Procedimiento Nº AP/00001/2019

RESOLUCIÓN: R/00237/2019

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00001/2019**, instruido por la Agencia Española de Protección de Datos a la ***DIRECCION GENERAL DE LA POLICIA***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 5 de noviembre de 2018 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación con la información difundida en medios de comunicación sobre posibles accesos a datos de ficheros policiales del Ministerio del Interior, que denotaría un posible incumplimiento de medidas de seguridad sobre los citados ficheros.

SEGUNDO: Por los Servicios de Inspección de esta Agencia se practican diligencias de investigación teniendo conocimiento de lo siguiente:

1- Se han examinado las publicaciones en prensa (EL PAIS, LA VOZ DE GALICIA, LAS PROVINCIAS, EL DIARIO, EL MUNDO, LA VANGUARDIA), constatándose lo siguiente:

1.1 Diferentes medios publican información sobre accesos a bases de datos policiales por parte de A.A.A. en el marco del Proyecto Pintor, para recabar supuestamente información de un empresario y un abogado.

1.2 Para acceder a esta información se valió de otros dos policías, que son mencionados en los artículos publicados como un subinspector de lucha antiterrorista y un agente de seguridad ciudadana de Granada.

En concreto, en la información sobre la denominada Operación Tándem, se menciona que dos los agentes ayudaron a A.A.A. sin ser descubiertos, realizando accesos cuatro bases de datos:

a la aplicación ARGOS que engloba varias bases de datos policiales,

a SIDENPOL (Sistema de Información de Denuncias Policiales),

a Control de Hospederías,

a Entradas y Salidas de España.

1.3 Se menciona que las consultas a ARGOS y a SIDENPOL se realizaron entre marzo y abril de 2017.

1.4 No se han encontrado en los artículos publicados los nombres de los agentes que realizaron las consultas en los ficheros policiales, ni los del empresario o el abogado sobre los que se realizaron las citadas consultas.

2 -Con fecha 22 de noviembre de 2018 se ha girado una visita de inspección al Centro de Proceso de Datos de la Dirección General de la Policía ubicado en El Escorial, Madrid, realizando sus representantes las siguientes manifestaciones:

1. La Dirección General de la Policía es titular de los ficheros policiales denominados PERSONAS y OBJETOS, en los cuales se registra la información relativa a personas y objetos de interés policial. La gestión de dichos ficheros se realiza mediante sendas aplicaciones con las mismas denominaciones: PERSONAS y OBJETOS.

   La información contenida en estos ficheros se actualiza (alta, bajas y modificaciones) por el personal autorizado del Cuerpo Nacional de la Policía utilizando dichas aplicaciones informáticas. La información contenida en los ficheros que cumple determinados requisitos pasa a la Base de Datos de Señalamientos Nacionales (BDSN), y en los casos procedentes, se eleva al SIS.

2. Así mismo, las distintas unidades de la Policía Nacional disponen de una aplicación denominada ARGOS que les permite realizar consultas sobre los ficheros policiales, entre los que se encuentran: PERSONAS, OBJETOS, BDSN y SIS.

   La aplicación ARGOS además gestiona otras bases de datos como la de movimientos de personas que incorpora, entre otros, los datos de los viajeros facilitados por las compañías aéreas y los datos de personas alojadas en establecimientos hoteleros o control de Hospederías.

3. Las aplicaciones ARGOS, PERSONAS y OBJETOS disponen de un control de acceso formado por un identificador de usuario (DNI del funcionario) más una clave y una contraseña de 8 caracteres alfanuméricos que deben ser cambiados periódicamente.

4. Respecto de la gestión de usuarios:

a) La Dirección General de la Policía ha desarrollado una aplicación denominada GESACCES para la gestión de altas, bajas y modificación de los usuarios autorizados para acceder a los ficheros policiales. Esta aplicación, a su vez, dispone de un control de acceso formado por un identificador de usuario (DNI del funcionario) más una clave y una contraseña de 8 caracteres alfanuméricos que deben ser cambiados periódicamente.

b) En cada Jefatura Superior de cada provincia y en cada Comisaría General existe un Delegado TIC con autorización de acceso a la aplicación GESACCES y son los encargados de tramitar las solicitudes de alta, baja y modificaciones de los usuarios autorizados a acceder a las aplicaciones. Dicha autorización es solicitada para cada persona destinada en la correspondiente unidad por los Jefes Superiores de Policía a nivel provincial o por los Comisarios Generales a nivel central. La solicitud incluye la información del perfil de usuario necesario para el puesto de trabajo que va a desarrollar.

c) En la aplicación GESACCES han sido definidas una serie de plantillas para los distintos perfiles de usuario, las cuales determinan los subsistemas a los que se puede tener acceso en cada una de las aplicaciones, de manera que los usuarios una vez identificados solo verán los menús a los que tienen acceso.

d) Asimismo, GESACCES dispone de un módulo de auditoria que registra los accesos realizados a dicha aplicación para la consulta, alta, baja o modificación de las autorizaciones de acceso a las aplicaciones policiales. Dicho registro contiene los siguientes campos: Usuario que accede, aplicación, programa, DNI consultado, fecha de conexión, hora de conexión, terminal y observaciones. En el campo observaciones se describen los cambios que se han realizados en los datos del usuario accedido (alta, baja o modificación).

e) Cuando un usuario cambia de destino o puesto de trabajo, o causa baja, el sistema de gestión de personal procede a dar de baja automáticamente las autorizaciones de acceso a los sistemas, debiendo solicitarse las nuevas autorizaciones en el nuevo destino.

5. Respecto del Registro de Accesos:

a) Todos los accesos realizados a todas estas aplicaciones quedan registrados en un fichero de log (registro de accesos) que almacena las siguientes categorías de datos: identificación de usuario, fecha de consulta (fecha y hora), plantilla asignada al usuario, terminal, operación (motivo del acceso), criterio (parámetros de búsqueda), aplicación (aplicación informática utilizada para el acceso).

b) La Dirección General de la Policía ha desarrollado una aplicación denominada CAUPOL que garantiza, entre otras, la posibilidad de determinar, respecto a los usuarios de las aplicaciones, qué datos han sido solicitados, en qué momento, por quién y con qué fin. También quedan registrados los accesos a la propia CAUPOL.

c) La aplicación CAUPOL requiere el mismo control de acceso formado por un identificador de usuario (DNI del funcionario) más una clave y una contraseña de 8 caracteres alfanuméricos que deben ser cambiados periódicamente.

d) Todos los usuarios con acceso a los sistemas de información de la Policía Nacional tienen un acceso básico autorizado a la aplicación CAUPOL al objeto de hacer verificaciones. Cada usuario puede consultar exclusivamente sus propios accesos, con el fin de realizar las comprobaciones oportunas (por ej: que no se han utilizado su identificación durante periodos en los que ha estado ausente).

   El sistema únicamente permite el acceso on-line a los registros que se han generado en los dos últimos años. Las copias de seguridad de CAUPOL se conservan indefinidamente.

e) La Unidad de Asuntos Internos de la Policía dispone de acceso total, autorizado en el ámbito de sus competencias, a la aplicación CAUPOL pudiendo auditar los accesos de todos los usuarios.

   El Secretario General de cada Comisaría General dispone de acceso a CAUPOL pudiendo supervisar los accesos del personal asignado a su Comisaría General.

   En cada Jefatura Superior de Policía existe una Unidad de Cooperación Territorial (UCOT) con acceso a CAUPOL pudiendo supervisar los accesos de todos los usuarios de la correspondiente Comunidad Autónoma.

   En cada provincia existe una Unidad de Cooperación Provincial (UCOP) con acceso a CAUPOL pudiendo supervisar los accesos de todos los usuarios de la correspondiente provincia.

   Asimismo, el administrador del Sistema dispone de acceso a CAUPOL a nivel técnico.

f) **No se realiza ninguna explotación preventiva de los registros de accesos**. Solo cuando ocurre un incidente determinado, se analiza la información contenida en el fichero CAUPOL. Así mismo, se revisa dicha información para dar contestación a las solicitudes de autoridades judiciales o en el transcurso de alguna investigación.

   No se realizan revisiones de la información de control registrada en los ficheros de logs, ni se elaboran informes periódicos sobre los mismos.

6. Durante la inspección realizada, los inspectores actuantes solicitaron acceso a la investigación realizada con ocasión del procedimiento judicial al que hacen referencia los medios de comunicación, con relación a posibles accesos a ficheros policiales por el A.A.A. y por parte de dos funcionarios (un subinspector de lucha antiterrorista y un agente de seguridad ciudadana de Granada) que supuestamente colaboraron con él.

Los representantes de la Dirección General de la Policía manifestaron no poder facilitar dicha información, desconociendo si existe un informe de investigación sobre los accesos registrados.

Indicaron que para acceder a los datos registrados sobre los posibles accesos es necesario conocer al menos los nombres de los funcionarios que accedieron, o la identificación de las personas u objetos accedidos, así como los rangos de fechas de los accesos.

Manifestaron que se registran aproximadamente un total de 5.000.000 de consultas al mes a través de la aplicación ARGOS y unas 2.000.000 de consultas al fichero SIDENPOL, por un total aproximado de 30.000 usuarios, no solo del Cuerpo Nacional de Policía, sino de otros organismos ajenos como Guardia Civil, Instituciones Penitenciarias, Cuerpos y Fuerzas de Seguridad autonómicas, etc., lo que introduce una gran complejidad a posible explotación de los registros de auditoria.

7. Los inspectores de la Agencia solicitaron también el estado del usuario de A.A.A..

Se comprobó que en la aplicación GESACCES aparecen los campos de fechas con valor cero, que, según manifestaciones de los representantes de la Dirección General de la Policía, significa que posiblemente no ha tenido nunca autorización de acceso en los actuales sistemas.

Se comprobó que en el fichero de sincronización entre el fichero de personal con los ficheros de gestión de identidades y el directorio LDAP (directorio activo de usuarios de los Sistemas de Información de la organización, que permite o deniega de forma unificada el acceso a los mismos), de fecha 22/06/2016, aparece el pase a la situación de jubilado. Se comprobó que en el fichero de personal (SIGESPOL) como fecha de jubilación figura 22/06/2016.

TERCERO: Con fecha 11 de enero de 2019**,** la Directora de la Agencia Española de Protección de Datos, acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a DIRECCION GENERAL DE LA POLICIA con arreglo a lo dispuesto en el artículo 46 de LOPD, por la presunta infracción del artículo 9 de dicha norma en relación con el artículo 103.5 del RDLOPD, tipificada como grave en el artículo 44.3 j) de la citada Ley Orgánica.

CUARTO: En fecha de 28/01/2019 la DIRECCION GENERAL DE LA POLICIA presento escrito de alegaciones en el que manifestaba, en síntesis, lo siguiente:

Que la explotación preventiva de los registros de accesos en los términos previstos en el artículo 103.5 RDLOPD están recogidas en el procedimiento "PRO-6.5.20-N3-DGP-Monitorizacion de los Sistemas" que forma parte de la Política de Seguridad de la Información de la DGP. (ANEXO 1)

2. Que en el Plan de Tratamiento de Riesgos se registra el proyecto PR-008: Monitorización y gestión de registros de seguridad para llevar a cabo las acciones necesarias para cumplir con el procedimiento anterior en su punto 4. (ANEXO 2).

3. Que las acciones realizadas para el cumplimiento del proyecto PR-008 son:

a. Reuniones con los diferentes servicios, desarrollo y base de datos, para la estandarización de un formato de log apropiado para un posterior tratamiento en los procesos de inteligencia realizados en el SIEM.

b. Redimensionamiento de la capacidad inicial del SIEM como consecuencia de la estimación de crecimiento de los ficheros de log aportados por los sistemas.

c. Establecimiento de diferentes canales de comunicación para la carga de los ficheros de log, vía SYSLOGS o FTP seguro.

4. Que la previsión para las primeras cargas está planificada para el 18 de febrero del año en curso.

Se adjunta un ANEXO 1 y 2:

ANEXO 1
PRO-6.5.20-N3-DGP-Monitorizacion de los Sistemas
4 revisiones Periódicas
"El Responsable de Sistemas o en quien delegue realizará revisiones periódicas de los registros de accesos, el uso de las cuentas de administrador, alertas y fallos del sistema, reglas de acceso sobre los dispositivos.
La periodicidad de revisión será mensualmente pero siempre adecuándose al nivel de riesgo.
Después de realizar las revisiones se generará un informe, ver Anexo I del presente documento, donde se indicará cuando se ha realizado la revisión, quien ha realizado la revisión y cuál ha sido el dispositivo afectado en la revisión. Dicho informe será enviado al Responsable de Seguridad de la Información para su revisión."

En el **ANEXO 2 PR-008: Monitorización y gestión de registros de seguridad**, figura en el apartado *TIEMPO DE EJECUCION: Fecha estimada de inicio: 2019 y Fecha estimada de fin: 2021.*

Asimismo, figura la siguiente información:

Objetivo:

La presente actividad tiene por objetivo revisar y gestionar en la DGP los registros de seguridad, conforme a los criterios de seguridad que derivan del nivel de clasificación de los activos.

Esta actividad afectará a todos los activos tecnológicos relacionados con los sistemas de información de la DGP que estén implicados.

Justificación:

El ENS exige tener monitorizados todos los eventos de seguridad de los sistemas de categoría ALTA, ya sea para la detección de intrusos como para el desempeño de la actividad del sistema en temas de seguridad. Por esto se hace necesaria la ejecución de la presente actividad.

En el caso de la DGP, al existir requisitos de nivel alto en trazabilidad se hace indispensable revisar que todos los sistemas identificados registran todos los puntos que el ENS solicita en este punto, así como la activación de los registros de auditoría que no estuviesen activos y fuese necesario activar, debido a este motivo, además es necesario aumentar las capacidades de monitorización de los sistemas de información de la DGP y de gestión integral de incidentes de seguridad TIC.

QUINTO: Con fecha **12/03/2019** se acordó por el Instructor del procedimiento la apertura de un período de práctica de pruebas, según lo dispuesto en el artículo 77 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, practicándose las siguientes:

1. Se dan por reproducidos a efectos probatorios los documentos obtenidos y generados por los Servicios de Inspección y el Informe de actuaciones previas de Inspección que forman parte del expediente E/06483/2018.

2. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio AP/00001/2019 presentadas por DIRECCION GENERAL DE LA POLICIA, y la documentación que a ellas acompaña.

3. En relación con el contenido de las alegaciones formuladas por la DIRECCION GENERAL DE LA POLICIA en su apartado 3 y 4, se solicita que, en el plazo de quince días hábiles, se aporte la siguiente información:

   3.1 Información completa sobre la planificación prevista de las acciones/revisiones (PR-008: Monitorización y gestión de registros de seguridad) que manifiestan se van a realizar que incluya alcance, extensión y periodicidad de las revisiones.

SEXTO: Mediante escrito de fecha de entrada 01/04/2019, la DIRECCION GENERAL DE LA POLICIA presentó la siguiente documentación:

6º.1 ACTA RS. 14/03/2019 que versa sobre la reunión donde se tratan temas relacionados con el seguimiento de acciones con el responsable de seguridad.

Entre otras cuestiones figura en el citado documento lo siguiente:

(…) *A continuación FJG pregunta por el avance de los proyectos identificativos en el plan de tratamiento de riesgos. En ese momento JAF indica el porcentaje del cumplimiento:*

PR-008 MONITORIZACION Y GESTION DE REGISTROS DE SEGURIDAD, 23.08 % completado.

(….) *El Servicio de desarrollo* (…) *les ha señalado las siguientes tareas asi como los plazos.*

1.- Interlocución con responsable del Servicio de Desarrollo – 1 Semana. Completado.

2.- Adecuación y selección de eventos- del 19 de febrero al 1 de septiembre.

3.- Estudio de almacenamiento – del 1 de septiembre al 30 de septiembre.

4.- Elección del método de envío de logs – 1 de octubre al 31 de octubre.

5.- Interconexión de sistemas – del 1 de noviembre al 31 de diciembre.

6.- Implantación del método de envío – del 1 de enero al 31 de enero.

7. Generación de informes y documentación – del 1 de febrero al 28 de febrero de 2020. (…)

6º.2 Se adjunta copia de varios correos electrónicos enviados entre el 8, 14 y 15 de febrero de 2019 relativos a la petición y entrega de logs generados por la aplicación SINDEPOL y PERSONAS.

6º.3 Se adjunta copia de varios correos electrónicos enviados el 27 de marzo de 2019, entre el jefe del Servicio de Seguridad TIC y don A.P.R relativos al cumplimiento de la planificación de tareas relacionadas con el proyecto PR-008: Monitorización y gestión de registros de seguridad.

SEPTIMO: En fecha de 10/04/2019, por el Instructor del procedimiento se emitió Propuesta de Resolución solicitando, que por la Directora de la Agencia Española de Protección de Datos, se emita resolución en la que se acuerde:

(…) PRIMERO: Declarar que el DIRECCION GENERAL DE LA POLICIA ha infringido lo dispuesto en el artículo 9 de la LOPD, tipificada como grave en el artículo 44.3 h) de dicha norma, en relación con lo dispuesto en el artículo 103.5 del RDLOPD.

SEGUNDO: Requerir a DIRECCION GENERAL DE LA POLICIA, para que adopte las medidas de orden interno que impidan que se siga produciendo la infracción del artículo 9 de la LOPD, en relación con el articulo 103.5 RDLOPD, en los términos indicados en el Fundamento de Derecho VIII.

TERCERO: Notificar la Resolución que se adopte al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados.

CUARTO: Comunicar la Resolución que se adopte al Defensor del Pueblo de conformidad con lo establecido en el artículo 46.4 de la Ley Orgánica 15/1999. (…)

OCTAVO: La propuesta de resolución fue notificada en fecha de 10/04/2019, se que conste la presentación de alegaciones en el plazo concedido al efecto.

NOVENO: De las actuaciones practicadas han resultado acreditados los siguientes

HECHOS PROBADOS

UNO. - En fecha de 22/11/2018, se realiza inspección presencial en la DGP donde los representantes que asisten a los inspectores de la Agencia reconocen que

(…) *no se realiza ninguna explotación preventiva de los registros de accesos* (…)

(…) *no se realizan revisiones de la información de control registrada en los ficheros de logs, ni se elaboran informes periódicos sobre los mismos* (…) (folio 37)

DOS. – Mediante escritos de fechas 28/01/2019 y 01/04/2019, la DGP aporta documentación en la que se prevé la implementación de varias medidas de seguridad a través de diversos proyectos, en concreto se aporta lo siguiente:

En el punto 4 del proyecto PRO-6.5.20-N3-DGP-Monitorizacion de los Sistemas, figura lo siguiente: (…) revisiones Periódicas: "*El Responsable de Sistemas o en quien delegue realizará revisiones periódicas de los registros de accesos, el uso de las cuentas de administrador, alertas y fallos del sistema, reglas de acceso sobre los dispositivos.*

La periodicidad de revisión será mensualmente pero siempre adecuándose al nivel de riesgo.

Después de realizar las revisiones se generará un informe, ver Anexo I del presente documento, donde se indicará cuando se ha realizado la revisión, quien ha realizado la revisión y cuál ha sido el dispositivo afectado en la revisión. Dicho informe será enviado al Responsable de Seguridad de la Información para su revisión." (folio 58)

TRES. - La DGP manifiesta que para desarrollar el apartado 4 del proyecto PRO-6.5.20-N3-DGP, se registra el proyecto *PR-008: Monitorización y gestión de registros de seguridad*, que tiene una previsión estimada de tiempo de ejecución de 2019 a 2021. (folio 58 y 59)

CUATRO. - Según consta en el Acta de la reunión celebrada en fecha de 14/03/2019 (folio 68) los plazos y fases de cumplimiento y previsión del proyecto son los siguientes:

1.- Interlocución con responsable del Servicio de Desarrollo – 1 Semana. Completado.

2.- Adecuación y selección de eventos- del 19 de febrero al 1 de septiembre.

3.- Estudio de almacenamiento – del 1 de septiembre al 30 de septiembre.

4.- Elección del método de envío de logs – 1 de octubre al 31 de octubre.

5.- Interconexión de sistemas – del 1 de noviembre al 31 de diciembre.

6.- Implantación del método de envío – del 1 de enero al 31 de enero.

7. Generación de informes y documentación – del 1 de febrero al 28 de febrero de 2020.

CINCO. - En la información aportada por la DGP, en su escrito de 1/04/2019, figura que se ha completado el apartado relativo a, *Interlocución con responsable del Servicio de Desarrollo* que supone un 23.08 % del citado proyecto. (folio 68)

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

La disposición transitoria cuarta de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD en lo sucesivo) determina lo siguiente:

Disposición transitoria cuarta. Tratamientos sometidos a la Directiva (UE) 2016/680

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

III

Determina el **artículo 22** de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD en lo sucesivo), bajo la rúbrica "*Ficheros de las Fuerzas y Cuerpos de Seguridad*", lo siguiente:

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

IV

Determina **el artículo 9 de la LOPD** lo siguiente: "1*. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley*",

Determinan los **artículos 81.3 b)** y **103 apartados 1 a 5** del *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (RDLOPD en lo sucesivo) lo siguiente:

<u>Artículo 81. Aplicación de los niveles de seguridad</u>

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

Artículo 103. Registro de accesos

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados. (el subrayado es de la Agencia Española de Protección de Datos)

V

En el presente caso, ha resultado probado de las actuaciones practicadas que la DIRECCION GENERAL DE LA POLICIA, no ha dado cumplimiento a lo dispuesto en el art. 103.5 del RDLOPD, por cuanto:

- En las actuaciones de inspección presenciales, de fecha 22/11/2018, reconocen que

(…) *no se realiza ninguna explotación preventiva de los registros de accesos* (…)

(…) *no se realizan revisiones de la información de control registrada en los ficheros de logs, ni se elaboran informes periódicos sobre los mismos* (…)

- En la documentación aportada se indica que la existencia del registros y su explotación esta prevista en el punto 4 del proyecto PRO-6.5.20-N3-DGP-Monitorizacion de los Sistemas, y que para llevar a cabo las acciones necesarias para cumplirlo, se registra el proyecto PR-008: Monitorización y gestión de registros de seguridad, que en la actualidad, manifiesta la DGP que se ha cumplido un 23 %, es decir, de 7 apartados que contiene que se sucederán entre el mes de febrero de 2019 y el año 2020 han realizado 1 apartado, relativo a Interlocución con responsable del Servicio de Desarrollo.

Es decir, de lo expuesto hasta ahora no se deduce que exista y este implementado, mecanismo alguno que de cumplimiento a lo dispuesto en el art. 103.5

del RDLOPD, pues únicamente se puede afirmar que la DGP, tiene previsto su implementación con un horizonte temporal de al menos el año 2020.

VI

El RDLOPD de 21 de diciembre de 2007, entró en vigor en tres meses después de su publicación integra en el BOE, que se produjo en fecha de 19 de enero de 2008.

No obstante, lo anterior, en la **Disposición transitoria segunda** bajo la rúbrica "*Plazos de implantación de las medidas de seguridad*" se establece lo siguiente:

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y <u>en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros</u>:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

(…)

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

De lo expuesto, se deduce que han transcurrido tiempo suficiente hasta la actualidad, tanto para generar la obligación de implantación de las medidas de seguridad de nivel alto, *– y en concreto la prevista en el artículo 103.5 RDLOPD -* como para realizar su cumplimiento por parte de los responsables del tratamiento obligados a ello.

De las actuaciones obrantes en el expediente no es posible determinar que la medida indicada este implementada en la actualidad.

No siendo suficiente a los efectos de dar cumplimiento al citado precepto, que exista una "previsión" – dilatada en el tiempo- para su implementación, sino que ya debería existir, lo que constituye la conducta típica, antijuridica y culpable, que se determina a continuación.

VII

El artículo 44.3 h) de la LOPD, considera infracción grave, "*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".* En el presente caso se da la conducta descrita en el citado precepto.

Dispone el Artículo 28 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, bajo la rúbrica de "Responsabilidad" lo siguiente:

"*1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."*

En el presente caso es atribuible la comisión de la infracción a la DGP al menos a título de negligencia culposa, derivado del principio relativo a la sujeción de los poderes públicos al ordenamiento jurídico previsto en el artículo 9 de la Constitución Española y en especial, derivado del tiempo transcurrido desde que la

obligación prevista en el RDLOPD es exigible (ver disposición transitoria segunda parcialmente transcrita ut supra), hasta la actualidad.

VIII

Si bien la *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos*, no ha sido traspuesta al ordenamiento jurídico español, -y de ahí la aplicación de la LOPD y su normativa de desarrollo- , conviene traer a colación, a efectos meramente divulgativos, lo dispuesto en sus artículos 25 y 29 lo siguiente:

(…) Artículo 25 “Registro de operaciones”

1. Los Estados miembros velarán por que se conserven registros de, al menos, las operaciones de tratamiento en sistemas de tratamiento automatizados siguientes: recogida, alteración, consulta, comunicación incluidas las transferencias, combinación o supresión. Los registros de consulta y comunicación harán posible determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales.

2. Dichos registros se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales y en el ámbito de los procesos penales.

3. El responsable y el encargado del tratamiento pondrán los registros de operaciones a disposición de la autoridad de control a solicitud de esta.

(…) Artículo 29 “Seguridad del tratamiento”

1. Los Estados miembros dispondrán que el responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, sobre todo en lo que se refiere al tratamiento de las categorías especiales de datos personales previstas en el artículo 10.

2. Por lo que respecta al tratamiento automatizado, cada Estado miembro dispondrá que el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, ponga en práctica medidas destinadas a:

a) denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos);

b) impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);

c) impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento);

d) impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);

e) garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);

f) garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos (control de la transmisión);

g) garantizar que pueda verificarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento);

j) garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad). (…)

IX

Determina el artículo 46 de la LOPD, bajo la rúbrica “Infracciones de las Administraciones públicas”, lo siguiente:

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los

efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

En el presente caso, se determina como medida a requerir al responsable la siguiente, la realización de un plan de seguimiento de la implementación de medidas mencionadas en el proyecto **PR-008: Monitorización y gestión de registros de seguridad.**

En ese sentido, se solicitará que, con una periodicidad, al menos bimensual, se remita, en el marco del presente expediente, informe de actualización con los avances, desarrollos e incidencias que se vayan produciendo en la ejecución del Proyecto.

Los informes deberán cumplir al menos determinados requisitos:

• Deberán de estar firmados por el responsable del sistema y fechados.

• Deberán de indicar la fecha en la que esté previsto remitir el siguiente informe, que no podrá ser posterior a los dos meses desde el envío del inmediato anterior.

• Deberán utilizarse los mismos términos para describir las tareas que las descripciones utilizadas en la planificación.

• Deberán incluir la actualización de los análisis de riesgos de los que se derivan las acciones planificadas.

• Para cada acción, además del título descriptivo, deberá de incluirse una descripción detallada de las acciones en que cada acción se desagrega, así como sus salidas o resultados y las pruebas que se van a realizar para determinar que funcionan correctamente.

• En relación a las acciones terminadas, deberán de proporcionarse las evaluaciones en las que se valoren sus resultados y la efectividad de las medidas adoptadas.

La entidad investigada no presentó alegaciones a la propuesta de resolución dónde se incluían las medidas que se han descrito *ut supra*.

Vistos los preceptos citados y demás de general aplicación,

la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR que la DIRECCION GENERAL DE LA POLICIA ha infringido lo dispuesto en el artículo 9 de la LOPD, tipificada como grave en el artículo 44.3 h) de dicha norma, en relación con lo dispuesto en el artículo 103.5 del RDLOPD.

SEGUNDO: REQUERIR a DIRECCION GENERAL DE LA POLICIA, para que adopte las medidas de orden interno que impidan que se siga produciendo la infracción del artículo 9 de la LOPD, en relación con el articulo 103.5 RDLOPD, en los términos indicados en el Fundamento de Derecho IX.

TERCERO: **NOTIFICAR** la presente resolución a la DIRECCIÓN GENERAL DE LA POLICIA y al superior jerárquico SECRETARIA DE ESTADO DE SEGURIDAD, MINISTERIO DEL INTERIOR.

CUARTO: **COMUNICAR** la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 114.1 c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de acuerdo con lo establecido en su artículo 123, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos