

Expediente Nº: E/03814/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **CONSEJERIA DE JUSTICIA E INTERIOR DE LA JUNTA DE ANDALUCIA** en virtud de denuncia presentada por **A.A.A. Y OTROS**, y teniendo como base los siguientes

HECHOS

PRIMERO: El 25 de marzo tienen entrada en esta Agencia diversos escritos remitidos por D^a. **A.A.A. y 79 firmantes**, en los que se declara lo siguiente:

1. Que se ha instalado un sistema de información denominado JARA para la gestión de archivos judiciales en la Ciudad de la Justicia de Málaga, así como una aplicación denominada LEXNET para el envío de notificaciones telemáticas por parte de los órganos judiciales.
2. Que dicho sistema es utilizado entre otros por el personal del Cuerpo de Auxilio Judicial quienes para su uso deben de utilizar un certificado digital de firma electrónica de forma obligatoria pudiendo optar entre el habilitado para DNI electrónico o el denominado CERTIFICADO DE PERSONA FISICA expedido por la Fábrica Nacional de Moneda y Timbre (FNMT).
3. Que la propia FNMT dispone de otros certificados de firma digital como el que se emite para EMPLEADOS PÚBLICOS, cuya utilización en este caso sería más adecuada, ya que entienden que tanto el DNI electrónico como el CERTIFICADO DE PERSONA FISICA están pensados para su utilización en el ámbito privado de su titular y no en el ámbito profesional derivado de su condición de empleado público.
4. Señalan también la existencia de un riesgo derivado de que la explotación del sistema de información sobre el que actúan dichos certificados digitales se ha externalizado en una empresa privada y que el pliego del concurso para dicha prestación no hace referencia alguna a las medidas de seguridad, limitándose a indicar, de modo genérico, la confidencialidad de los datos de carácter personal, lo que resulta a juicio de los denunciantes insuficiente habida cuenta de que dicho sistema va a albergar datos sensibles de nivel alto como por ejemplo los derivados de procedimientos penales y violencia de genero.
5. Añaden también que se ha vulnerado el art. 20 de la LOPD sobre creación, modificación o supresión de ficheros de titularidad pública ya que el sistema trata datos de los certificados digitales de los empleados y esta circunstancia no se recoge en la disposición de creación de los ficheros a su juicio implicado: TARJETAS CRIPTOGRÁFICAS, USUARIOS, GESTIÓN DE ARCHIVOS.

Junto a la denuncia aporta la siguiente documentación:

Copia de la información albergada en la página web de la Junta de Andalucía sobre administración electrónica y gestión del portafirmas electrónico.

Copia de la información albergada en la página web de la FNMT sobre los diferentes tipos de certificados electrónicos emitidos por dicho organismo.

Copia del Pliego de Prescripciones Técnicas elaborado por la Junta de Andalucía para la contratación del servicio de gestión de la documentación del archivo judicial territorial de Málaga.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

En fecha de 14 de enero de 2015 se solicita información a la CONSEJERIA DE JUSTICIA E INTERIOR de la JUNTA DE ANDALUCIA quien remite escrito de respuesta recibido en fecha de 10 de febrero de 2015 del que se desprende lo siguiente:

1. Respecto del sistema **JARA**:

- 1.1. JARA es un sistema web para la gestión de forma automática de los préstamos y transferencia de información judicial entre el Órgano Judicial y el Archivo de la Sede Judicial.
- 1.2. JARA no contiene información procesal, ésta se encuentra en sistema "ADRIANO", sino las referencias: número de asunto, tipo de procedimiento y su ubicación, es decir, si se encuentra en el archivo o en el propio juzgado. JARA permite también generar los formularios asociados a las peticiones y movimiento de documentación entre los juzgados y el archivo.
- 1.3. JARA es accesible para sus usuarios desde todas las sedes de la red judicial a través del "ESCRITORIO JUDICIAL" y dispone de un control de acceso basado en certificado digital, DNle, o usuario y contraseña. Actualmente JARA está conectado con la plataforma de firma de la Junta de Andalucía "@firma" y se está trabajando en la integración con el Sistema de Gestión Procesal "ADRIANO" para el volcado de la información.
- 1.4. Las entidades intervinientes en el sistema son los Juzgados y el Archivo Judicial Territorial.
- 1.5. Los datos personales que incluye el sistema son: nombre y apellidos de los usuarios en los campos de auditoria de la base de datos, y nombre, apellidos y DNI de los Secretarios Judiciales (como firmantes de documentos) y, en su caso, del personal en quien deleguen la firma.
- 1.6. JARA se encuentra implantado actualmente en diferentes grados en Sevilla, Málaga y Almería y se extenderá en un futuro al resto de provincias de Andalucía.

2. Respecto del sistema **LEXNET**:

- 2.1. LEXNET es una aplicación del MINISTERIO DE JUSTICIA para el intercambio seguro de información a través de Internet entre los órganos judiciales y una gran diversidad de operadores jurídicos para el

- intercambio de documentos judiciales: notificaciones, escritos y demandas.
- 2.2. LEXNET permite el uso de firma electrónica reconocida admitiendo que los usuarios dispongan de los siguientes tipos de certificados digitales instalados en un soporte físico: DNle, FNMT, FNMT APE, FNMT Administración Pública, ACA, CatCert, GVA, ANF, CamerFirma (RACER, Camerales, AAPP).
 - 2.3. LEXNET se encuentra conectado con el Sistema de Gestión Procesal "ADRIANO".
 - 2.4. Las entidades intervinientes en el sistema son:
 - 2.4.1. Órganos judiciales y Oficinas de Registro y Reparto (Secretario Judiciales).
 - 2.4.2. Procuradores y Colegio de Procuradores.
 - 2.4.3. Abogacía del Estado.
 - 2.4.4. Abogacías dependientes de la Abogacía del Estado (FOGASA, SEPES, AEAT y Consorcio Compensación de Seguros).
 - 2.4.5. Abogacía Comunidad. (Gabinete Jurídico)
 - 2.4.6. Abogacía SJSS.
 - 2.4.7. Fiscalías.
 - 2.4.8. Abogados y Colegios de Abogados.
 - 2.4.9. Graduados Sociales
 - 2.4.10. Comisiones de Asistencia Jurídica Gratuita.
 - 2.5. Los datos personales que incluye el sistema son: nombre, apellidos, DNI, rol, entidad, provincia y municipio del usuario.
 - 2.6. LEXNET se encuentra implantado actualmente en diferentes grados en todas las provincias de Andalucía y desde su arranque en 2009 se han realizado a través de dicho sistema un total cercano a 24 millones de notificaciones.
3. Respecto de los ficheros implicados en los sistemas descritos:
 - 3.1. Ficheros declarados por el **CONSEJO GENERAL DEL PODER JUDICIAL**: declarados en el *Acuerdo 20 de septiembre de 2006, del Pleno del Consejo General del Poder Judicial, de creación de ficheros de carácter personal dependientes de los órganos judiciales*, publicado en el BOE número 244 de 12 de octubre de 2006. Estos ficheros son los siguientes:
 - 3.1.1. Asuntos Jurisdiccionales.**
 - 3.1.2. Registro de Asuntos.**
 - 3.1.3. Usuarios.**
 - 3.2. Ficheros declarados por **JUNTA DE ANDALUCÍA**,
 - 3.2.1. **Usuarios**: fichero declarado en la *Orden de 5 de octubre de 2005, de la Consejería de Justicia y Administración Pública, por la que se modifican ficheros automatizados con datos de carácter personal contenidos en las órdenes de 1 de septiembre de 2003 y de 9 de diciembre de 2003.*
 - 3.2.2. **Tarjetas Criptográficas (*****)**: fichero declarado en la *Orden de 1 de septiembre de 2003, por la que se amplía la de 24 de septiembre de 2002, para regular los ficheros automatizados con datos de carácter personal gestionados por la Consejería*, es un fichero en vías de darse de baja, debido a que se creó con el objetivo de dotar de una entidad certificadora que proveyera

certificados digitales propios adscritos a la Junta de Andalucía. Finalmente, la provisión de certificados digitales por parte de la Junta de Andalucía a los usuarios de la Administración de Justicia se realiza mediante un convenio con la FNMT, por lo que no procede la existencia de dicho fichero *Tarjetas Criptográficas*, ya que no se recoge ninguna información salvo la necesaria para la FNMT.

3.3. Ficheros declarados por el **MINISTERIO DE JUSTICIA**,

3.3.1. **Gestión de usuarios del sistema LEXNET** declarado en el *Real Decreto 84/2007, de 26 de enero sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos*.

3.4. Respecto de la externalización de servicios a empresas privadas

3.4.1. Respecto al riesgo derivado de la explotación de los sistemas por empresas privadas externas, dicha externalización puede resultar necesaria para mantener los servicios tecnológicos de la Consejería. No obstante dicho riesgo se encuentra cubierto mediante cláusulas de seguridad y de protección de datos que se incluyen en los pliegos de adjudicación y que se reproducen a continuación:

"11 PROPIEDAD, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

11.1 INFORMACIÓN DE BASE

La Junta de Andalucía facilitará al adjudicatario cuanta información disponga relacionada con las materias objeto del presente trabajo. Toda la información que se proporcione, es propiedad de la Junta de Andalucía y no podrá ser utilizada en futuros trabajos ya sea como referencia o como base de los mismos, a menos que se cuente con la autorización expresa, por escrito, de la Junta de Andalucía.

11.2 CONFIDENCIALIDAD DE LA INFORMACIÓN

La Consejería de Gobernación y Justicia facilitará a la empresa adjudicataria toda la información necesaria para la ejecución de las tareas objeto del presente contrato.

No se podrá transferir información alguna sobre los trabajos a personas o entidades no explícitamente mencionados en este sentido en el contrato sin el consentimiento, por escrito, de la Junta de Andalucía.

Todo el personal de la empresa adjudicataria participante en los trabajos a que se refiere el presente pliego, queda expresamente sometido a la normativa vigente, en cuanto a la confidencialidad e integridad de los datos manejados y la documentación facilitada.

11.3 TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El adjudicatario, en cumplimiento de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", únicamente tratará los datos conforme a las instrucciones de la Consejería, y no los aplicará o utilizará con fin distinto al del contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Además, deberá cumplir las medidas técnicas y organizativas estipuladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de dicha Ley Orgánica 15/1999 y que establece el "Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal". En el caso de que la empresa, o cualquiera de sus miembros, destinen los datos a otra finalidad, los comunique, o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas.

11.4 PROPIEDAD DE LOS DOCUMENTOS, TRABAJOS E INFRAESTRUCTURA

Todos los documentos y trabajos realizados serán propiedad de la Consejería de Gobernación y Justicia de la Junta de Andalucía. Ésta podrá ejercer el derecho a explotación de los mismos, incluyendo la modificación, reproducción, divulgación o comunicación pública de los trabajos.

La empresa adjudicataria podrá hacer uso de dichos trabajos, para su referencia o reutilización, siempre que cuente con autorización expresa y por escrito de la Consejería de Gobernación y Justicia.

Todos los elementos de infraestructura requeridos y proporcionados en el ámbito del contrato, si resultara el caso, serán suministrados a la Consejería de Gobernación y Justicia, en régimen de propiedad."

La relación de los principales servicios que han sido objeto de externalización es la siguiente:

CSU: (Centro de Servicios a Usuarios): Atención de primer nivel a los usuarios judiciales para resolución de incidencias y gestión de peticiones.

Servicio de apoyo a SISTEMAS: Encargado del análisis y seguimiento de necesidades tecnológicas, gestión, administración y mantenimiento de la infraestructura tecnológica en los Servicios Centrales y sedes judiciales.

ASISTENCIA técnica provincializada: Servicio integral de soporte a las infraestructuras TIC en las Delegaciones de Gobierno de la Consejería, que aporte soluciones técnicas a las incidencias surgidas, y asesoramiento en el uso de los medios desplegados.

Servicio de FORMACIÓN e implantación: Servicio de formación e implantación destinado a los usuarios judiciales: jueces y magistrados, secretarios, funcionarios con perfil auxilio, tramitadores y gestión, fiscales, personal adscrito a los Institutos de Medicina Legal y a cualquier otro perfil involucrado en la Administración de Justicia.

Servicio de ASESORÍA procesal y resolución de incidencias de los sistemas de gestión procesal. Sus funciones son:

- Asesoramiento al Servicio de Informática en materia procesal.
- La resolución de las incidencias procesales y atención de consultas relacionadas con la explotación de dichos sistemas.
- Apoyo en materia procesal para el desarrollo, evolución y adaptación de los sistemas,

- participación en pilotos y pruebas de aplicativos.
- Adaptación de los sistemas a la legalidad vigente.
- Adecuación de los esquemas de tramitación procesal y colecciones documentales a las normas establecidas del Test de Compatibilidad.

Servicio de DESARROLLO de aplicaciones: Se encarga del análisis, diseño y construcción de los sistemas de información, así como del mantenimiento de los mismos. Entre ellas JARA.

Servicio de mantenimiento del sistema procesal ADRIANO: Se encarga de los evolutivos y correctivos del Sistema ADRIANO, además se encargó de la integración con LEXNET.

Mantenimiento de los sistemas de grabación de vistas: Servicio encargado de mantenimiento, administración y asistencia para el funcionamiento de los sistemas de grabación de Salas de Vistas y equipamientos asociados instalados en las sedes judiciales de Andalucía.

3.5. Respecto de las medidas de seguridad estas se encuentran recogidas en la página web:

<http://www.juntadeandalucia.es.....>



3.5.1. En dicho portal se recogen los documentos de seguridad relativos al *SISTEMA DE GESTIÓN PROCESAL DEL CGPJ* y al *CGI – Dirección General de Infraestructuras y Sistemas*.

3.5.2. Respecto del documento de seguridad relativos al *SISTEMA DE GESTIÓN PROCESAL DEL CGPJ*, se resalta que si bien no se trata del documento de seguridad completo pues no incorpora los anexos y por lo tanto no revela información sensible de la entidad, sí que se recoge en dicho documento los datos personales de una persona de nombre **B.B.B.** encargada de su modificación, lo que no se justifica en un documento de este tipo que se encuentra

disponible a cualquier persona usuario de Internet.

3.5.3. Respecto al segundo documento de seguridad relativos al CGI – *Dirección General de Infraestructuras y Sistemas* se señala que también se revelan datos personales identificativos como son **C.C.C. y D.D.D.**, ambos de departamento de sistemas y pertenecientes al *GRUPO DE TRABAJO DE SEGURIDAD Y REDES (GTSR)* en su calidad de usuarios autorizados del fichero de *TARJETAS CRIPTOGRÁFICAS*, o **E.E.E.** que figura como administrador de los ficheros *INCIDENCIAS INFORMÁTICAS* y *USUARIOS*, **F.F.F.** como administrador del fichero *PERMISOS Y LICENCIAS*, **G.G.G.** administrador de los ficheros *HISTORIALES CLÍNICA FORENSE IML* y *AGENDA CITACIONES IML*. Además de revelarse públicamente en dicho documento los datos personales mencionados también se revela información que puede comprometer la seguridad dado que se describe la infraestructura y el entorno tecnológico con un nivel de detalle que llega a incluir incluso a especificar la marca, el modelo y la versión de equipos de seguridad, así como procedimientos asociados a la política de gestión de usuarios y contraseñas que únicamente deben ser conocidos por las personas que tengan que conocerlo.

3.5.4. En relación a los dos puntos anteriores cabe señalar que el Documento de Seguridad tiene la consideración de “*documento interno*” de la organización tal y como recoge el artículo 88 del Real Decreto 1720/2007, a cuyo acceso se debe de aplicar el principio de “*necesidad de conocer*” recogido en el artículo 91, **por lo que no se justifica que la información citada se encuentre disponible a cualquier usuario de Internet.**

3.6. Respecto a la Información facilitada a los usuarios en general y sobre la utilización de los certificados digitales en particular:

3.6.1. Tanto a los usuarios de JARA como de LexNET, que una vez finalice la implantación de dichos sistemas serán los mismos, se les forma en las diferentes aplicaciones incluyendo los contenidos en materia de firma digital.

3.6.2. Además, en la Junta de Andalucía existe un plan de formación en el que se encuentran diferentes cursos en materia de seguridad y de Protección de Datos, en concreto dentro del Plan de Formación de 2015, el curso de *Aplicación de la Ley Orgánica de Protección de Datos en la Administración de Justicia destinado a los funcionarios/as al servicio de la Administración de Justicia de la Comunidad Autónoma de Andalucía, de los Cuerpos de Gestión y Tramitación Procesal y Administrativa y Auxilio Judicial*.

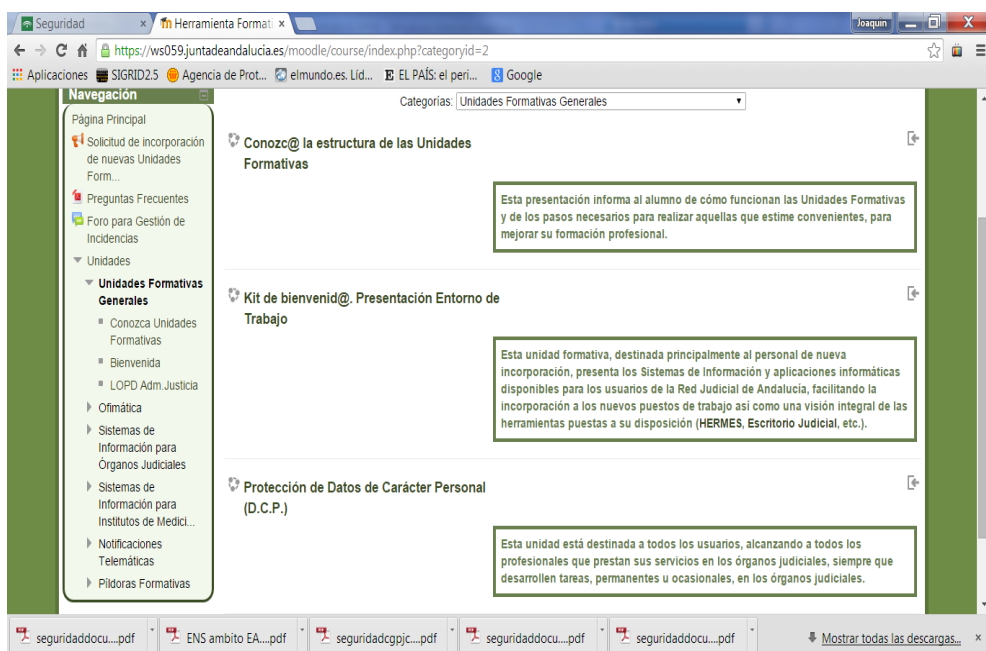
3.6.3. A sabiendas que estos cursos suelen tener plazas limitadas, en el Portal Adriano, donde pueden acceder todos los usuarios se encuentra toda la información sobre seguridad disponible, como se

puede comprobar en este enlace:

<http://www.juntadeandalucia.es.....>

3.6.4. Además, en el apartado de formación no reglada se encuentra un pequeño curso introductorio sobre LOPD que solo se encuentra disponible para accesos realizados desde dentro de la red judicial:

<https://.....>



3.7. Respecto a la justificación en base a la cual se ha obligado a la

utilización de los certificados digitales indicados (DNI electrónico o certificado de persona física) y no se ha optado por utilizar otros certificados como por ejemplo el de empleado público las razones esgrimidas por la Junta de Andalucía son las siguientes:

3.7.1. Señala la Junta de Andalucía que para poder implantar la administración electrónica en Justicia, al igual que en la administración general, se hace necesario disponer de unos mecanismos que permitan realizar la autenticación de la persona y que se pueda realizar la firma digital de la documentación.

3.7.2. En este sentido añaden que la Ley 59/2003, de 19 de diciembre, de firma electrónica, en su artículo 6 establece el concepto de certificado electrónico y de firmante de la siguiente manera:

1. *Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.*

2. *El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.*

3.7.3. El Capítulo II de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, se dedica a las formas de identificación y autenticación, tanto de ciudadanos y profesionales como de la propia Administración de Justicia. Respecto a los primeros, se contempla la posibilidad de uso de diversos sistemas de firma electrónica además del incorporado al Documento Nacional de Identidad (eDNI). En cuanto a los órganos y oficinas judiciales, se establece la obligatoriedad de que la Administración competente facilite a los mismos los sistemas de firma electrónica consistentes en sello electrónico y código seguro de verificación.

3.7.4. El artículo 8 de la Ley 18/2011, regula el uso obligatorio de medios e instrumentos electrónicos indicando que *"los sistemas informáticos puestos al servicio de la Administración de Justicia serán de uso obligatorio en el desarrollo de la actividad de los órganos y oficinas judiciales y de las fiscalías por parte de todos los integrantes de las mismas, conforme a los criterios e instrucciones de uso que dicten, en el ámbito de sus competencias, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Administraciones competentes, así como a los protocolos de actuación aprobados por los Secretarios de Gobierno."*

3.7.5. Asimismo el artículo 21.2 de esta misma ley establece que *las Administraciones, en el ámbito de sus competencias, proveerán a secretarios judiciales, fiscales, forenses y demás personal al servicio de la Administración de Justicia, de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo y el cargo e identificar también a la oficina u órgano judicial en la que presta sus servicios.*

3.7.6. Por otro lado, a través del Convenio de colaboración entre el Ministerio de Justicia y la Consejería de Justicia y Administración

Pública de la Junta de Andalucía para la cesión de los derechos de uso del sistema Lexnet del Ministerio de Justicia, firmado el 16 de febrero de 2009 se empieza a implantar Lexnet en Andalucía y, según el *Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos* se hace necesario, tal como establece su artículo 2, el uso de la firma electrónica reconocida y que deberán poseer el personal que aparece en su Anexo II, es decir:

- “1. Funcionarios del Cuerpo Superior Jurídico de Secretarios Judiciales.
2. Funcionarios del Cuerpo de Gestión Procesal y Administrativa.
3. Funcionarios del Cuerpo de Tramitación Procesal y Administrativa.
4. Funcionarios del Cuerpo de Auxilio Judicial.
5. Abogacía del Estado.
6. Ministerio Fiscal.
7. Procuradores de los Tribunales.
8. Abogados.
9. Graduados Sociales.
10. Administrador del Colegio de Procuradores.
11. Órganos de la Administración General del Estado y sus organismos públicos, así como otras Administraciones e instituciones que habitualmente se relacionen con la Administración de Justicia”.

3.7.7.Y en el anexo IV se establece que “se admitirá, a los usuarios que se relacionan en el Anexo II, la presentación y recepción telemática de documentos mediante firma electrónica, basadas en un certificado que cumpla con la recomendación UIT X.509.V3 o superiores (ISO/IEC 9594-8 de 1997) o aquellas otras que pudieran ser publicadas en el Diario Oficial de la Unión Europea, de conformidad con lo previsto por la Ley 59/2003, de 19 de diciembre, de firma electrónica.”.

3.7.8.Con este escenario normativo, y la necesidad de seguir avanzando en la administración electrónica, la Consejería manifiesta que comenzó un despliegue de certificados digitales que permitieran trabajar con estas nuevas herramientas al personal de la Administración de Justicia.

3.7.9.Tal y como establece la normativa, es necesario identificarse digitalmente para poder actuar en los sistemas descritos; para ello se puede usar cualquier certificado digital reconocido, entre ellos el DNle o los certificados digitales expedidos por la FNMT.

3.7.10.La Junta de Andalucía firmó con la FNMT un convenio para dotar de firma digital a todos los andaluces de forma gratuita y, de esta forma, potenciar su uso y habilitar los trámites telemáticos con la administración. Tanto la infraestructura para la dotación como el coste de la tramitación de los certificados está siendo sufragada por la propia Junta de Andalucía.

3.7.11.Desde la Consejería, consideran que dichos certificados son completamente válidos para realizar trámites internos, dentro de

las diferentes administraciones, o externos, con otras administraciones, por lo que alegan que se aprovechó dicha infraestructura para dotar a cada uno de los usuarios de la Administración de Justicia que no tuvieran mecanismos de firma digital, de los mismos. Añaden que actualmente se ha dotado de más de 4.000 certificados, con los que se están realizando trámites (notificaciones a través de Lexnet, solicitudes de informes e informes en materia de drogadicción, solicitud de préstamos al archivo y transferencias, etc.)

3.7.12. La Junta de Andalucía entiende que los sistemas deben poder usar cualquier mecanismo reconocido para realizar firma digital (DNle, certificado de la FNMT, o de cualquier otro organismo reconocido); por ello, y para no dotar al personal de Justicia de un certificado distinto para cada trámite con las Administraciones, se ha decidido reutilizar el DNle o el certificado digital de la FNMT, cuya infraestructura para poder expedirlo ya dispone la propia Junta de Andalucía, como se ha mencionado anteriormente, ahorrando costes y facilitando al usuario la autenticación en los sistemas con un sólo certificado.

3.7.13. **A nivel de protección de datos**, el uso del certificado digital es similar a la información que ya está declarada en la Agencia. El uso de certificado para acceder a sistemas o para firmar no altera la información recogida en los sistemas, ya que el Nombre, DNI y cargo del personal de justicia ya está declarado en el sistema de gestión procesal. A través de dicho certificado se puede acceder a los sistemas y se comprueba la persona identificada con la base de datos que ya existe de cargos.

3.7.14. En concreto, el sistema LexNET, que depende del Ministerio de Justicia, tiene declarado un fichero tal y como se expone en el anexo I Fichero 2. *Gestión de usuarios del sistema Lexnet*, del Real Decreto 84/2007 (Ver ANEXO IV de la documentada por la Junta de Andalucía). Con lo que no existiría incumplimiento de la Ley Orgánica de Protección de Datos al respecto, por el uso de dicho sistema.

3.7.15. Con la dotación de los certificados digitales de la FNMT, la Junta de Andalucía entiende que no se vulnera ninguna privacidad de la firma digital, ni se pierde intimidad en el acceso de la información; con el actual certificado proporcionado por la Junta de Andalucía se pueden realizar trámites con las diferentes administraciones o gestiones privadas, de la misma manera que con DNle. Lo que hace la Consejería es dotarle de ese certificado, si no lo tuviera y de forma gratuita, y le habilita para realizar también gestiones con los sistemas de trámite interno (JARA, LEXNET, ADRIANO, etc.), tal y como se desarrolla en los trámites en la Administración Electrónica de la Junta de Andalucía.

3.7.16. Tanto el certificado denominado de “persona física” como el de “empleado público” emitidos por la FNMT, como el DNle, se adecúan a la norma X.509.V3. El certificado de “empleado público” certifica adicionalmente el cargo y el organismo en el que se desempeña dicho cargo, mientras que el certificado incluido en el

DNle incorpora la fecha de nacimiento. En todo caso, cualquiera de los tres facilita autenticación de la persona que lo utiliza y permite firmar documentos de acuerdo con la Ley 18/2011.

El empleo de un certificado personal o de empleado público no tiene relevancia desde la óptica de la protección de datos, ya que en ninguno de los dos casos existiría la posibilidad para el organismo de realizar un seguimiento de la utilización que el usuario del certificado pudiera hacer del mismo fuera del ámbito del organismo. Es decir ni el Ministerio del Interior, entidad emisora del DNle, ni la FNMT entidad emisora de sus certificados, ni el organismo o entidad con quien se interactúa utilizando estos certificados de firma electrónica, puede conocer que otras interacciones realiza el usuario con terceros utilizando los mismos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La denunciante y 79 firmantes denuncian las siguientes cuestiones que, a su juicio, pueden constituir infracciones a la normativa de protección de datos:

a) La instalación en la Ciudad de la Justicia de Málaga del sistema de información JARA para la gestión de archivos judiciales en la Ciudad de la Justicia de Málaga así como de una aplicación LEXNET para el envío de notificaciones telemáticas por parte de los órganos judiciales que son utilizados, entre otros, por el personal del Cuerpo de Auxilio Judicial “obliga” a utilizar un certificado digital de firma electrónica pudiendo optar entre el DNI electrónico o Certificado de Persona Física expedido por la Fábrica Nacional de Moneda y Timbre -FNMT-, otros certificados de firma digital como el que se emite para “Empleados Públicos”, cuya utilización en este caso sería más adecuada ya que entienden que tanto el DNI electrónico como el Certificado de Persona Física están pensados para su utilización en el ámbito privado de su titular y no en el ámbito profesional derivado de su condición de empleado público.

b) Que la explotación de los sistemas de información sobre el que actúan dichos certificados digitales se ha externalizado en una empresa privada y el pliego del concurso para dicha prestación no hace referencia alguna a las “medidas de seguridad” limitándose a indicar, de modo genérico, la confidencialidad de los datos de carácter personal, lo que resulta a juicio de los denunciantes insuficiente habida cuenta de que dicho sistema va a albergar datos sensibles de nivel alto como por ejemplo los derivados de procedimientos penales y violencia de género.

y c) que se ha vulnera el art. 20 de la LOPD sobre creación, modificación o supresión de ficheros de titularidad pública ya que el sistema trata datos de los

certificados digitales de los empleados y esta circunstancia no se recoge en la disposición de creación de los ficheros a su juicio implicado de Tarjetas Criptográficas, Usuarios, Gestión de Archivos.

III

La LOPD en su artículo 40 reconoce a la AEPD la *“potestad inspectora”* y en su apartado 1, recoge: *“Las autoridades de control podrán inspeccionar...”* El Reglamento 1720/2007 de 21/12, por el que se aprueba el Reglamento de desarrollo de la LOPD en su artículo 122 prevé: *“1...., se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación...”* y el R. D. 1398/1993, de 4/08, del Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora en su artículo 12 dispone lo siguiente: *“ Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas de investigación..”*

De acuerdo con la normativa citada corresponde al Director de la Agencia Española de Protección de Datos -AEPD- determinar si, a la vista de la denuncia formulada y de los elementos aportados en justificación de la misma, concurre causa justificativa que lleve a la realización de actuaciones previas de inspección, de suerte que en el presente caso, se realizaron dichas actuaciones previas con el resultado expuesto en el Hecho Segundo de la presente resolución.

Se debe señalar que la Consejería de Justicia tras requerimiento de inspección desarrolló un exhaustivo informe sobre la justificación de los sistemas informáticos implantados, legislación que los sustenta, , ficheros implicados, medidas de seguridad y trascendencia de los certificados digitales desde el punto de vista de protección de datos.

IV

La LOPD en su artículo 6, dispone:

“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.

Respecto a la justificación en virtud de la cual se ha obligado a la utilización de los certificados digitales indicados (DNI electrónico o certificado de persona física) y no se ha optado por utilizar otros certificados como por ejemplo el de “Empleado Público”, ha quedado acreditado que tanto el certificado de *“persona física”* como el de *“empleado público”* emitidos por la FNMT se adecuan a la norma X.509.V3 y certifican la identidad de la persona con su nombre, apellidos y DNI. El certificado “personal” únicamente incluye como dato adicional la fecha de nacimiento. El certificado de

“*empleado público*” certifica adicionalmente el cargo y el organismo en el que se desempeña, es decir, contiene datos adicionales respecto del de “*persona física*”.

EL empleo de un certificado u otro no tiene relevancia desde la óptica de la protección de datos, ya que en ninguno de los dos casos existiría la posibilidad para el organismo de poder realizar un seguimiento de la utilización por el usuario del certificado fuera del ámbito del organismo. Es decir, ni la FNMT entidad emisora de sus certificados, ni el organismo o entidad con quien se interactúe utilizando estos certificados de firma electrónica, puede conocer de interacciones adicionales con terceros utilizando los mismos. En el mismo sentido, el Ministerio del Interior, entidad emisora del DNle tampoco puede acceder a esta información.

Además aunque el certificado personal incluye como dato adicional la fecha de nacimiento su conocimiento no desborda el ámbito de la Consejería en el que tal información es conocida.

V

La LOPD en su artículo 12, prevé:

“La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

En lo concerniente a la alegación consistente en que los datos de los certificados son tratados por una empresa privada y que el pliego del concurso para dicha prestación no hace referencia alguna a las “medidas de seguridad”, lo que resulta a juicio de los denunciantes insuficiente habida cuenta de que dicho sistema va a albergar datos sensibles de nivel alto como los derivados de procedimientos penales y de violencia de género, la inspección ha acreditado lo siguiente:

La complejidad e implicación de los sistemas informáticos implantados justifican la externalización para mantener los servicios tecnológicos de la Consejería. El hipotético riesgo alegado se encuentra cubierto mediante exhaustivas cláusulas de seguridad y de protección de datos que se incluyen en los pliegos de adjudicación recogidas en el apartado 3.4 del Hecho Segundo de la presente resolución que no se reproducen a efectos de brevedad, si bien se relacionan los enunciados de las cláusulas previstas:

“11 PROPIEDAD, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

11.1 INFORMACIÓN DE BASE

11.2 CONFIDENCIALIDAD DE LA INFORMACIÓN

11.3 TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

11.4 PROPIEDAD DE LOS DOCUMENTOS, TRABAJOS E INFRAESTRUCTURA

Asimismo, a continuación del referido apartado 11.4 se especifican los principales servicios que han sido objeto de externalización.

Los requisitos exigidos en el artículo 12 de la LOPD se encuentran en consecuencia, implementados.

VI

El artículo 20 de la LOPD, prevé:

“2 Las disposiciones de creación o de modificación de ficheros deberá indicar:

- a) La finalidad del fichero y los usos previstos para el mismo.*
- b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.*
- c) El procedimiento de recogida de los datos de carácter personal.*
- d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.*
- e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.*
- f) Los órganos de las Administraciones responsables del fichero.*
- g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.*
- h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.*

En lo concerniente a la posible vulneración del transcrito artículo 20 de la LOPD consistente en que los datos de los certificados digitales de los empleados no se recogen en la disposición de creación del fichero denominado, “Tarjetas Criptográficas, Usuarios, Gestión de Archivos”, la Consejería de Justicia expone que los “ficheros” implicados en los sistemas descritos son, al menos, los siguientes:

- Ficheros declarados por el Consejo General del Poder Judicial -CGPJ- en el *Acuerdo 20 de septiembre de 2006, del Pleno, de creación de ficheros de carácter personal dependientes de los órganos judiciales*, publicado en el BOE número 244 de 12 de octubre de 2006. Estos ficheros son los siguientes

Asuntos Jurisdiccionales.
Registro de Asuntos.

Usuarios.

- Ficheros declarados por la JUNTA DE ANDALUCIA,

Usuarios: fichero declarado en la *Orden de 5 de octubre de 2005, de la Consejería de Justicia y Administración Pública, por la que se modifican ficheros automatizados con datos de carácter personal contenidos en las órdenes de 1 de septiembre de 2003 y de 9 de diciembre de 2003.*

Tarjetas Criptográficas): fichero declarado en la *Orden de 1 de septiembre de 2003, por la que se amplía la de 24 de septiembre de 2002, para regular los ficheros automatizados con datos de carácter personal gestionados por la Consejería.*

- Ficheros declarados por el MINISTERIO DE JUSTICIA,

Gestión de usuarios del sistema LEXNET declarado en el *Real Decreto 84/2007, de 26 de enero sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.*

Existe en consecuencia cobertura suficiente en los ficheros declarados.

VII

La LOPD en su artículo 9, 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 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” .

Las medidas de seguridad se encuentran accesibles en <http://www.juntadeandalucia.es...../> que recoge anexos de los documentos de seguridad relativos al Sistema de Gestión Procesal del CGPJ y del CGI (de la Dirección General de Infraestructuras y Sistemas) que contienen datos de carácter personal identificativos de personas físicas.

Al objeto de investigar el alcance y trascendencia de su difusión externa al ámbito de la organización, se procede a declarar la caducidad de las actuaciones de investigación, **E/3814/2014**, por el transcurso de 12 meses desde la presentación de la denuncia y abrir nuevas actuaciones, **E/2285/2015**.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1 PROCEDER AL ARCHIVO de la denuncia en cuanto a:

- la utilización como certificado digital de firma electrónica del DNI electrónico o Certificado de Persona Física en lugar del Certificado digital de Empleado Público.
- la externalización a empresas privadas del tratamiento de los datos de los certificados de los usuarios.
- la declaración de un fichero con la finalidad del tratamiento de los datos de los certificados.

2 DECLARAR CADUCIDAD de la actuaciones, E/3814/2014 y **ABRIR** las Diligencias, **E/2285/2015**, al objeto de investigar el alcance y trascendencia de la difusión externa al ámbito de la organización de datos de carácter personal incorporados al documento de seguridad,

3 NOTIFICAR la presente Resolución a la **CONSEJERIA DE JUSTICIA E INTERIOR** de la **JUNTA DE ANDALUCIA** y a D.^a **A.A.A. Y OTROS**.

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos