i vida sexual, d'infraccions penals, dades de circumstàncies socials (allotjament o habitatge, situació militar i aficions i estils de vida), dades acadèmiques i professionals (formació i titulacions, experiència professional i historial acadèmic) i dades d'ocupació laboral (historial laboral).*

La finalitat del fitxer d'autòpsies no té cobertura dins el fitxer d'informes mèdics regulat a l'Ordre JUS/86/2007, tota vegada que aquest últim es refereix al tractament de dades que es realitza a les persones que es visiten a la Clínica Medicoforense, activitat que no coincideix amb les autòpsies que es realitzen als difunts, i aquest tipus de tractament es corresponia el fitxer que es trobava a Internet. A més, el fitxer "Arxiu d'informes mèdics" protegeix les dades dels "*ciutadans i ciutadanes atesos al Servei de Clínica Medicoforense"*, mentre que el fitxer d'autòpsies hauria de tutelar les dades dels metges i altre personal que intervenen en l'autòpsia. Per tant, aquesta al·legació no podia prosperar.

C) Al·legació Tercera: la Secretaria demanava tenir accés als arxius informàtics que han donat lloc a l'inici del present procediment per tal de comprovar si les dades són reals.

Al respecte, s'ha procedit de conformitat amb la petició realitzada, atès que aquesta instructora va trametre una còpia d'aquests fitxers a la Secretaria de Relacions amb l'Administració de Justícia, que va ser entregada a la Secretaria el dia 12/06/08, alhora que va informar que es podia sol·licitar vista de l'expedient quan ho considerés oportú, sens perjudici del tràmit d'audiència que se li concediria prèviament a la resolució.

D) Al·legació Quarta: la Secretaria exposava quina és la situació del Departament de Justícia pel que fa al compliment de les mesures de seguretat que la normativa de protecció de dades

exigeix. Manifestava que va començar a implementar aquestes mesures i a formar el seu personal l'any 2005, que ha realitzat auditories internes per tal d'implementar el nou document de seguretat, que l'any 2007 va procedir a actualitzar els seus fitxers i actualment ha aprovat un nou document de seguretat i es troba en fase de publicació d'una nova ordre de declaració de fitxers. Volia destacar, així, l'esforç realitzar per adequar-se a la normativa de protecció de dades.

Respecte dels fitxers de l'IMELEC, reconeix l'existència de certes mancances pel que fa al compliment de mesures de seguretat organitzatives especificades al document de seguretat, però no succeeix el mateix amb les mesures tècniques o jurídiques. Així mateix, manifesta que en tractar-se d'un dels serveis menys voluminosos del Departament i per tractar-se de ciutadans que es troben en el marc d'un procediment judicial, no ha estat un dels objectius prioritaris d'adequació a la LOPD respecte d'altres unitats o serveis departamentals.

Aquesta al·legació no exonera a la Secretaria de Relacions amb l'Administració de Justícia respecte de les obligacions que té en el tractament de les dades de caràcter personal. La LOPD i el reglament que la desenvolupa estableix l'obligació de garantir la seguretat de les dades des del mateix moment en què aquestes dades són objecte de tractament. Per tant, l'efectivitat d'aquestes garanties, que no es pot oblidar deriven d'obligacions legalment configurades, no es poden veure supeditades a la planificació estratègica dels sistemes d'informació del Departament.

Tercer.- En data 8/10/08 han tingut entrada les al·legacions formulades per la Secretaria de Relacions amb l'Administració de Justícia davant la proposta de resolució formulada per la instructora el 18/09/2008. L'entitat imputada manifesta que és qüestionable si la gradació de la vulneració del deure de secret correspon a l'atribuïda, ja que la conducta ha estat qualificada com a molt greu en atenció a que s'han posat a disposició dels usuaris de xarxes d'intercanvi dades de salut de persones identificades. Però sosté la Secretaria que a les bases de dades "Llibre Registre Autopsies.mdb" i "Control_Salas_y_Tecnicos_Access2003.mdb" no es recullen dades especialment protegides, i a la base de dades "Malpraxis20041210 Access 2000.mdb" no es recullen dades relatives a la salut.

En primer lloc, escau assenyalar que tal com es feia constar al Fonament de Dret Tercer de la Proposta de resolució i al Fonament de Dret Quart d'aquesta resolució, les dades del fitxer d'autòpsies i del de control de sales i tècnics, són de nivell bàsic, mentre que el de malpraxis, es va considerar que eren de nivell alt. Atès que són tres els fitxers que van aparèixer a Internet es podia considerar que eren tres les infraccions comeses, no obstant això, es va valorar aquesta posada a disposició a Internet com una sola conducta i es va sancionar per la conducta més greu, que era la vulneració del deure de secret de l'article 44.4.g) LOPD.

En segon lloc, pel que fa al fitxer de malpraxis, del qual la Secretaria de Relacions amb l'Administració de Justícia entén que no conté dades de salut, escau fer la consideració següent. En primer lloc, aquest fitxer conté una sèrie de registres amb dades personals de la persona que es objecte de revisió pels metges forenses de l'IMELEC i del metge que efectua aquesta revisió. A més, hi ha dades relatives a procediments judicials, com ara el Jutjat que tramita les actuacions, el tipus de procediment i nombre de les diligències o procediment, per la qual cosa aquestes dades són de nivell mig. Però no només això, ja que del conjunt d'informació que contenen els registres s'infereix informació relativa a la salut de les persones. En aquest sentit, escau assenyalar que els registres relatius a les persones que se sotmetien als reconeixements

mèdic forenses contenen informació –relacionada amb la salut- tal com demostren alguns dels exemples que es recullen a continuació:

- Resultat de l'informe: "Existencia malpraxis", "Resultado postquirúrgico no deseado", "No malpraxis", "Error diagnóstico"

- Tipus d'informe: "Pericial malpraxis", "Lesiones", "Ampliación informe médico forense", "Respuesta preguntas"

- Especialitat: "Obstetrícia i Ginecologia", "Oftalmologia", "Oncologia Mèdica", etc.

- Observacions: "*Cabe considerar que se ha producido un retraso en la administración de la transfusuón sanguïnea, según el informe médico forense"* (registre 68); *"Segun el informe, la anestesia suministrada a la parturienta al iniciarse el perido expulsivo del parto no era la adecuada para un caso de cesárea" (*registre 74); *" El informe dice que la secuela descrita es probablemente consecutiva en primer lugar a una inmovilización que se prolongó durante 35 dias en lugar de 21 dias de inmovilización para las fracturas del cuello de los metacarpianos, según la bibliografia consultada"* (registre 129),etc.

- Bibliografia consultada: "*Capítulos de Laparoscopia y Biopsia y Biopsia Hepática*" (registre 14); "*Trasplante de médula ósea*" (registre 100), etc.

Per tant, del conjunt de la informació que oferien els diferents camps de dades del fitxer, sí que es pot extreure informació relativa a la salut de les persones, per la qual cosa resulta d'aplicació el nivell alt.

Per tant, aquesta al·legació no pot prosperar.

Quart.- L'article 10 LOPD estableix:

"El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardar-les, obligacions que subsisteixen fins i tot després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el seu responsable."

L'article 44.4.g) LOPD disposa que és una infracció molt greu:

"La vulneració del deure de guardar secret sobre les dades de caràcter personal a què fan referència els apartats 2 i 3 de l'article 7, així com les que hagin estat recollides per a finalitats policials sense el consentiment de les persones afectades."

El deure de secret o de confidencialitat que preveu l'article 10 LOPD comporta que tant el responsable del fitxer com qualsevol altra persona que intervingui en el tractament de les dades, no les doni a conèixer a tercers fora dels casos permesos per la llei, és a dir, suposa un deure de custodiar amb diligència les dades personals objecte de tractament. La persona física titular de la dada ha de tenir la garantia que el responsable del fitxer preservarà la seva intimitat, que tractarà les seves dades d'acord amb el consentiment atorgat per a una determinada finalitat, o la disposició legal que habiliti aquest tractament, i que existirà una confidencialitat absoluta. Aquesta obligació inclou tan les conductes actives, com seria la difusió directa de d'aquestes

dades, com les conductes per omissió, és a dir, la manca de mesures de seguretat dirigides a evitar aquesta difusió.

Aquest deure resulta especialment important en les organitzacions actuals, ja que els avanços de la tècnica poden provocar situacions de major risc per a les dades, tal com ha succeït en el present cas, ja que tres fitxers de l'IMELEC van aparèixer en una xarxa pública d'intercanvi d'arxius d'Internet, i van estar durant un temps indefinit accessibles a tercers. Per tant, el responsable del fitxer, com a màxim responsable de la custòdia de les dades, va infringir aquest deure de secret.

Tot i que la difusió d'informació s'ha portat a terme per personal de l'IMELEC, el règim sancionador previst a la LOPD comporta l'atribució de responsabilitat pels fets imputats a la Secretaria de Relacions amb l'Administració de Justícia, per la seva condició de responsable del fitxer. Això, sense perjudici de la possibilitat d'iniciar les actuacions disciplinàries que es considerin procedents.

Les dades personals que contenien aquests fitxers eren de nivell bàsic, mig i alt. D'una banda, el fitxer d'autòpsies, recollia les dades del personal de l'IMELEC (metge forense o tècnic) que intervenia en l'autòpsia (les dades de les persones difuntes queden forma de l'àmbit de protecció de la LOPD), per tant aquestes dades identificatives, laborals i professionals (treballador de l'IMELEC i categoria professional) tenen la consideració de dades bàsiques. En segon lloc, el fitxer de malpraxis, té un conjunt de dades que a part de les dades identificatives (nivell bàsic), també recull dades de procediments judicials (nivell mig) i altres dades que permeten inferir l'estat de salut (nivell alt), tal com s'ha exposat a l'apartat anterior. Per últim, el fitxer de control de sales i tècnics, conté diferents taules amb dades identificatives del personal de l'IMELEC, professionals, laborals, etc (nivell bàsic).

La LOPD qualifica la vulneració del deure de secret com a infracció lleu, greu o molt greu, depenent del contingut de la informació objecte de difusió. Escau assenyalar que quan es va dictar l'acord d'inici del present procediment sancionador, es va considerar que els fets podien ser constitutius de les infraccions lleu de l'article 44.2.e) i molt greu de l'article 44.4.g) de la LOPD, ambdues relacionades amb el deure de secret. No obstant això, s'ha valorat la conducta en conjunt i s'ha considerat que en tractar-se d'un únic acte de difusió de dades a través d'Internet, procedeix sancionar aquests fets per la conducta més greu, que és la revelació de les dades de salut, constitutiva de la infracció prevista a l'article 44.4 g) de la LOPD, enlloc de sancionar de forma individualitzada la revelació de dades derivada de la publicació a través d'Internet de cadascun dels fitxers.. De tal manera que, tenint en compte que s'hauria comès una infracció molt greu per vulneració del deure de secret, en aquest tipus s'inclourien també les infraccions lleus referents a la vulneració del deure de secret.

Cinquè.- L'article 9 LOPD preveu el següent:

"1. 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.

2. No s'han de registrar dades de caràcter personal en fitxers que no compleixin les condicions que es determinin per via reglamentària en relació amb la seva integritat i seguretat i a les dels centres de tractament, locals, equips, sistemes i programes.
3. S'han d'establir per reglament els requisits i les condicions que han de complir els fitxers i les persones que intervinguin en el tractament de les dades a què es refereix l'article 7 d'aquesta Llei."

En aquest sentit, el Reial decret 994/1999, d'11 de juny, pel qual s'aprova el Reglament de seguretat dels fitxers automatitzats que continguin dades de caràcter personal, que resultava d'aplicació en el moment en què van succeir els fets, preveu, entre altres, les següents mesures de seguretat:

Article 6
"L'execució de tractament de dades de caràcter personal fora dels locals de la ubicació del fitxer ha de ser autoritzada expressament pel responsable del fitxer i, en tot cas, s'ha de garantir el nivell de seguretat corresponent al tipus de fitxer tractat."

Article 9
Funcions i obligacions del personal
"1. Les funcions i les obligacions de cada una de les persones amb accés a les dades de caràcter personal i als sistemes d'informació estan clarament definides i documentades, d'acord amb el que preveu l'article 8.2.c).
2. El responsable del fitxer ha d'adoptar les mesures necessàries perquè el personal conegui les normes de seguretat que afecten l'exercici de les seves funcions, com també les conseqüències en què pugui incórrer en cas d'incompliment."

Article 13
Gestió de suports
"1. Els suports informàtics que continguin dades de caràcter personal han de permetre d'identificar el tipus d'informació que contenen, ser inventariats i emmagatzemar-se en un lloc amb accés restringit al personal autoritzat per fer-ho en el document de seguretat.
2. La sortida de suports informàtics que continguin dades de caràcter personal, fora dels locals en què estigui ubicat el fitxer, només pot ser autoritzada pel responsable del fitxer."

Article 17
Auditoria
"1. Els sistemes d'informació i les instal·lacions de tractament de dades s'han de sotmetre a una auditoria interna o externa que verifiqui el compliment d'aquest Reglament, dels procediments i les instruccions vigents en matèria de seguretat de dades, com a mínim, cada dos anys.
2. L'informe d'auditoria ha d'emetre dictamen sobre l'adequació de les mesures i els controls a aquest Reglament, identificar-ne les deficiències i proposar les mesures correctores o complementàries necessàries. També ha d'incloure les dades, els fets i les observacions en què es basin els dictàmens fets i les recomanacions proposades.
3. Els informes d'auditories han de ser analitzats pel responsable de seguretat competent, que ha d'elevar les conclusions al responsable del fitxer perquè adopti les mesures correctores adequades, i queden a disposició de l'Agència de Protecció de Dades."

Article 20
Gestió de suports
"1. S'ha d'establir un sistema de registre d'entrada de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data
i l'hora, l'emissor, el nombre de suports, el tipus d'informació que contenen,
la forma d'enviament i la persona responsable de la recepció que ha d'estar degudament autoritzada.

2. També s'ha de disposar d'un sistema de registre de sortida de suports informàtics que permeti, directament o indirecta, de conèixer el tipus de suport, la data i l'hora, el destinatari, el nombre de suports, el tipus d'informació que contenen, la forma d'enviament i la persona responsable del lliurament que ha d'estar degudament autoritzada.
3. Quan un suport hagi de ser rebutjat o reutilitzat, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació posterior de la informació emmagatzemada, abans de procedir a donar-lo de baixa en l'inventari.
4. Quan el suports hagin de sortir fora dels locals en què estiguin ubicats els fitxers com a conseqüència d'operacions de manteniment, s'han d'adoptar les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada."

L'incompliment de les mesures de seguretat és constitutiu d'una infracció greu, d'acord amb l'article 44.3.h) LOPD:

"Mantenir els fitxers, locals, programes o equips que continguin dades de caràcter personal sense les degudes condicions de seguretat que es determinin per la via reglamentària."

L'article 9 LOPD recull el principi de seguretat de les dades, com a una de les garanties màximes del tractament de les dades personals, i obliga als responsables de fitxer a adoptar les mesures de seguretat tècniques i organitzatives legalment previstes per garantir aquest principi.

Durant la tramitació d'aquest procediment s'ha acreditat que la Secretaria de Relacions amb l'Administració de Justícia disposava d'un document de seguretat que determinava les mesures de seguretat aplicables als fitxers de l'IMELEC. Però la realitat de la gestió dels sistemes d'informació d'aquest organisme no s'adequava a les previsions que contenia el document esmentat. Sense que s'hagi realitzat una auditoria completa dels sistemes d'informació de l'IMELEC, les actuacions realitzades han permès determinar que la gestió de sortida de suports no complia els mínims requeriments de seguretat, tota vegada que un treballador de l'IMELEC, s'emportava de forma habitual en suports portàtils els fitxers que van aparèixer a Internet, amb una finalitat legítima, com és la gestió del servei que té encomanat, però en unes condicions de seguretat que no complien amb les exigències legals. La sortida de la seu de l'IMELEC dels suports amb informació es feia prescindint de les garanties legals i de les directrius que donava el document de seguretat.

La formació del personal en matèria de protecció de dades i les prevencions que han de tenir a l'hora de tractar les dades tampoc no s'ha portat a terme de forma adequada per part del responsable del fitxer. De res serveix definir i implementar mesures de seguretat si no es forma adequadament al personal que tracta les dades i es defineixen clarament les obligacions concretes que cadascú té en el tractament d'aquestes dades. Una adequada formació i informació al personal que tracta les dades podria haver evitat els fets que han donat lloc al present procediment.

Així mateix, si s'hagués realitzat l'auditoria bianual que preveu l'article 17 del Reial decret 994/1999, es podria haver detectat la situació real pel que fa a la seguretat dels fitxers, ja que l'informe d'auditoria forçosament s'ha de referir a l'adequació de les mesures de seguretat i controls al Reial decret de mesures de seguerat, també ha d'identificar les deficiències i proposar les mesures correctores. L'auditoria no consisteix en un mer tràmit, sinó que persegueix fer efectiva la seguretat, detectar deficiències, revisar la situació de les mesures adoptades, si encara continuen efectives, etc. Per tant, la realització d'aquesta auditoria, hauria permès detectar les mancances de seguretat dels fitxers de l'IMELEC.

Per tant, la Secretaria de Relacions amb l'Administració de Justícia no va implementar de forma efectiva les mesures de seguretat, tècniques i organitzatives, necessàries per evitar que les dades personals objecte de tractament arribessin a tercers no autoritzats, i, en conseqüència, va incórrer en la infracció de l'article 44.3.h LOPD.

Sisè.- L'article 44.3.a) de la LOPD estableix que és una infracció greu:

"Crear fitxers de titularitat pública o iniciar la recollida de dades de caràcter personal per als mateixos fitxers, sense l'autorització de disposició de caràcter general, publicada en el Butlletí Oficial de l'Estat o el diari oficial corresponent"

L'article 20.1 de la LOPD preveu que:

"La creació, la modificació o la supressió dels fitxers de les administracions públiques només es poden fer per mitjà d'una disposició general publicada en el Butlletí Oficial de l'Estat o en el diari oficial corresponent."

L'IMELEC disposa d'un fitxer d'autòpsies que recull dades personals dels metges forenses i tècnics que hi intervenen. Aquest tractament de dades s'ha realitzat amb incompliment de l'obligació de l'article 20 LOPD que preveu que la creació de fitxers es faci mitjançant una disposició de caràcter general publicada al diari oficial que correspongui. Aquesta disposició de caràcter general és la que autoritza i dóna cobertura al tractament de dades, per la qual cosa s'ha de portar a terme abans que s'iniciï el tractament de dades.

La Secretaria de Relacions amb l'Administració de Justícia, per tant, hauria de procedir a crear aquest fitxer o bé, en el seu cas, modificar algun dels fitxers dels què té legalment constituïts, de manera que doni cobertura al tractament de dades que realitza mitjançant el fitxer d'autòpsies, és a dir, les dades personals dels metges i personal tècnic de l'IMELEC que porten a terme les autòpsies..

D'altra banda, l'IMELEC té un fitxer anomenat "Control de Sales i Tècnics", que té una finalitat organitzativa de les persones i recursos (sales) a fi de garantir la seva disponibilitat i localització. Aquest fitxer s'alimenta de les dades personals del personal de l'IMELEC, és a dir, dades identificatives i de contacte, situació personal a efectes de substitucions, etc. Aquesta finalitat no es correspon ni es pot considerar inclosa amb les finalitats que té el fitxer GIP-SIP, tota vegada que aquest últim té com a finalitat gestionar les dades personals, econòmiques i laborals del personal de la Generalitat. Per tant, la Secretaria de Relacions amb l'Administració de Justícia hauria de procedir a la creació d'aquest fitxer mitjançant disposició de caràcter general, i adequar-lo als requeriments de la LOPD.

Fent ús de les facultats que em confereix l'article 15 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat de Catalunya,

RESOLC

Primer.- Declarar que la Secretaria de Relacions amb l'Administració de Justícia ha comès una infracció molt greu prevista a l'article 44.4.g) en relació amb el deure de secret previst a l'article 10, ambdós de la LOPD; una infracció greu prevista a l'article 44.3.h) en relació amb l'article 9 de la LOPD i les obligacions derivades de l'aplicació del Reial decret 994/1999, d'11 de juny, pel qual s'aprova el Reglament de seguretat dels fitxers automatitzats que continguin dades de caràcter personal; i una altra infracció greu prevista a l'article 44.3.a) LOPD, en relació amb l'article 20 de la LOPD.

Segon.- Notificar aquesta resolució a la Secretaria de Relacions amb l'Administració de Justícia, i comunicar-la a la persona denunciant.

Tercer.- Comunicar aquesta resolució al Síndic de Greuges, de conformitat amb el que preveu l'article 16.4 de la Llei 5/2002, de 19 d'abril, mitjançant el seu trasllat literal, segons el que especifica l'Acord Tercer del Conveni de Col·laboració entre el Síndic de Greuges de Catalunya i l'Agència Catalana de Protecció de Dades de data 23 de juny de 2006.

La directora

Esther Mitjans i Perelló

Barcelona, 6 de novembre de 2008