Expediente Nº: E/06941/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **DIRECCION GENERAL DE LA POLICIA,** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha **11 de abril de 2014**, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.***, Abogado en representación de 24 Magistrados destinados en órganos judiciales de Cataluña (en adelante, los denunciantes), en el que denuncian al Ministerio del Interior y al diario La Razón por la publicación, el día 3 de marzo de 2014, de una noticia titulada "*La conspiración de los 33 jueces soberanistas"* en relación con un manifiesto firmado por Magistrados de diversos tribunales. En el artículo se indica los nombres y apellidos de los comparecientes, su destino como miembros de la judicatura, y acompaña una fotografía de cada uno de ellos que, según manifiestan, no han sido facilitadas al diario por parte de los interesados ni han autorizado para su difusión; alegando al respecto las siguientes circunstancias:

- Que las imágenes están publicadas en color mientras que en el Documento Nacional de Identidad –DNI- original entregado a los interesados están impresas en blanco y negro.
- Que el Real Decreto 1553/2005, de 23 de diciembre, que regula el DNI, establece en el artículo 5.1b) que para tramitar el carnet se debe facilitar una fotografía en color del rostro del solicitante; y el Real Decreto 1586/2009, que modifica dicha disposición establece que el fondo de la fotografía debe ser blanco.
- Que la Ley Orgánica 2/1986, de 13 de marzo, atribuye la expedición y custodia del fichero del DNI al Cuerpo Nacional de la Policía, dependiente del Ministerio del Interior y que el fichero de identificación de los ciudadanos es uno de los ficheros públicos más sensibles, por contener los datos esenciales para la identificación de los ciudadanos, entre los que se encuentra la fotografía en color.
- Que todas las fotografías denunciadas forman parte del fichero de identificación de las personas DNI, gestionado por el Ministerio del Interior, por lo que el diario no ha podido tener acceso, salvo que lo haya realizado a través de alguien que tenía acceso al fichero, que lo ha facilitado al diario La Razón contraviniendo a lo establecido en la Ley Orgánica 15/1999.

Con el escrito de denuncia se aporta la siguiente documentación:

- Páginas 4 y 5 del diario La Razón, del día 3 de marzo de 2014, artículo "*La conspiración de los 33 jueces soberanistas",* en el que consta el nombre, apellidos y puesto ocupado en órganos judiciales entre los que se encuentran los denunciantes. Si bien, en "9" de ellos solamente consta el primer apellido.

- También, asociados a los mismos figura una fotografía en color del rostro de “33” personas, de ellas “28” con fondo en blanco y “5” con el fondo que posiblemente no es blanco.
- Fotocopia de “24” DNI de denunciantes en color si bien la fotografía figura en blanco y negro y el fondo de la misma en blanco.

SEGUNDO: Tras la recepción de aquella denuncia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación. Con fecha 21 de diciembre de 2018, dos Inspectores de la mencionada Subdirección, se personaron en la Subdirección general de Logística de la Dirección General de la Policía, realizando Acta de Inspección en la que se recogen los siguientes hechos, manifestaciones y comprobaciones:

a) Que en la Comisaría de Policía en Cataluña, se elaboró un informe que denominan de inteligencia y que los funcionarios policiales califican de " Nota Interna”, nota informativa número XXX/XXX, en el que constan “33” fotografías correspondientes a los denunciantes, asociadas al nombre, apellidos, DNI, fecha y lugar de nacimiento, nombre de los padres y domicilio. Así mismo, figura el destino profesional de cada uno de ellos en órganos jurisdiccionales y, en algunos casos, otras actividades como docentes, pertenecientes a asociaciones, publicaciones, etc. En dicho informe no consta identificación de la unidad o persona que lo ha realizado.

b) Que la Jefatura Superior de Policía en Cataluña informó a la inspección que no facilitó ningún dato de los denunciantes a medios de comunicación y que el Juzgado de Instrucción nº 22 de Barcelona inició las Diligencias Previas YYY/YYYY, y la Audiencia Provincial de Barcelona aceptó la inhibición a favor del Juzgado de Instrucción nº 15 de Madrid, quien tramita actualmente el Procedimiento: Diligencias Previas RRR/RRRR.

c) Asimismo, de las declaraciones de los funcionarios de policía, realizadas en el Juzgado de Instrucción 22 de Barcelona, Proc. Previas YYY/YYYY K, manifiestan que desconocen cómo pudieron llegar al diario La Razón las fotografías de los denunciantes y que no se realizó una investigación sino un informe de inteligencia, en el que comprobaron la identidad de las personas y que la información la obtuvieron de “fuentes” abiertas.

d) Que los Informes de Actuaciones Previas de Inspección se motiva exhaustivamente que de las 33 fotografías publicadas por el diario La Razón puestas en relación con las fotografías de la Nota Interna, por su formato, su colorido y su configuración se puede concluir que algunas pueden coincidir con el formato de la fotografía que obran en el fichero del DNI; sin embargo, otras fotografías no son coincidentes debiendo ser obtenidas de diferentes medios de difusión, coincidiendo con la versión de la Policía en relación con las fotografías obrantes en su Nota Interna Además, en “9” de las fotografías de los denunciantes solamente consta el primer apellido y en la Nota interna el primer y segundo apellidos.

e) Finalmente señalar que el Juzgado de Instrucción nº 15 de Madrid ha informado, con fecha de 3/12/2015 y de 27/01/2016, en relación con las Diligencias Previas, Procedimiento. Abreviado RRR/RRRR, por denuncia de la publicación de datos personales de los denunciantes en el periódico La Razón lo siguiente:

"…Las actuaciones se encuentran en recurso de Reforma y Subsidiario de apelación interpuesto por las partes denunciantes contra el AUTO de sobreseimiento provisional y archivo de las actuaciones dictado con fecha de 16 de octubre de 2015.." en base, en resumen, a que "…De la instrucción realizada cabe extraer que los hechos investigados son constitutivos de infracción penal, si bien no existen motivos suficientes para atribuir su perpetración a persona alguna determinada a la vista de las declaraciones de los Funcionarios del Cuerpo Nacional de Policía que accedieron a la base de datos de los datos personales de los denunciantes y del Director del periódico La Razón no se deducen identidades que permitan la imputación de los hechos perseguidos a persona determinada alguna, teniendo en cuenta que al Director del medio le ampara el secreto profesional sobre las informaciones que pudieran haber llegado a dicho medio…"

Por todo lo señalado, se procedió al Archivo de las actuaciones, sin perjuicio de que pudiese, en el supuesto de producirse un nuevo pronunciamiento de un órgano jurisdiccional sobre la cuestión analizada, en su caso procederse a la reapertura de las actuaciones ello, sin perjuicio, del instituto de la prescripción.

TERCERO: La resolución de archivo fue recurrida en reposición, siendo desestimado por la Directora de la Agencia Española de Protección de Datos. Los denunciantes interpusieron recurso contencioso administrativo ante la Audiencia Nacional.

CUARTO: La Audiencia Nacional dictó sentencia, de fecha 30 de mayo de 2018, Procedimiento Ordinario 0608/2016, estimando el recurso contencioso-administrativo frente a la Resolución de la Agencia Española de Protección de Datos (AEPD), de fecha 17 de marzo de 2016, que declaraba el archivo del expediente de actuaciones previas E/01860/2015, y confirmada en recurso de reposición RR/0302/2016, de fecha 30 mayo de 2016, resolviendo *que debe anularse la resolución que se impugna para que la AEPD realice una completa investigación de los hechos denunciados, y una vez finalizada adopte la resolución que considere procedente.*

En los fundamentos de derecho de la Sentencia se señala lo siguiente:

> *La denuncia que los recurrentes presentaron ante la AEPD era frente al Ministerio del Interior y el Diario La Razón, por la publicación en dicho periódico de una noticia en donde aparecían datos personales de los recurrentes con fotografías que se presumían obtenidas a partir de los ficheros de dicho Ministerio y que, en el escrito de demanda, solicita la parte actora que se reabra la investigación por posible vulneración, de diversos preceptos de la Ley Orgánica 15/1999 (en adelante, LOPD), entre ellos el artículo 9 de la misma.*
>
> *La resolución adoptada por el Juzgado de Instrucción 15 de Madrid, que acordó el archivo provisional de las actuaciones, por no poder atribuir a ninguna persona determinada los hechos investigados. Nótese que los hechos investigados en vía penal, eran exclusivamente la publicación de datos personales de los denunciantes en un medio de comunicación, acompañados de sus fotografías que, según declara el Juzgado, "son coincidentes con las utilizadas para la confección por parte de los Servicios y Fuerzas de seguridad del estado del DNI" y que el órgano judicial consideraba que de la instrucción realizada "cabe extraer que los hechos investigados son constitutivos de infracción penal", añadiendo que "no se*

deducen identidades que permitan la imputación de los hechos perseguidos a persona determinada alguna, teniendo en cuenta que al Director del medio le ampara el secreto profesional".

En ninguna de las resoluciones dictadas por la AEPD se menciona la existencia de ninguna actividad investigadora respecto del deber de custodia y de la posible vulneración del artículo 9 de la LOPD denunciada. Dicho precepto, relativo a la Seguridad de los Datos, dispone:

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….*
2. *Por su parte el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 1720/2017 (en adelante, RLOPD), en sus artículos 79 a 114, establece con cierta minuciosidad las medidas de seguridad en el tratamiento de datos de carácter personal aplicables a ficheros y tratamientos automatizados, que califica como medidas de nivel básico, medio o alto.*

A la vista de lo expuesto y de los preceptos aplicables al supuesto que se enjuicia, la AEPD ha realizado una investigación, y ha procedido a realizar determinadas actuaciones en averiguación de los hechos denunciados (incluso en dos momentos temporales distintos), es parecer de la Sala que dichas actuaciones han sido solo parciales, y se concretaron en uno de los aspectos de las supuestas vulneraciones denunciadas, como es la autoría de la filtración, respecto de la que, al no existir autor conocido, llevó al Juzgado de Instrucción de Madrid a decretar el sobreseimiento provisional, y a continuación la AEPD, con esta misma fundamentación, al archivo de la denuncia.

QUINTO: Tras la recepción de la Sentencia, la Subdirección General de Inspección de Datos procedió a la realización de las actuaciones solicitadas, teniendo conocimiento de los siguientes extremos:

De las actuaciones realizadas en el Área de Informática de la Dirección General de la Policía (en adelante, DGP) y de la documentación recabada en las mismas, todo ello referente a las medidas de seguridad en el tratamiento de datos de carácter personal establecidas en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), y en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), del sistema de información del Documento Nacional de Identidad (en adelante, DNI), denominado fichero ADDNIFIL, se desprende lo siguiente:

El Sistema de Información del DNI tiene como finalidad la gestión de la identificación de los ciudadanos españoles y la procedencia de los datos son las solicitudes de expedición o renovación del documento facilitadas por los propios ciudadanos.

La estructura del fichero se compone de los siguientes datos: identificativos (filiación), personales (fotografía, firma manuscrita y huellas), relativos a la expedición del documento y datos incorporados electrónicamente en el chip. El

sistema de tratamiento es totalmente automatizado desde el año 2006 y el nivel de seguridad exigible según el Reglamento de Medidas de Seguridad es Alto.

El órgano responsable del fichero es la División de Documentación de la DGP y los destinatarios de las comunicaciones previstas son las Fuerzas y Cuerpos de Seguridad del Estado (excluido Policía Local), Órganos judiciales, Defensor del Pueblo y las Administraciones Públicas.

En relación con el Documento de Seguridad que contiene las medidas de índole técnica y organizativa implementadas en el sistema de información:

El DNI electrónico fue desarrollado en el año 2006; no obstante, de conformidad y al amparo de le dispuesto en el Reglamente de Medidas de Seguridad se elaboró en el año 2004 la versión 1.0 del documento en el que se recogen las medidas que garantizan la confidencialidad e integridad de la información automatizada y no automatizada. Dicho documento ha sido revisado en cinco ocasiones, siendo la versión 3.3 la correspondiente a enero del 2017. Al ser un documento en el que se realizan actualizaciones periódicamente por parte del Responsable de Seguridad y aprobadas por el responsable del fichero solamente se dispone de la última versión.

Los diferentes apartados del documento hacen referencia a ordenes, procedimientos, normas, informes, manuales o instrucciones, en los que se desarrollan y actualizan los aspectos referenciados en los mismos, que se encuentran disponibles en el repositorio común de la DGP, de tal forma que todos los documentos puedan identificarse y definirse unívocamente.

La existencia del Documento de Seguridad ha sido puesta en conocimiento de todo el personal, interno y externo, con acceso a los datos automatizados y no automatizados de carácter personal de la DGP.

En el año 2009 se creó el Comité de Seguridad de la Información, órgano interdisciplinar, cuyo objetivo es proveer una dirección clara y estratégica destinada a promover y coordinar la seguridad de la información en el ámbito de la DGP.

Se ha recabado *Documento de Seguridad del fichero ADDDNIFIL* y diversa documentación de procedimientos y normas que lo desarrollan como Definición del Sistema de Gestión de la Seguridad de la Información y control de acceso Físico.

Con respecto a las **funciones y obligaciones del personal** con acceso al sistema de información:

Los usuarios a los que se les proporciona acceso a los sistemas de información de la DGP deben suscribir el documento *Compromiso de confidencialidad* para garantizar el tratamiento adecuado de la información de acuerdo con la legislación vigente, en el que constan, entre otras, las siguientes cláusulas:

1. *Que conozco los principios básicos que rigen la protección de la información en el CNP, la legislación aplicable y el marco normativo de seguridad de la información del Área de Informática del CNP, y que me comprometo a respetarlos.*
2. *Que me comprometo, asimismo:*

a) A mantener el más estricto secreto —incluso una vez extinguida mi relación con el CNP— sobre cualquier información a la que pueda tener acceso, en forma escrita o verbal, referente y/o perteneciente al CNP.

b) A limitar mi acceso a los datos y a las operaciones que sean imprescindibles para la finalidad de desempeñar las funciones profesionales correspondientes a mi puesto.

c) A no tratar, ceder, comunicar o utilizar en beneficio propio y a no revelar a terceras personas los datos de carácter personal a los que tenga acceso, y también a respetar en todo momento la privacidad y la confidencialidad de esos datos.

d) A no acceder a datos correspondientes a las personas siguientes, salvo que obtenga el consentimiento expreso de la persona titular de sus datos:

personas con cualquier tipo de relación con el usuario (familiar, laboral, etc.);

personas conocidas públicamente o con posible interés público.

3. *Que declaro que conozco y acepto el hecho de que mi acceso al sistema será monitorizado, de conformidad con el artículo 103 del Real Decreto 1720/2007".*

En la pantalla inicial de la intranet de la DGP figura una pestaña *Seguridad T.I.C.* (Tecnologías de la Información y las Comunicaciones) en la que se despliega una relación de documentos sobre seguridad de la información como: Procedimiento sobre el buen uso de los recursos TIC, Manual de seguridad de la información, Normativa de seguridad, etc.

Se ha recabado diversa documentación relativa a instrucciones y procedimientos sobre: seguridad de la información, el buen uso de los recursos y funciones y obligaciones del personal.

Con respecto al **registro de incidencias** que afecten al sistema de información:

La notificación y gestión de las incidencias que afectan a los datos de carácter personal se registran por medio de una herramienta en la que es necesario reflejar, entre otros, los siguientes datos: fecha y hora, persona que realiza la notificación, resumen y consecuencias.

Las incidencias se reportan al Centro de Atención al Usuario (CAU) que es el encargado de su clasificación, asignación del usuario que la atiende, medidas correctoras y resolución o traslado a la unidad responsable de resolverla.

Los hechos objeto de investigación en las presentes actuaciones no fueron notificados al registro de incidencias ya que no se realizaron accesos indebidos al fichero ADDNIFIL.

Se ha verificado que en el registro de incidencias constan registradas "400" notificaciones asociadas al criterio "DNI" la mayoría por problemas del equipamiento físico.

En relación con el **control de acceso** y las medidas de **identificación y autenticación** de los usuarios con acceso a datos de carácter personal:

Las directrices y procedimientos para controlar el acceso a los sistemas de información se encuentran aprobados por el Comité de Seguridad y constan en la "*Norma.11"* que detalla las responsabilidades de los usuarios, la gestión de los privilegios y contraseñas, el control de acceso a redes, a aplicaciones, a equipos móviles y teletrabajo.

La DGP ha desarrollado una aplicación denominada GESACCES para la gestión de altas, bajas y modificación de los usuarios autorizados para acceder a los ficheros policiales que a su vez dispone de un control de acceso.

En cada Jefatura Superior de cada provincia y en cada Comisaría General existe un delegado TIC con autorización de acceso a la aplicación GESACCES que son los encargados de tramitar las solicitudes. La solicitud incluye la información del perfil de usuario necesario para el puesto de trabajo que va a desarrollar.

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 se visualizaran los menús a los que tienen acceso. Asimismo, la aplicación dispone de un módulo de auditoría que registra los accesos realizados a la misma.

Cuando un usuario cambia de destino o puesto de trabajo, 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.

En el caso de los usuarios que requieren acceso al fichero del DNI, son autorizados por la División de Documentación. En la actualidad están autorizados a acceder nivel de gestión: personal de la División de Documentación: Oficinas de documentación integradoras de los equipos de expedición del DNI y pasaporte con un total de 4.800 usuarios. Con perfil de consulta de investigación, de manera muy restrictiva, policía judicial, científica y de información, seguridad ciudadana y otros, con un total de unos 1.500 usuarios, si bien existen dos niveles, la mayoría de los usuarios con perfil que no pueden acceder a las fotografías.

Se ha recabado diversa documentación relativa a control de acceso y perfiles de usuarios la más antigua data del año 2010.

En relación con las **copias de respaldo y recuperación** de los datos de carácter personal:

El procedimiento de actuación para la realización de las copias de seguridad, así como de recuperación, que garanticen la reconstrucción del fichero ADDNIFIL se encuentran documentadas y son controladas por el personal de la sección de sistemas del Centro de Proceso de Datos.

Para la realización de las copias de respaldo se utiliza una herramienta específica y existen dos niveles:

Copia completa en dos soportes cada viernes, que se conservan trece días en ubicaciones especiales y una de ellas se traslada por personal del centro fuera de las instalaciones.

Copia incremental en dos soportes cada día laborable que se conservan ocho días.

El procedimiento de recuperación debe ser autorizada por el Jefe del Proyecto y posteriormente se solicitará a la sección de sistemas para que ejecute el proceso. En el caso del fichero ADDNIFIL debe ser autorizada por el responsable del fichero.

Se ha recabado diversa documentación relativa a los procedimientos de copias de respaldo y recuperación de la información la más antigua de enero de 2012.

Con respecto a la realización de **auditorías** internas o externas que verifiquen el cumplimiento de las medidas de seguridad:

La DGP realiza auditorias de seguridad de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, internas o externas, conforme a la normativa y a los estándares vigentes en cada momento y, en concreto, del fichero del DNI la primera se realizó en el primer semestre de 2012.

En junio del 2012 se realizó auditoria UNE-ISO/IEC 27001:2007 llevada a cabo por un equipo auditor de la Asociación Española de Normalización y Certificación (AENOR), en la cual, además de los puntos fuertes, se incluyeron las recomendaciones sobre las mejoras a implantar. También, en febrero de 2011, AENOR Certifica que la DGP dispone de un sistema de gestión de seguridad de la información conforme con la citada norma.

Por otra parte, en noviembre de 2013, se realizó un *análisis de riesgos*, con la herramienta PILAR, la cual se basa en la Metodología de análisis y gestión de riesgos de los sistemas de información del Ministerio de Administraciones Públicas, con el propósito de determinar cuáles de los activos de los sistemas de información (como el fichero del DNI) tienen mayor vulnerabilidad.

Se ha recabado diversa documentación relativa a informes de auditorías, relación de auditorías desde 2011 a enero de 2019, análisis de riesgos y plan de acción y diagnóstico del cumplimiento del Esquema Nacional de Seguridad.

En relación con el **registro de accesos** del sistema de información que contenga datos de carácter personal:

Todos los accesos al fichero ADDNIFIL (consultas, altas, bajas, actualizaciones) se guardan en un fichero de log (registro de accesos) que almacena las siguientes categorías de datos: identificación de usuario, fecha y hora, plantilla asignada al usuario, terminal, operación (motivo del acceso), criterio (parámetros de búsqueda), aplicación (aplicación informática utilizada para el acceso).

El registro de accesos contiene información desde el año 1998 y tiene implementadas ciertas alarmas automáticas con objeto detectar accesos que podrían ser irregulares, además, desde 2015 la División de Documentación realiza una explotación proactiva de dicha información.

Con respecto a las medidas de seguridad aplicables a ficheros y tratamientos no automatizados:

En el *Documento de controles y pruebas de control de acceso y usuarios* se detallan las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos, los ficheros, los centros de tratamiento, locales, equipos, sistemas (automatizados o no), programas y las personas que intervienen en los tratamientos, sujetos al régimen de aplicación de la LOPD.

En dicho documento se detalla que para los ficheros no automatizados les será de aplicación las medidas que serán similares que para los automatizados, entre otros, lo relativo a las funciones y obligaciones del personal y el control de accesos. Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

También, se indica en el documento los controles realizados a los dispositivos de almacenamiento que se encuentran en áreas de acceso restringido.

Por parte de la Inspección de Datos se ha verificado que fueron realizadas consultas al fichero ADDNIFIL, los días 13 y/o 14 de febrero de 2014, por funcionarios de la Brigada de Información de Barcelona, al menos, a seis personas cuyo DNI coincide con los denunciantes. Los funcionarios que realizaron las consultas estaban autorizados por el perfil de acceso según las funciones que desempeñaban en su puesto de trabajo.

También, se ha constatado que para cada consulta que se realiza al fichero ADDNIFIL es necesario facilitar al sistema el motivo de la misma.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

La Sentencia de la Audiencia Nacional indica que no ha existido ninguna actividad investigadora respecto al deber de custodia de los datos personales de los denunciantes y de la posible vulneración del artículo 9 de la LOPD, que era uno de los hechos denunciados, y distinto de la autoría de la filtración que fue denunciado ante la jurisdicción penal. Estas actuaciones se realizaron para comprobar las medidas de seguridad que tenía implantadas la Dirección General de la Policía en el momento en que se produjeron los hechos denunciados, y relacionadas con el sistema de información del DNI, denominado fichero ADDNIFIL.

El artículo 9 de la LOPD, referido a la seguridad de los datos dispone 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.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. En este caso, el fichero del sistema de información del Documento Nacional de Identidad (en adelante, DNI), denominado fichero ADDNIFIL, tiene como finalidad la gestión de la identificación de los ciudadanos españoles y la procedencia de los datos son las solicitudes de expedición o renovación del documento facilitadas por los propios ciudadanos. El sistema de tratamiento es totalmente automatizado desde el año 2006 y el nivel de seguridad exigible según el Reglamento de Medidas de Seguridad es Alto.

El Artículo 88 del Reglamento de desarrollo de la LOPD determina, en referencia al documento de seguridad, lo siguiente:

"1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización…

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal."

En relación con el Documento de Seguridad**,** éste se elaboró en el año 2004, y se recogen las medidas que garantizan la confidencialidad e integridad de la

información automatizada y no automatizada. Este documento ha sido revisado en cinco ocasiones, siendo la última versión la correspondiente a enero del 2017.

Como se ha indicado de forma pormenorizada en los Antecedentes de esta Resolución, los apartados del documento hacen referencia a ordenes, procedimientos, normas, informes, manuales o instrucciones, en los que se desarrollan y actualizan los aspectos referenciados en los mismos, que se encuentran disponibles en el repositorio común de la DGP, de tal forma que todos los documentos puedan identificarse y definirse unívocamente.

La existencia del Documento de Seguridad se puso en conocimiento de todo el personal, interno y externo, con acceso a los datos automatizados y no automatizados de carácter personal de la DGP.

En el año 2009 se creó el Comité de Seguridad de la Información, órgano interdisciplinar, cuyo objetivo es proveer una dirección clara y estratégica destinada a promover y coordinar la seguridad de la información en el ámbito de la DGP.

III

El artículo 89 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, determina lo siguiente:

"1. Las funciones y obligaciones de cada *uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.*

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento".

Relacionado con esta obligación, durante la visita de inspección se pudo verificar que los usuarios a los que se les proporciona acceso a los sistemas de información de la DGP suscriben el documento *Compromiso de confidencialidad* para garantizar el tratamiento adecuado de la información de acuerdo con la legislación vigente.

Además, para recordarlo y tenerlo accesible, en la pantalla inicial de la intranet de la DGP figura una pestaña *Seguridad T.I.C.* (Tecnologías de la Información y las Comunicaciones) en la que se despliega una relación de documentos sobre seguridad de la información como: Procedimiento sobre el buen uso de los recursos TIC, Manual de seguridad de la información, Normativa de seguridad, etc.

Se han dictado instrucciones y procedimientos sobre: seguridad de la información, el buen uso de los recursos y funciones y obligaciones del personal.

El artículo 90 del Real Decreto mencionado indica:

"Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso,

detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas".

La DGP, en relación con el sistema de información objeto de inspección, registra la notificación y gestión de las incidencias que afectan a los datos de carácter personal por medio de una herramienta en la que es necesario reflejar, entre otros, los siguientes datos: fecha y hora, persona que realiza la notificación, resumen y consecuencias.

Las incidencias se remiten al Centro de Atención al Usuario (CAU) que es el encargado de su clasificación, asignación del usuario que la atiende, medidas correctoras y resolución o traslado a la unidad responsable de resolverla.

En el caso denunciado no se notificó incidencia alguna al no haberse realizado accesos indebidos al fichero ADDNIFIL.

IV

En relación con el control de acceso y la identificación y autenticación de los usuarios, los artículos 91 y 93 del Real Decreto tantas veces mencionado establecen lo siguiente:

"Artículo 91. 1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

La DGP tiene directrices y procedimientos para controlar el acceso a los sistemas de información, los cuales se encuentran aprobados por el Comité de Seguridad, y que detalla las responsabilidades de los usuarios, la gestión de los privilegios y contraseñas, el control de acceso a redes, a aplicaciones, a equipos móviles y teletrabajo. Disponen de una aplicación para gestionar altas, bajas y modificación de los usuarios autorizados para acceder a los ficheros policiales que a su vez dispone de un control de acceso.

En cada Jefatura Superior de cada provincia y en cada Comisaría General hay un delegado TIC y son los encargados de tramitar las solicitudes. La solicitud incluye la información del perfil de usuario necesario para el puesto de trabajo que va a desarrollar.

En la aplicación han definido una serie de plantillas para los distintos perfiles de usuario, de manera que los usuarios una vez identificados solo se visualizaran los menús a los que tienen acceso. Asimismo, la aplicación dispone de un módulo de auditoría que registra los accesos realizados a la misma.

Cuando un usuario cambia de destino o puesto de trabajo, 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.

En el caso concreto de los usuarios que requieren acceso al fichero del DNI, son autorizados por la División de Documentación. En la actualidad están autorizados a acceder nivel de gestión: personal de la División de Documentación: Oficinas de documentación integradoras de los equipos de expedición del DNI y pasaporte con un total de 4.800 usuarios. Con perfil de consulta de investigación, de manera muy restrictiva, policía judicial, científica y de información, seguridad ciudadana y otros, con un total de unos 1.500 usuarios, si bien existen dos niveles, la mayoría de los usuarios con perfil que no pueden acceder a las fotografías.

Mantienen documentación relativa al control de acceso y perfiles de usuarios; siendo la más antigua del año 2010.

V

El artículo 94 de la misma norma especifica lo siguiente:

"1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se

deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad".

El procedimiento de actuación para la realización de las copias de seguridad, así como de recuperación, que garanticen la reconstrucción del fichero ADDNIFIL se encuentran documentadas y son controladas por el personal de la sección de sistemas del Centro de Proceso de Datos.

Para la realización de las copias de respaldo se utiliza una herramienta específica y existen dos niveles:

Copia completa en dos soportes cada viernes, que se conservan trece días en ubicaciones especiales y una de ellas se traslada por personal del centro fuera de las instalaciones.

Copia incremental en dos soportes cada día laborable que se conservan ocho días.

El procedimiento de recuperación debe ser autorizada por el Jefe del Proyecto y posteriormente se solicitará a la sección de sistemas para que ejecute el proceso. En el caso del fichero ADDNIFIL debe ser autorizada por el responsable del fichero.

Mantienen documentación relativa a los procedimientos de copias de respaldo y recuperación de la información la más antigua de enero de 2012.

En cuanto a las auditorías, el artículo 96 del Real Decreto 1720/2007, establece:

"1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas."

La DGP realiza auditorias de seguridad de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, internas o externas, conforme a la normativa y a los estándares vigentes en cada momento y, en concreto, del fichero del DNI la primera se realizó en el primer semestre de 2012.

En junio del 2012 se realizó auditoria en la cual, además de los puntos fuertes, se incluyeron las recomendaciones sobre las mejoras a implantar.

En noviembre de 2013, se realizó un análisis de riesgos, con la herramienta PILAR, la cual se basa en la Metodología de análisis y gestión de riesgos de los sistemas de información del Ministerio de Administraciones Públicas, con el propósito de determinar cuáles de los activos de los sistemas de información (como el fichero del DNI) tienen mayor vulnerabilidad.

La DGP facilitó relación de auditorías desde 2011 a enero de 2019, análisis de riesgos y plan de acción y diagnóstico del cumplimiento del Esquema Nacional de Seguridad.

El artículo 103 regula el Registro de accesos, señalando lo siguiente:

"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.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Todos los accesos al fichero ADDNIFIL (consultas, altas, bajas, actualizaciones) se guardan en un fichero de log (registro de accesos) que almacena las siguientes categorías de datos: identificación de usuario, fecha y hora, plantilla asignada al

usuario, terminal, operación (motivo del acceso), criterio (parámetros de búsqueda), aplicación (aplicación informática utilizada para el acceso).

El registro de accesos contiene información desde el año 1998 y tiene implementadas ciertas alarmas automáticas con objeto detectar accesos que podrían ser irregulares, además, desde 2015 la División de Documentación realiza una explotación proactiva de dicha información.

VI

Asimismo, la DGP tiene incorporadas medidas de seguridad para los ficheros no automatizados, que serán similares que para los automatizados, entre otros, lo relativo a las funciones y obligaciones del personal y el control de accesos. Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura (según establece al artículo 107 del Real Decreto citado). Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada, según indica el artículo 108 de la misma norma.

También, se indica en el documento los controles realizados a los dispositivos de almacenamiento que se encuentran en áreas de acceso restringido.

Se ha verificado que se realizadas consultas al fichero ADDNIFIL, los días 13 y/o 14 de febrero de 2014, por funcionarios de la Brigada de Información de Barcelona, al menos, a seis personas cuyo DNI coincide con los denunciantes. Los funcionarios que realizaron las consultas estaban autorizados por el perfil de acceso según las funciones que desempeñaban en su puesto de trabajo. También, se constató que para cada consulta que se realiza al fichero ADDNIFIL es necesario facilitar al sistema el motivo de la misma.

Tras las actuaciones realizadas por la Inspección de Datos, se ha constatado que la DGP cumplía las medidas de seguridad establecidas en la normativa de protección de datos en el momento de los hechos denunciados y también en el momento actual, ya que ha ido actualizando el documento de seguridad, dictando instrucciones dirigidas al cumplimiento y conocimiento de las medidas de seguridad por parte del personal, y realizando auditorías para verificar el cumplimiento de las medidas.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a la Dirección General de la Policía, y a Don ***A.A.A.***.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa, y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

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