Autoritat Catalana de Protecció de Dades

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

RESOLUCIÓ del procediment sancionador núm. PS 68/2013, referent al Departament de Territori i Sostenibilitat de la Generalitat de Catalunya.

Antecedents

Primer.- En data 22/03/2013 va tenir entrada a l'Autoritat Catalana de Protecció de Dades una denúncia formulada per tres ciutadans en relació a un presumpte incompliment de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (en endavant, LOPD).

En primer lloc, les persones denunciants exposaven: a) que el Departament de Política Territorial i Obres Públiques (ara, Departament de Territori i Sostenibilitat) va signar, en data 04/11/2009, un contracte administratiu amb l'empresa Informática el Corte Inglés, SA (en endavant, IECISA), per tal que aquesta empresa dugués a terme l'execució dels *"Serveis de facilitació de l'ús de les TIC i assegurament de la disponibilitat dels elements que formen la infraestructura TIC del Departament de Política Territorial i Obres Públiques – Lot 2: Prestació de serveis TIC de gestió de sistemes, parc informàtic, explotació i xarxa pel departament de Política Territorial i Obres Públiques",* b*)* que l'empresa IECISA, com a encarregada del tractament, va subcontractar diverses empreses ("Empresa A", "Empresa B", "Empresa C", "Empresa D" i "Empresa E"), per tal que aquestes empreses prestessin determinants serveis informàtics al Departament en el marc de la contractació administrativa esmentada; i, c) que les persones aquí denunciants, que havien prestat els seus serveis al Departament com a treballadors de dues de les empreses subcontractades, havien detectat determinades actuacions que podien vulnerar la LOPD, en concret:

- Que *"el servidor que emmagatzema els expedients mèdics del personal de Departament és el PTBRPREVEN01, i era totalment accessible a tots els treballadors* (s'entén a tots els treballadors de les empreses subcontractades), *incloent la base de dades. El tractament que es donava a aquest servidor era l'habitual, es realitzaven exportacions de dades i backups a nivell de dades sense cap limitació".*

- Que aquests treballadors de les empreses subcontractades podien accedir a una *"eina de monitorització i proxy web on es podia veure sense limitacions les pàgines web visitades per qualsevol usuari relacionant IP-Pàgina visitada".*

- Que, *"quan un usuari tenia un problema a una aplicació concreta i la incidència arribava a un dels treballadors de les empreses externes subcontractades, el tècnic es connectava al PC (local o remotament), de forma que podia veure les dades que l'usuari en qüestió estava tramitant".*

- Que *"existia un repositori de contrasenyes, on tots els treballadors d'aquestes empreses subcontractades podien veure l'usuari i contrasenya per accedir a tots els servidors"*.

En segon lloc les persones denunciants manifestaven que en l'acte d'inspecció que es va dur a terme en el si de la informació prèvia núm. IP 249/2011, iniciada arran d'una denúncia que

havien presentat elles mateixes amb anterioritat, i que va derivar en la incoació del PS 19/2012 contra el Departament de Territori i Sostenibilitat, el Departament no va posar en coneixement del personal inspector determinats fets (en concret la subcontractació de les empreses abans esmentades en relació a la contractació administrativa citada), fet que hauria de considerar-se com una obstrucció a l'actuació inspectora.

Les persones denunciants van aportar, juntament amb la seva denúncia rebuda el 22/03/2013 i també a través d'un escrit posterior presentat a l'Autoritat el dia 19/04/2013, diversa documentació relativa als fets denunciats. Entre aquesta documentació consta un correu electrònic enviat el dia 25/05/2011 per una de les persones aquí denunciants a diverses persones –amb còpia també a varies persones- en el que figura el literal següent:

"Asunto: Repositori de Passwords (...).
Bon dia: XXX m'ha encomanat un PorTic de «persecució» així que no m'ho feu difícil!!! Abans de Divendres (m'ho ha recalcat un parell de cops) heu de revisar el repositori de passwords actual i comprovar que TOTS els passwords que vosaltres feu servir en la vostra operativa diària (...)
URL: https://clipperz.(...)
Usuari: (...)
Pass: l'haurieu de saber"

Segon.- L'Autoritat va obrir una fase d'informació prèvia (IP 52/2013), d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, en relació amb la DT 2ª de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, per tal d'obtenir més informació sobre les circumstàncies dels fets i els subjectes responsables.

S'incorporà a aquesta informació prèvia una còpia de la documentació que seguidament es detalla, inclosa en les actuacions corresponents al procediment sancionador núm. 19/2012 referent al Departament de Territori i Sostenibilitat, atès que la contractació a la qual es referien les persones denunciants és la mateixa contractació administrativa que fou analitzada en el citat procediment sancionador.

1. Contracte, de data 04/11/2009, celebrat entre el Departament de Política Territorial i Obres Públiques i l'empresa IECISA, mitjançant el qual la dita empresa es compromet a l'execució dels *"Serveis de facilitació de l'ús de les TIC i assegurament de la disponibilitat dels elements que formen la infraestructura TIC del Departament de Política Territorial i Obres Públiques – Lot 2: Prestació de serveis TIC de gestió de sistemes, parc informàtic, explotació i xarxa pel departament de Política Territorial i Obres Públiques".*

2. La part corresponent al Lot 2 *("Prestació de serveis TIC de gestió de sistemes, parc informàtic, explotació i xarxa pel departament de Política Territorial i Obres Públiques")* del plec de prescripcions tècniques relatives al contracte de serveis *"Serveis de facilitació de l'ús de les TIC i assegurament de la disponibilitat dels elements que formen la infraestructura TIC del Departament de Política Territorial i Obres Públiques".*

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

A l'apartat 7 d'aquest plec, anomenat *"Altres condicionants",* es preveu el següent: *"Com una de les eines principals de servei seran les eines de control remot, cal establir que qualsevol actuació que s'hagi de fer als ordinadors del DPTOP assignats a usuaris, sempre que es facin servir aquestes eines, requerirà prèviament l'autorització de l'usuari que el té assignat".*

3. Plec de clàusules administratives particulars relatives al contracte de serveis *"Serveis de facilitació de l'ús de les TIC i assegurament de la disponibilitat dels elements que formen la infraestructura TIC del Departament de Política Territorial i Obres Públiques".*

En el si d'aquesta fase d'informació, per mitjà d'ofici de data 08/04/2013, es va requerir el Departament de Territori i Sostenibilitat per tal que donés compliment al següent:

- Que informés sobre els perfils d'usuari que tenien definit els treballadors de les empreses que prestaven els seus serveis a les dependències del Departament ("Empresa A", "Empresa B", "Empresa C", "Empresa D" i "Empresa E") i concreció dels tractaments o fitxers amb dades personals als quals podien accedir.

- Que aportés el document de seguretat vigent en el període en què van prestar serveis al Departament les citades empreses subcontractades.

El Departament va respondre l'anterior requeriment a través d'escrit de data 22/04/2013, pel qual s'exposava, entre d'altres, el següent:

"Pel que fa als perfils d'accés, a continuació us els especifiquem en funció del serveis concrets que prestava cada empresa al Departament i d'acord amb la informació facilitada per IECISA: (...)
1- Personal de Sistemes: "Empresa D" *(Sr.... i Sr... La seva tasca consistia en l'administració dels sistemes operatius dels servidors Windows Linux i virtualitzacions. Aquest personal disposava d'usuaris nominatius amb un nivell de privilegis que comportava l'accés a tots els servidors del Departament on hi ha repositoris de dades d'usuaris, repositoris de dades compartides d'usuaris i còpies de seguretat; no tenien accés, en canvi, a les bases de dades, la gestió de les quals assumia un altre grup de servei.*
2- Personal administrador de la plataforma web: "Empresa E" *(Sr...). La seva tasca consistia en desplegar les aplicacions en la plataforma web i fer-ne el manteniment. La persona disposava d'usuari nominatiu amb un nivell de privilegis limitat a l'accés als entorns de gestió de la plataforma web, cosa que no comporta accedir a les dades contingudes a les aplicacions (aquest accés està regulat i concedit per personal gestor del Departament)*
3- Personal d'Operació: "Empresa B" *(Sr...). La seva tasca consistia en realitzar la monitorització dels sistemes del Departament i les restauracions i control de les còpies de seguretat i de les dades compartides dels servidors. La persona disposava d'un usuari nominatiu amb un nivell de privilegis que li permetia accedir de manera directa a dades de recursos compartits per poder atorgar o denegar accessos sota demanda o verificar les còpies de seguretat o restauració de dades.*

4- Personal de comunicacions: "Empresa D" *fins primer semestre 2011* - "Empresa C" *des del segon semestre de 2011 (Sr...) La seva tasca consistia en la gestió de la xarxa de comunicacions del Departament (routers, swichs, etc) La persona disposava d'usuari nominatiu amb un nivell de privilegis que no li permetia accedir a cap servidor amb dades de caràcter personal.*
5- Personal de Sistemes d'Informació Geogràfica (SIG): "Empresa A" *(Sr...). La seva tasca consistia en la gestió de la cartografia i de les aplicacions SIG. La persona disposava d'usuari nominatiu amb un nivell de privilegis que només li permetia accedir als servidors amb informació cartogràfica i geogràfica, sense accés, per tant, a dades de caràcter personal.*
6- Personal de base de dades: "Empresa D" *fins el primer semestre 2011* - "Empresa C" *des del segon semestre 2011 (Sr...) i* "Empresa B" *des del segon semestre de 2011 (Sr...). La seva tasca consistia en gestionar els servidors que contenen bases de dades. Les persones disposaven d'usuari específic amb un nivell de privilegis que permet accedir als registres emmagatzemats en les bases de dades dels aplicatius del Departament."*

D'aquesta informació es desprèn que el personal de sistemes, d'operació i de base de dades podien accedir a dades de caràcter personal, tot i que el desenvolupament normal de les seves funcions no ho requeria.

Pel que fa als fitxers als quals podien accedir, val a dir que atesos els permisos exposats, les persones que podien tenir eventualment accés a dades, el tenien al conjunt de fitxers responsabilitat del Departament.

(...) entenem que l'accés a dades per part de les persones contractades o subcontractades no era, en si mateix, dolent ni erroni –en alguns casos podia ser fins i tot necessari per dur a terme les funcions encomanades- des del moment en què estaven subjectes, per contracte, a guardar secret respecte de la informació que poguessin conèixer en el desenvolupament de la seva tasca professional."

Juntament amb aquest escrit, el Departament aportava el Document de Seguretat del Departament de Territori i Sostenibilitat, versió 1.1 de desembre de 2010.

També en el si d'aquesta fase d'informació prèvia, mitjançant ofici de 23/04/2013, es va requerir IECISA per tal que aportés, entre d'altres, la següent informació: les persones concretes de les empreses subcontractades "Empresa A", "Empresa B", "Empresa C", "Empresa D", "Empresa E" que van prestar serveis al Departament de Territori i Sostenibilitat, especificant en relació a cadascuna d'aquestes persones a quina empresa estava vinculada i el període durant el qual va prestar serveis al Departament.

IECISA va respondre l'anterior requeriment a través d'escrit de data 08/05/2013, en el qual informava sobre les persones concretes de les empreses subcontractades que havien prestat serveis al Departament, així com el període durant el qual van prestar aquest servei. En concret:

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

"NOMBRE	*EMPRESA*	*PERIODO DE SERVICIO*
Sr...	"Empresa E"	*01/10/2099 A 27/06/2011*
Sr...	"Empresa A"	*01/10/2009 a 31/12/2012*
Sr...	"Empresa C"	*11/07/2011 a 31/12/2012*
Sr...	"Empresa C"	*11/07/2011 a 31/12/2012*
Sr...	"Empresa D"	*01/10/2009 A 27/06/2011*
Sr...	"Empresa D"	*01/10/2009 A 27/06/2011*
Sr...	"Empresa D"	*01/10/2009 A 27/06/2011*
Sr...	"Empresa D"	*01/10/2009 A 27/06/2011*
Sr...	"Empresa B"	*09/12/2009 a 25/05/2012*
Sr...	"Empresa B"	*08/09/2011 a 31/12/2012*

També en aquesta fase d'informació prèvia, mitjançant escrit de data 29/05/2013, es va requerir IECISA per tal que aportés la informació següent:

- Si ha estat operatiu un repositori de contrasenyes al qual podia accedir el personal de les empreses subcontractades per IECISA per prestar serveis al Departament, cosa que permetria conèixer al citat personal l'usuari i contrasenya per accedir a tots els servidors. Que en cas afirmatiu, es concretés:

- Les persones que haurien tingut accés al citat repositori i les raons que justificarien que aquestes persones tinguessin coneixement recíproc d'usuaris i contrasenyes.

- La data fins a la qual s'hauria mantingut operatiu el citat repositori.

IECISA va donar resposta a l'anterior requeriment a través d'escrit de data 14/06/2013, en el qual informava del següent:

- Que *"en los proyectos de referencia en los que IECISA prestaba sus servicios como adjudicatario al Departament de Territori i Sostenibilitat de la Generalitat de Catalunya (…) y en complimiento de lo establecido en el artículo 93 del RD 1720/2007 de 21 de diciembre de desarrollo de la LOPD, el Departament como responsable del fichero, tenía implementada una herramienta para la gestión de las contraseñas denominada CLIPPERZ (https://www.cliperz.....) de la que IECISA, desde el mismo momento en que se hizo cargo del servicio (finales de 2009) y en calidad de Encargado del tratamiento, empezó a utilizar siguiendo en todo momento las instrucciones del responsable del fichero, cuyo interlocutor principal era el Gestor de Tecnología del Área TIC del Departament (Don XXX).*

A continuación les hacemos una breve referencia de las características de esta herramienta aunque, para una mayor aclaración sobre su funcionamiento, les aconsejamos consulten directamente al Departament de Territori i Sostenibilitat de la Generalitat de Catalunya que decidió su uso e implantación:

a) CLIPPERZ es una aplicación específica para la gestión de contraseñas la cual está debidamente securizada ya que las mismas están cifradas. El cifrado se lleva a cabo mediante una serie de algoritmos criptográficos conocidos, como AES, SHA, lo cual impide que pueda tener acceso a las mismas personas que desconozcan los parámetros de acceso.

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

b) La finalidad del repositorio de contraseñas que implementó el Departament era mantener el registro de todas las contraseñas de administrador de los servidores que dispone el Departament al objeto de que, en caso de emergencia, cambio de personal de gestión de los sistemas o cualquier otra contingencia que pudiera disponer de las mismas.
c) El acceso a la información se llevaba a cabo a través del nombre del servidor, que una vez estaba localizado, permitía el acceso conforme a la contraseña que tuviera asociada.
d) La propia aplicación no permite el acceso mediante perfiles lo que supone que el personal que tenía acceso a las mismas lo era tan sólo en modo consulta y debía realizar la búsqueda del servidor específico ya que esta era la manera en la que la información estaba indexada, dentro de su área de gestión.
e) Tan sólo el personal técnico, con privilegios para modificar la información, era el autorizado para llevar a cabo los mismos (…)

Cada gestor técnico era responsable de un grupo de servidores sin que tuviera conocimiento de los servidores que gestionaban el resto de sus compañeros (…)".

- Que *"el repositorio de contraseñas estaba operativo por parte del Departament con anterioridad a la entrada a prestar el servicio por parte de IECISA. Desconocemos si el mismo sigue operativo ya que IECISA no es, actualmente, el prestador del mismo aunque no tenemos noticias de que haya dejado de estar en activo".*

IECISA aportava, juntament amb aquest escrit, documentació diversa.

També en el si d'aquesta fase d'investigació, el dia 23/07/2013, l'Autoritat va realitzar un acte d'inspecció a la seu del Departament de Territori i Sostenibilitat, el resultat de la qual consta a l'acta d'inspecció incorporada a les actuacions. A aquest acte, a més dels representants del Departament, també hi van assistir representants de l'empresa IECISA.

Durant l'acte d'inspecció, els representants de les diferents entitats presents van manifestar, entre d'altres qüestions, el següent:

a) En relació a l'accés, per part dels treballadors de les empreses subcontractades al servidor que emmagatzema els expedients mèdics del personal de Departament, exposaren:

- Que hi ha un conjunt d'administradors de sistemes que tenen accés a tots el servidors, El password de cada base de dades només el té el seu "Data Base Administrator" (DBA).
- Que administradors de sistemes hi havia 4 persones (2 de IECISA i 2 d'empreses subcontractades).
- Que com administradors de sistemes, com a regla general, tenen accés a les funcions d'administració de tot els servidors, excepte per servidors o funcionalitats concretes que només podien accedir determinats administradors de sistemes.
- Que en relació al perfil dels treballadors de les empreses subcontractades i autoritzacions d'accés, es remeten a l'escrit que el Departament va dirigir a l'Autoritat en el marc d'aquesta informació prèvia el dia 22/04/2013.

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

- Que el DBA de la base de dades de prevenció de riscos, situada al servidor PTBRPREVEN01, podia accedir a les dades contingudes en aquesta base de dades, ateses les funcions que tenia encomanades i que desconeix si podien haver mecanismes addicionals de protecció de la informació que impedissin accedir a les dades personals.

b) En relació a l'accés, per part dels treballadors de les empreses subcontractades, a una eina de monitorització i proxy web on es podia veure sense limitacions les pàgines web visitades per qualsevol usuari relacionant IP-Pàgina visitada, exposaren:

- Que tenen coneixement que hi havia un projecte per tal d'implementar aquesta eina de monitorització i proxy web, però que finalment no es va posar en marxa.
- El representant de IECISA manifesta que aquest projecte en cap cas no havia estat promogut per la seva empresa.

c) En relació a l'existència d'un repositori de contrasenyes, on tots els treballadors de les empreses subcontractades podrien veure l'usuari i contrasenya per accedir a tots els servidors, exposaren:

- Els representants del Departament manifesten que no tenen constància que l'ús de l'aplicació CLIPPERZ hagi estat a requeriment del Departament.
- El representant de IECISA manifesta que, tal com estava definit el circuit de relacions entre proveïdors i Departament, suposa que l'ús d'aquesta aplicació venia determinat pel gestor tècnic del Departament (CTTI) i que s'hauria utilitzat seguint les seves instruccions.
- Que la funcionalitat d'aquesta aplicació és recopilar la informació de totes les contrasenyes d'administradors d'entorns tecnològics (sistemes operatius de servidors, de bases de dades, serveis web, servidors de fitxers, etc)
- Que aquesta aplicació està instal·lada en el CPD del Departament.
- Que a aquesta aplicació hi podien accedir les persones que treballaven a les empreses subcontractades per IECISA, mitjançant un únic usuari i contrasenya que permet entrar a l'aplicació per consultar les dades referides a usuaris i contrasenyes de cada entorn tecnològic.
- Que el filtre de consulta d'usuaris i contrasenyes d'aquesta aplicació no depèn de perfils d'accés, sinó per nom de servidors, base de dades o recurs dels quals es vol conèixer l'usuari i password.
- Que tots aquests tècnics podien accedir a l'aplicació en mode de consulta. Que en mode escriptura només podien accedir determinades persones. Que existeix un registre d'accessos a aquesta aplicació.
- Que per limitacions pròpies de l'aplicació, no era possible limitar l'accés mitjançant perfils.

En aquell mateix acte d'inspecció es va requerir, tant al Departament, com a IECISA, que aportés a l'Autoritat diversa documentació, en concret:

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

- Document de Seguretat del Departament de Territori i Sostenibilitat, en la part que es defineixen els perfils d'accés.
- Informe sobre qui va promoure la implementació d'una eina de monitorització i proxy web i qui va decidir finalment que no s'implementés per raons tècniques.
- Informe sobre les instruccions que havia de seguir IECISA en relació amb la utilització de l'eina CLIPPERZ.

Mitjançant escrit de data 02/08/2013, IECISA va facilitar a l'Autoritat la informació següent:

- Que *"el equipo de trabajo de IECISA no dispone de evidencia material de la petición del Gestor Tecnológico existente en aquel momento en la cual se hiciera petición expresa de la instalación de una herramienta de monitorización y proxi web. (…)*
La implementación de dicha herramienta le fue asignada a un par de empresas, de las cuales tuvo dificultades que no le permitió concluir con los trabajos, y la segunda emitió un informe en el que se indicaban cuáles eran los requerimientos para que la herramienta de monitorización funcionara en los sistemas del Departamento (sic)*".*

- Que *"teniendo en cuenta lo ya expuesto por IECISA en escritos dirigidos a la Autoridad Catalana de Protección de Datos en referencia a anteriores requerimientos dentro de este expediente, corroboramos las peticiones realizadas por el Gestor Tecnológico del Departament (…) en referencia a la utilización de la herramienta CLIPPERZ (…)".*

IECISA aportà, juntament amb el seu escrit, diversa documentació.

Finalment, mitjançant escrit de data 01/08/2013, el Departament va aportar a l'Autoritat *"l'Annex del Document de Seguretat, on es defineixen els perfils d'accés vigent en el període en què les empreses subcontractades esmentades van prestar serveis al Departament".*

Tercer.- En data 30/10/2013 la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar procediment sancionador contra el Departament de Territori i Sostenibilitat per una presumpta infracció greu prevista a l'article 44.3.h) en relació amb l'article 9, ambdós de la LOPD i 93 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la LOPD (en endavant, RLOPD). Així mateix, va nomenar persona instructora de l'expedient a la funcionària de l'Autoritat Catalana de Protecció de Dades, Sra. XXX. Aquest acord d'inici, juntament amb el plec de càrrecs, es va notificar a l'entitat imputada el 05/11/2013.

En el mateix acord d'inici es van explicitar els motius pels quals no s'efectuà cap imputació respecte a d'altres fets denunciats. Al respecte, s'exposava en el fonament de dret quart de l'acord d'inici el següent:

"*Seguidament procedeix abordar la resta de fets que han estat objecte de denúncia, i respecte dels quals no es considera procedent efectuar cap imputació, per les raons que s'apunten seguidament.*

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

4.1.- Pel que fa a l'accés del personal TIC de les empreses subcontractades a determinats servidors.

Les persones denunciants posaven de manifest que el personal TIC de les empreses subcontractades per IECISA podia accedir a les bases de dades contingudes al servidor que emmagatzemava els expedients mèdics (PTBRPREVEN01).

A aquest respecte, segons exposà el Departament, tant en el seu escrit de data 22/04/2013, com en l'acte d'inspecció, el personal TIC només tindria accés als servidors i bases de dades autoritzades, d'acord amb les funcions encomanades.

Cal partir de la premissa que correspon al responsable del fitxer o tractament determinar quins usuaris han de tenir accés als recursos per a l'exercici de les seves funcions. A partir d'aquí, en aquest fet concret denunciat no s'observa cap incompliment de les mesures de seguretat; d'una banda, perquè podria estar justificat l'accés de determinat personal TIC al servidor i a les bases de dades citades pels denunciants, d'acord amb les funcions descrites al Document de Seguretat; i d'altra banda, perquè els accessos autoritzats consten previstos en la relació d'usuaris del citat document de seguretat. D'altra banda, cal dir que no hi ha cap evidència que permeti inferir que persones no autoritzades hagin accedit al servidor o la base de dades mencionada.

Així les coses, resulta aplicable el principi de presumpció d'innocència previst a l'article 137 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (en endavant, LRJPAC), atès que no s'ha pogut acreditar l'existència d'indicis d'infracció.

4.2.- Pel que fa a l'accés per part del personal de les empreses subcontractades a una eina de monitorització i proxy web.

Les persones denunciants manifestaven que el personal de les empreses subcontractades tenien accés a una eina de monitorització i proxy web on es podia veure sense limitacions les pàgines web visitades per qualsevol usuari relacionant IP-Pàgina visitada".

A aquest respecte, cal posar de manifest que les persones denunciants no han aportat cap element tendent a corroborar aquest fet concret denunciat, i amb les actuacions d'investigació efectuades tampoc no s'ha pogut detectar l'existència de cap indici al respecte. Ans al contrari, tot sembla indicar que aquesta eina de monitorització i proxy web no es va arribar mai a instal·lar per part del Departament.

4.3.- En relació a la monitorització de PC's del Departament.

Les persones denunciants exposaven que "quan un usuari tenia un problema a una aplicació concreta i la incidència arribava a un dels treballadors de les empreses externes subcontractades, el tècnic es connectava al PC (local o remotament), de forma que podia veure les dades que l'usuari en qüestió estava tramitant".

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

Respecte a aquesta qüestió cal dir el següent: a) que no hi ha cap evidència que el personal TIC de les empreses subcontractades hagi procedit a la monitorització de PC's del Departament, b) que en cas que la citada monitorització s'hagués produït, no hi ha cap indici que permeti inferir que a través d'aquesta monitorització el personal informàtic que hipotèticament l'hagués dut a terme hagi tingut accés no autoritzat a dades de caràcter personal. A més, cal dir que la monitorització és una operació prevista en el plec de prescripcions tècniques que regia la contractació administrativa entre el Departament i IECISA, monitorització que requeria, segons el citat plec, el consentiment de l'usuari del PC monitoritzat.

És per això que entraria també aquí en joc el principi de presumpció d'innocència previst a l'article 137 de la LRJPAC, atès que no s'ha pogut acreditar l'existència d'indicis que permetin imputar la comissió de cap infracció.

4.4.- Pel que fa a presumpta obstrucció de l'actuació inspectora per part del Departament.

Les persones denunciants entenien que el fet que el Departament, en l'acte d'inspecció que es va dur a terme en el si de la informació prèvia núm. IP 249/2011 -que va derivar en la incoació del PS 19/2012 contra el Departament de Territori i Sostenibilitat-, no posés en coneixement del personal inspector determinats fets, suposava una obstrucció a l'actuació inspectora. En concret, els fets que el Departament –segons els denunciants- hauria ocultat als inspectors de l'Autoritat, serien que IECISA havia subcontractat a les empreses especificades en la seva actual denúncia, en la qual es remarca que l'objecte d'aquelles actuacions d'investigació anteriors fou investigar la subcontractació per part de IECISA d'unes determinades empreses -identificades en aquella denúncia anterior, i diferents a les aquí denunciades- en el marc de la mateixa contractació administrativa de referència.

Atesos els termes de la denúncia, resulta essencial precisar quin és el supòsit de fet de la infracció tipificada a l'article 44.3.j) de la LOPD ("l'obstrucció a l'exercici de la funció inspectora"), supòsit que queda perfectament definit en la sentència de l'Audiència Nacional de 22/04/2009, quan diu:

"La sanción de 60.101,21 euros impuesta a Banco Santander SA, deriva de lo previsto en el artículo 44.3.j) de la LOPD, que tipifica como infracción grave "La obstrucción al ejercicio de la función inspectora".
Infracción que ha de ponerse en relación con el artículo 40 de la LOPD , según el cual:
"1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos".

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

Razona con acierto la resolución de la AEPD combatida que obstruir, según el Diccionario de la Real Academia Española, equivale a "impedir la operación de un agente, sea en lo físico, sea en lo inmaterial", o a "impedir la acción", por lo que bastará con dificultar, poner obstáculos o no colaborar para que pueda estimarse la conducta recogida en el artículo 44.3 .j), y ello sin perjuicio, y al margen, de que se llegue o no al conocimiento de los datos o de la actividad investigada, pues lo que se sanciona no es un resultado sino una conducta que obstruye la tarea inspectora.
Aunque son pocas las ocasiones en que esta Sala ha conocido de infracciones por obstrucción a la labor inspectora de la Agencia, como antecedente hemos de citar la SAN de 15/12/2005 (Rec. 153/2004) que confirmó la legalidad de la sanción impuesta, por considerar que los inspectores de la AEPD estaban legalmente habilitados para requerir la aportación de ciertos documentos a la demandante durante la investigación de la denuncia presentada, sin que en ese momento fuera legalmente obligatorio comunicar del contenido de la denuncia a dicha investigada. Además el Tribunal entendió que el documento requerido era adecuado al objeto y fin de la investigación (pertinente).
Refiriéndose igualmente a un supuesto de obstrucción a la labor inspectora la SAN de 18/4/2007 (Rec. 272/2005).”

En relació amb el cas concret aquí denunciat, cal dir que, d'acord amb el que consta en l'acta d'inspecció que es va expedir el dia 22/11/2011 en el si de la IP 249/11, el personal del Departament de Territori i Sostenibilitat va respondre a totes i cadascuna de les qüestions plantejades pel personal inspector de l'Autoritat, sense que en cap moment s'observés que el dit personal tenia un comportament obstruccionista o poc col·laborador. Cal significar que en el tipus infractor d'obstrucció a la inspecció, a diferència del que succeeix amb la majoria de tipus infractors, s'exigeix la concurrència clara de l'element volitiu, és a dir d'un ànim d'obstruir les funcions de la inspecció, requisit que en cap cas no es pot considerar present quan els representants de l'entitat inspeccionada faciliten tota la informació demanada pel personal inspector. D'acord amb això, el Departament no hauria dut a terme cap actuació que es pugui encabir en el tipus definit a l'article 44.3.j) de la LOPD.

És per tot això que no procedeix incloure entre els fets imputats al Departament les presumptes infraccions de la LOPD analitzades en aquest fonament de dret, per les raons que s'han exposat de forma separada als punts precedents”.

En el plec de càrrecs es concedia a l'entitat imputada un termini de deu dies hàbils comptadors a partir del dia següent de la notificació per formular al·legacions, presentar documents i proposar la pràctica de proves que considerés convenients per a la defensa dels seus interessos.

Quart.- El Departament de Territori i Sostenibilitat va formular al·legacions al plec de càrrecs mitjançant escrit de 15/11/2013.

Cinquè.- Mitjançant escrit de data 01/12/2013 una de les persones denunciants va interposar recurs de reposició en contra de la decisió de l'Autoritat de no imputar en el procediment sancionador incoat, altres fets que també s'havien denunciat.

Aquest recurs de reposició es va inadmetre, per manca de legitimació del recurrent, mitjançant resolució de la directora de l'Autoritat de data 30/01/2014.

Sisè.- En data 21/02/2014 la persona instructora d'aquest procediment va formular proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades declarés que el Departament de Territori i Sostenibilitat havia incorregut en una infracció greu prevista a l'article 44.3.h) en relació amb l'article 9, ambdós de la LOPD, i 93 del RLOPD. Aquesta proposta de resolució fou notificada en data 26/02/2014, i es concedia un termini de 10 dies per formular al·legacions.

Setè.- Per mitjà d'escrit de 06/03/2014 l'entitat imputada ha formulat al·legacions a la proposta de resolució.

Del conjunt de les actuacions practicades en aquest procediment es consideren acreditats els fets que seguidament es detallen com a fets provats.

Fets Provats

Únic.- El Departament de Territori i Sostenibilitat va vulnerar el principi de seguretat de les dades, atès que mitjançant una eina de gestió anomenada CLIPPERZ instal·lada pel citat Departament als seus sistemes d'informació, va permetre que diverses persones –aquelles que tenen accés a la dita eina- tinguessin coneixement a dades relatives a "usuaris" i "contrasenyes" que són compartides entre diferents usuaris de perfil tècnic.

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, segons el previst a la DT 2ª de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.

Segon.- En el si d'aquest procediment sancionador, l'entitat imputada va formular al·legacions davant el plec de càrrecs i també davant la proposta de resolució. El primer escrit d'al·legacions ja fou analitzat en la proposta de resolució formulada per la persona instructora, si bé es considera procedent fer-hi una menció en la present resolució, atès que en les al·legacions presentades davant la proposta de resolució es reprodueixen en part les formulades prèviament davant el plec de càrrecs. Tot seguit s'analitzen doncs el conjunt d'al·legacions de l'entitat imputada.

2.1.- En relació al número de persones amb accés a l'aplicació CLIPPERZ.

El Departament apuntava en el seu escrit d'al·legacions al plec de càrrecs i insisteix novament en el seu escrit d'al·legacions a la proposta, que només eren 10 les persones que tenen accés

a l'aplicació, les quals treballaven per a les empreses que prestaven els serveis de facilitació de l´ús de les TIC del Departament.

Respecte a aquesta qüestió, com ja va exposar la instructora a la proposta de resolució, cal dir que aquesta és una dada que no afecta als fets imputats, ni tampoc és una dada que resulti transcendent a altres efectes. El que aquí resulta rellevant, tal i com es detalla als fets provats, és el fet de permetre que diverses persones poguessin accedir a una aplicació en la qual hi figurava la identificació dels "usuaris" i les "contrasenyes" amb les quals accedien a determinats recursos d'informació, de tal manera que les dites contrasenyes potencialment podien ser compartides per diferents persones.

2.2.- En relació a la necessitat de l'accés.

El Departament afirmava al seu escrit d'al·legacions al plec de càrrecs que *"l'accés per part d'aquestes persones era necessari en el marc de la prestació del servei TIC"*, qüestió sobre la que torna a incidir l'entitat imputada en el seu escrit d'al·legacions a la proposta.

Al respecte cal dir que no es qüestiona aquí l'accés del personal de les empreses externes a l'eina de gestió CLIPPERZ, sinó que el que es considera contrari a la normativa de protecció de dades és el fet que a través de l'eina esmentada, les persones que hi accedien podien tenir coneixement dels codis d'"usuari" i "contrasenya" compartides per altres usuaris de perfil tècnic. D'altra banda, si amb aquesta afirmació el que pretén esgrimir el Departament en la seva defensa és que les persones amb accés a CLIPPERZ necessitaven compartir les contrasenyes allà dipositades per raons del servei, cal dir que el Departament no ha aportat a aquest procediment cap prova que justifiqui aquesta necessitat; i fins i tot en el cas que es donés aquesta eventualitat, s'ha d'assenyalar que tal actuació vulneraria l'article 93 del RLOPD.

2.3.- En relació a les garanties d'accés a les contrasenyes.

El Departament asseverava al seu escrit d'al·legacions al plec de càrrecs que per accedir a la contrasenya corresponent emmagatzemada a l'aplicació CLIPPERZ cal conèixer, a banda de la contrasenya per entrar a la dita aplicació, "*el nom del servidor o de la instància de BD"*, mesures de seguretat que són portades a col·lació novament al seu escrit d'al·legacions a la proposta de resolució.

Tal com va exposar la instructora del procediment a la proposta, aquesta circumstància apuntada pel Departament no és cap impediment per considerar vulnerat el principi de seguretat de les dades. I això perquè conèixer aquestes dades –nom de servidor o de la instància de BD- no sembla que hagués de ser cap obstacle per a les persones que tenen accés a la citada aplicació CLIPPERZ, ateses les seves capacitats i perfil tècnic.

2.4.- En relació al deure de confidencialitat.

El Departament feia referència en el seu escrit d'al·legacions al plec de càrrecs al deure de secret al que està obligat el personal que presta serveis a la seva organització.

Al respecte cal dir que el que s'imputa aquí, com ja s'ha dit, és una vulneració del principi de seguretat (art. 9 de la LOPD) relacionat amb la identificació i autenticació dels usuaris, principi de seguretat que és distint al deure de secret recollit a l'article 10 de la LOPD, al qual al·ludeix el Departament. Dit d'una altra manera, una cosa és que les persones que treballin a l'organització hagin de complir amb el deure de confidencialitat i una altra que el responsable de fitxer tingui l'obligació d'implementar les mesures tècniques i organitzatives pertinents per tal d'evitar l'alteració, pèrdua, tractament o accés no autoritzat a les dades emmagatzemades. Així doncs, es pot donar una vulneració del principi de seguretat de les dades, amb independència de si les persones que han de guardar secret compleixen o no amb aquesta obligació.

2.5.- En relació a la responsabilitat del Departament pel que fa a la implementació de l'eina CLIPPERZ.

En el seu escrit d'al·legacions a la proposta de resolució el Departament exposa que *"la implementació de les mesures de caire pròpiament tècnic estaven en mans del personal del CTTI* (Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya) *assignat al Departament que tenia encomanades aquestes funcions. En concret van decidir utilitzar l'eina CLIPPERZ (...)".*

Al respecte cal dir que el Departament no pot defugir la seva responsabilitat en la implementació de l'eina CLIPPERZ. Tot i que s'hagués donat el supòsit que el CTTI recomanés la implementació de la dita eina, no s'ha d'oblidar que aquest aplicatiu estava instal·lat en els sistemes informàtics del Departament i que els codis d'"usuari" i "contrasenya" que allà s'emmagatzemaven possibilitaven el tractament de dades personals incloses en fitxers dels quals és responsable el Departament, circumstància aquesta que comporta la consideració del Departament com a subjecte a qui s'ha d'imputar la infracció, d'acord amb el règim de responsabilitat previst a l'article 43.1 de la LOPD (*"els responsables dels fitxers i els encarregats dels tractaments estan subjectes al règim de sancionador que estableix aquesta Llei"*).

En definitiva, les al·legacions formulades pel Departament de Territori i Sostenibilitat en el curs d'aquest procediment sancionador i que s'han analitzat fins aquí, no desvirtuen els fets imputats, ni la seva qualificació jurídica, per les raons que s'han exposat en cada cas.

Tercer.- Els fets descrits a l'apartat de fets provats, tal com indicava la persona instructora, es consideren constitutius de la infracció prevista a l'article 44.3.d) de la LOPD, que en la seva redacció donada per la Llei 2/2011, de 4 de març, d'economia sostenible, tipifica com a infracció de caràcter greu:

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

En relació amb aquest tipus infractor, l'article 9 de la LOPD, sobre el principi de seguretat de les dades, disposa el següent:

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

"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".

Aquest desenvolupament reglamentari pel que fa a les mesures de seguretat a adoptar, s'ha dut a terme amb el RLOPD, i en concret, pel seu Títol VIII. D'acord amb els fets declarats provats, el Departament de Territori i Sostenibilitat ha vulnerat la previsió establerta en aquest Títol, en concret, l'article 93 del RLOPD.

L'article 93 del RLOPD, relatiu a la mesura de seguretat relativa a la identificació i autenticació, determina el següent:

"1. El responsable del fitxer o tractament ha d'adoptar les mesures que garanteixin la correcta identificació i autenticació dels usuaris.
2. El responsable del fitxer o tractament ha d'establir un mecanisme que permeti la identificació de forma inequívoca i personalitzada de qualsevol usuari que intenti accedir al sistema d'informació i la verificació conforme està autoritzat.
3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes, hi ha d'haver un procediment d'assignació, distribució i emmagatzematge que en garanteixi la confidencialitat i integritat.
4. El document de seguretat ha d'establir la periodicitat, que en cap cas ha de ser superior a un any, amb què s'han de canviar les contrasenyes que, mentre estiguin vigents, s'han d'emmagatzemar de forma inintel·ligible".

Així doncs, 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. Això comporta que la persona titular de les dades ha de tenir la garantia que aquestes estaran segures. Per tant, el responsable del fitxer o en el seu cas l'encarregat del tractament, tenen el deure d'actuar amb la diligència necessària per tal que la seguretat de les dades no es vegi disminuïda.

Doncs bé, com assenyalava la instructora en la proposta de resolució, durant la tramitació d'aquest procediment han quedat acreditats els fets que s'han descrit a l'apartat de fets provats d'aquesta resolució, fets que vulneren una de les mesures de seguretat de caràcter bàsic establertes a la normativa de protecció de dades, en concret a l'article 93 del RLOPD, atès el següent:

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

- Per una banda, el mecanisme adoptat pel Departament impedeix que s'identifiqui de forma inequívoca i personalitzada a alguns dels usuaris que poden tenir accés al sistema d'informació, ja que diverses persones, mitjançant l'eina de gestió CLIPPERZ, tenien coneixement de diversos codis d'"usuari" i "contrasenya". Dit d'una altra manera, no seria possible saber inequívocament qui ha accedit al sistema d'informació quan són diverses les persones que coneixen l'"usuari" i la "contrasenya" per accedir-hi. Aquesta actuació, doncs, no seria conforme a l'estipulat a l'article 93.2 del RLOPD, en allò referent al requisit d'exigir una identificació inequívoca i personalitzada.

- D'altra banda, la forma de distribució de les contrasenyes no garanteix la seva confidencialitat. En efecte, les contrasenyes són conegudes per més d'una persona, atesa la manera en què aquestes es distribueixen o donen a conèixer (mitjançant l'eina de gestió CLIPPERZ). Aquesta actuació seria contraria a allò que preveu l'article 93.3 del RLOPD, en allò referent al requisit de confidencialitat.

D'acord amb el que s'ha exposat, es considera acreditat que el Departament de Territori i Sostenibilitat va vulnerar el principi de seguretat de les dades, la qual cosa és constitutiva d'una infracció tipificada com a greu a l'article 44.3.h) en relació amb l'article 9, ambdós de la LOPD, i 93 del RLOPD.

Quart.- L'article 21 de la Llei 32/2010, en consonància amb l'article 46 de la LOPD, preveu que quan les infraccions siguin comeses per una administració pública, la resolució que declari la comissió d'una infracció, haurà d'establir les mesures que escau adoptar perquè cessin o es corregeixin els efectes de la infracció. En el cas que ens ocupa, l'entitat imputada ha posat de manifest en el seu escrit d'al·legacions a la proposta de resolució que l'eina CLIPPERZ ja no s'utilitza, raó per la qual es considera que no resulta necessària l'adopció de les mesures correctores que proposava la persona instructora a la proposta de resolució. Això, sense perjudici de les facultats d'inspecció d'aquesta Autoritat per tal d'efectuar les verificacions corresponents.

Fent ús de les facultats que em confereixen 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 el Departament de Territori i Sostenibilitat ha comès una infracció greu prevista a l'article 44.3.h) en relació amb l'article 9, ambdós de la LOPD, i 93 del RLOPD, sense que resulti necessari requerir mesures correctores per corregir els efectes de la infracció, de conformitat amb el que s'ha exposat al fonament de dret quart.

Carrer de la Llacuna, 166, 7a. Planta
08018 Barcelona

Segon.- Notificar aquesta resolució al Departament de Territori i Sostenibilitat.

Tercer.- Comunicar aquesta resolució al Síndic de Greuges, 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.

Quart.- Ordenar la publicació de la Resolució al web de l'Autoritat (www.apd.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar de l'endemà de la seva notificació, d'acord amb el que preveu l'article 116 i següents de la Llei 30/1992 o bé interposar directament recurs contenciós administratiu davant els Jutjats del Contenciós Administratiu, en el termini de dos mesos a comptar de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per a la defensa dels seus interessos.

La directora

M. Àngels Barbarà i Fondevila

Barcelona, 21 de març de 2014