Procedimiento Nº AP/00066/2017

RESOLUCIÓN: R/00433/2018

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00066/2017**, instruido por la Agencia Española de Protección de Datos a la Subdirección General de Nuevas Tecnologías de la Justicia, dependiente de la Secretaría General de la Administración de Justicia, Secretaria de Estado de Justicia, MINISTERIO DE JUSTICIA, y en virtud de los siguientes:

ANTECEDENTES

PRIMERO: Con fecha 28 de julio de 2017, se recibe notificación de la existencia de un incidente de seguridad en el sistema LexNET, firmada por el Subdirector General de Nuevas Tecnologías de la Secretaría General de la Administración de Justicia (en lo sucesivo SGNTJ), en el que se manifestaba:

> El incidente afectaba al buzón de correo de los usuarios de LexNET y consistía en que mediante la modificación deliberada de la dirección URL del navegador, cambiando los dígitos de identificación del usuario, se podía acceder a los buzones de otros usuarios. Dicha identificación consta de 10 dígitos, por lo que para acceder a un buzón concreto hay que conocer el identificador asociado a dicho usuario.
>
> En la SGNTJ se tuvo conocimiento del incidente de seguridad el día 27 de julio de 2017 al recibirse aviso de un usuario de LexNET. La brecha aparece en una versión de LexNET puesta en producción el 20 de julio de 2017. La primera acción que se tomo fue verificar que el incidente existía y, a continuación, se resolvió a las 5 horas desde la detección del incidente.
>
> No existen expedientes completos en LexNET, sino notificaciones, que es la información que ha quedado comprometida. El tipo de acceso no autorizado que permite la brecha habilita visualizar el buzón del tercero al que pertenece el identificador, pero no abrir una comunicación que no haya sido previamente abierta por el usuario legítimo.
>
> En relación con los hechos, se habían iniciado investigaciones internas para determinar lo sucedido.

En relación a dicha comunicación, con fecha de 28 de julio de 2017, la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación para que se realice el seguimiento de las consecuencias que dicha brecha haya podido tener y evaluar de las acciones tomadas por los responsables del sistema en el marco de la gestión del incidente.

A su vez, y por el mismo tema, se han recibido los escritos de tres denunciantes.

SEGUNDO: A la vista de los hechos, se iniciaron actuaciones de investigación con los siguientes resultados:

1. La disposición de creación del fichero LexNET es el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la administración de justicia, publicado el 1 de diciembre de 2015 en el BOE, en el que se determina que el responsable del mismo es la Subdirección General de Nuevas Tecnologías de la Justicia dependiente de la Secretaría General de la Administración de Justicia, Secretaria de Estado de Justicia, Ministerio de Justicia.

2. En el artículo 13 se define la naturaleza del sistema LexNET.

   Artículo 13. Definición y características.

   1. El sistema LexNET es un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos.

   ….

   2. El sistema LexNET tendrá la consideración de sistema de entrega electrónica certificada conforme al artículo 43 del Reglamento UE nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

3. En el mismo decreto, se declaran dos ficheros:

   a. Custodia de la información acreditativa de las transacciones realizadas en LexNET con un nivel de seguridad alto.

   b. Gestión de usuarios del sistema LexNET, con un nivel de seguridad básico.

4. En el Registro de Ficheros de la AEPD constan, a fecha 3 de agosto de 2017, y con fecha inicial de inscripción de 2 de abril de 2007, los ficheros anteriores. En ninguno de ellos se declara que se almacene información especialmente protegida o datos relativos a comisión de infracciones.

5. En el acta de inspección realizada en LexNET en el marco del E/00700/2016, se estableció entre otros:

   a. LexNET es una plataforma de intercambio seguro de información entre los órganos judiciales y múltiples operadores jurídicos que, en su trabajo diario, necesitan intercambiar documentos judiciales (notificaciones, escritos y demandas).

   b. LexNET se implantó en el año 2007 como un sistema de envío de documentación de los Procuradores a los Juzgados y desde entonces se han ido incorporando diversos colectivos, entre ellos, los Letrados de la Administración de Justicia (anteriormente Secretarios Judiciales) y, desde enero de 2016, se ha convertido en la plataforma de envío de comunicación obligatoria para todos los abogados del territorio del Ministerio de Justicia y Comunidades Autónomas excepto Cantabria, País Vasco, y Navarra; Cataluña solo utiliza LexNET para notificar y no para presentar escritos (Ley 42/2015, de Enjuiciamiento civil).

c. Actualmente LexNET cuenta con cientos de miles de usuarios, utilizándose en más de 3.500 órganos judiciales y se ha intercambiado más de 364 millones de documentos.

d. LexNET está desarrollada como una nube privada del Ministerio de Justicia.

e. La identificación y autenticación del usuario de LexNET se realiza por certificado digital.

f. Los usuarios tienen que solicitar el alta en LexNET la primera vez que acceden. En el caso de los abogados, procuradores y graduados sociales solo podrán tramitar la solicitud de alta a través de su Colegio profesional, y una vez tramitado, ya podrán acceder con su carnet colegial con firma electrónica (ACA).

g. LexNET funciona a través de privilegios de usuario (estructurados mediante roles) que permiten acceder a un determinado tipo de información.

h. Cada usuario tiene asignado al menos un "rol" y al menos un "buzón" espacio que permite el envío y recepción de los documentos.

i. En caso de que un usuario tenga más de un rol, al acceder a LexNET, el Sistema le muestra, por defecto, las notificaciones correspondientes al buzón o buzones asociados al primer rol que se le asignó en el registro inicial, pudiendo el usuario elegir cualquier de los otros roles que tenga asociado.

j. Los acuses de recibo son visibles en los buzones durante 60 días y posteriormente pueden ser localizados sin restricción temporal, tras hacer una solicitud expresa y ejecutar un proceso de auditoría específico sobre el sistema LexNET.

k. Las notificaciones también son visibles en los buzones durante el plazo que marca la normativa.

l. El acceso a LexNET puede ser directamente (https://lexnet.justicia.es) o a través de aplicaciones externas desarrolladas por diferentes colectivos, entre los que se encuentra el Colegio de Abogacía Española a través del sitio web http://www.abogacia.es, que desapareció en marzo de 2017.

m. Sea cual sea la ruta de acceso, el Sistema internamente utiliza el número de DNI del usuario para identificar su "rol" o "roles" y poder mostrar la información disponible en cada uno de los buzones asociados.

6. Con relación a la detección del incidente y la actividad en Internet del día 27 de julio de 2017, como se incluye en las diligencias, evidencia que:

   a. Qué a las 10:53 horas un usuario manifestaba que había encontrado un fallo en LexNET.

   b. Que a las 15:00 horas el Ministerio de Justicia avisaba sobre la existencia de un fallo en LexNET.

c. Que a las 15:15 el Ministerio de Justicia avisaba de una parada técnica de LexNET.

d. Que a las 16:25 el Ministerio de Justicia avisaba del restablecimiento del servicio.

7. Según fuentes del Ministerio de Justicia, el sistema LexNET en un día estándar puede intercambiar más de 200.000 mensajes y ha realizado desde el 2015 hasta finales de diciembre de 2017 más de 200 millones de comunicaciones.

8. En coordinación con esta Agencia, el Consejo General del Poder Judicial remitió el 4 de agosto de 2017 a la Subdirección General de Nuevas Tecnologías del Ministerio de Justicia diligencias informativas para ampliar el escrito de comunicación de la brecha de seguridad, respondido, con fecha 11 de septiembre de 2017, en el que se manifiesta, entre otros:

   a. Que la incidencia fue detectada por un usuario.

   b. Que la versión LexNET 4.10.1.0, la que tenía la brecha de seguridad, se puso en producción el 20 de julio a las 21:45, se detuvo a las 15:15 del 27 de julio y se sustituyó por una nueva versión a las 16:25 horas.

   c. Afectaba a la versión web, no a la versión para teléfono móvil o los web services que permitían el acceso de aplicaciones a LexNET.

   d. El propósito de dicha versión era permitir el acceso de usuarios a sus buzones de una forma más flexible. Los buzones son de distintos tipos: profesionales colegiados, personal autorizado por los mismos, peritos, administradores concursales, usuarios con acceso a buzones colectivos, organismos de la Administración.

   e. En dicha versión, “las validaciones que se realizan en versiones previas para verificar que el acceso a un buzón/carpeta es por parte de un usuario autorizado (…) se omitió incluirlas en todos y cada uno de los nuevos procesos de validación necesarios para soportar el acceso único a múltiples buzones, en concreto a las validaciones asociadas al control de buzón/carpeta por sesión del usuario”.

   f. Para el acceso a un buzón del que no se es el propietario se tenía que realizar las siguientes acciones:

      i. Autenticarse mediante certificado digital.

      ii. Introducir un número de diez dígitos que no tiene relación con el DNI del usuario.

   g. El acceso a un buzón ajeno permitía realizar las siguientes acciones:

      i. Acceso a las notificaciones practicadas, y traslado de escritos, demandas, notificaciones, partes hospitalarios, etc.

      ii. Acceder a las notificaciones ya aceptadas y a los acuses de recibo de los escritos presentados previamente por el usuario.

      iii. Acceso a las notificaciones no practicadas en caso de buzones de procuradores.

h. No puede realizar las siguientes acciones:

   i. Acceder a notificaciones no practicadas en caso de usuarios distintos a procuradores.

   ii. Realizar presentación de escritos en nombre de terceros.

   iii. Acceso a expedientes completos

   iv. Borrado manual y modificar datos del sistema

i. El sistema borra los datos de forma automática en 60 días.

j. El sistema cuenta con un sistema de auditoría que deja constancia de accesos al sistema y que permite identificar al usuario y la dirección de Internet desde el cual se realizó el acceso a un determinado buzón. Dichos registros se conservan a disposición del CGPJ.

k. Las acciones que se tomaron fueron:

   i. El equipo técnico evaluó, comprobó, confirmó e inició el análisis de la solución de la incidencia informada.

   ii. La solución consistió en incorporar mecanismos de validación de permisos en los accesos a todos los elementos del sistema.

   iii. La solución se validó para todos los tipos de buzones LexNET. Posteriormente se validó por el Personal de Pruebas y Calidad.

   iv. A las 15:15 se procede a parar el servicio en Producción para proceder al despliegue del parche corrector, y a las 16:25 del mismo día se finaliza el despliegue y se restablece el servicio.

9. Queda constancia de un tweet de 27 de julio de 2017 a las 23:24 de un usuario que manifiesta haber accedido a LexNET sin el certificado correspondiente.

   No se ha encontrado en Internet que la situación informada en el tweet anterior la haya replicado ningún usuario ni evidencia de que fuera real.

10. Con fecha 9 de octubre de 2017 se realiza una inspección a la Subdirección General de Nuevas Tecnologías de la Justicia, en cooperación con el equipo de inspección del Consejo General del Poder Judicial teniendo en su presencia al Subdirector General de Nuevas Tecnologías de la Justicia, a la Subdirectora General de Programación de la Modernización, a la Jefa del área de Producción, a la Responsable de Seguridad y representantes de la encomienda de ISDEFE. En dicha inspección, los anteriores mencionados realizaron las siguientes manifestaciones:

    a. La SGNTJ consta de personal propio y servicios externos adjudicados por distintas encomiendas de gestión a las empresas ISDEFE, TRAGSA e INECO.

    b. El desarrollo, pruebas y seguridad del sistema LexNET está asignado fundamentalmente al servicio prestado por ISDEFE.

    c. La comunicación de la incidencia se realizó de la siguiente forma:

i. En primer lugar, mediante un mensaje privado a la cuenta de Twitter de LexNET aproximadamente a las 02:00 horas (madrugada) del jueves 27 de julio de 2017 por el Decano del Colegio de Abogados de Cartagena (Murcia).

ii. A continuación, la misma persona envió un mensaje público por Twitter aproximadamente a las 9:30 horas del mismo día en el que se manifestaba cómo explotar la vulnerabilidad del incidente.

iii. No consta que se utilizase el canal de notificación de incidencias que incorpora la aplicación LexNET para la notificación del incidente. Se incorpora como Documento 1 captura de pantalla donde se evidencia la existencia de dicho canal de notificación de incidencias.

iv. Entre las 10:30 y 11:00 horas el Subdirector de la SGNTJ recibe llamada telefónica de dicha persona en relación a la incidencia de seguridad.

v. Entre las 11:30 y las 14:00 se realizan verificaciones exhaustivas, para comprobar si el comportamiento era anómalo o era un problema puntual de un único usuario.

vi. A las 14:00 se detiene el sistema.

vii. A las 16:20 está solucionado el error de programación que produjo el incidente de seguridad

d. La modificación que dio lugar a la incidencia de seguridad se realizó por las peticiones de los usuarios, que realizaban labores de sustitución legítima de otros usuarios en el sistema y por aquellos que tienen distintos roles, para que fuese posible acceder a los buzones de los sustituidos sin necesidad de cerrar la sesión del usuario y, de esta forma, consultar varios buzones de forma simultánea, incorporando un control multibuzón.

e. El error de seguridad se produjo al no incorporar, en dicha modificación, una comprobación de los permisos que disponía el usuario activo en el sistema para acceder a buzones de terceros.

f. Existen procedimientos de pruebas unitarias en la fase de Desarrollo de LexNET, pruebas funcionales en la fase de Pruebas, realizadas sobre un entorno de prueba, y validación del manual de producción e integración en la fase de puesta en Producción. Cada fase se finaliza documentando formalmente el procedimiento y los resultados, documentación que es un requisito necesario para pasar a la siguiente fase.

g. La numeración que identifica cada cuenta del buzón está formada por diez dígitos, los cuatro primeros constantes y los seis siguientes variables, utilizados para la identificación del buzón del usuario con una numeración aleatoria (pero fija para cada usuario) que no tiene relación con cualquier otro identificador del mismo. No todos los números correspondían a usuarios válidos, que asciendan a aproximadamente a

unos 270.000. Para poder acceder a buzones de otro usuario distinto al identificado en el inicio de sesión, era necesario manipular los seis últimos dígitos y encontrar un número de forma aleatoria que coincidiese.

h. Los tipos de cuenta que quedaron expuestas fueron las correspondientes a los colectivos de abogados, procuradores y graduados sociales. Otras cuentas más sensibles, como las correspondientes a la fiscalía, juzgados, fuerzas y cuerpos de seguridad, medicina legal, abogados del estado, servicios jurídicos de las CC.AA y Seguridad Social no estaban afectadas por el incidente.

i. Se estima que el número de abogados que, a pesar de tener cuenta de usuario en LexNET, utilizan esta herramienta como medio de acceso a sus notificaciones es aproximadamente de unos 26.000, ya que esta funcionalidad solo se utiliza por este colectivo en los procedimientos que no requieren procurador.

j. Todo acceso a LexNET o a sus contenidos es registrado en un fichero de log. El intento de acceso a una cuenta queda registrado y, excepto cuando la brecha de seguridad estaba activa, el intento de acceso a una cuenta sin permisos para ello saca al usuario de la sesión que tiene abierta, acción que también se registra en el fichero de log.

k. El incidente no permitía el acceso a notificaciones no aceptadas previamente, no permitía aceptar notificaciones, firmar escritos, modificar el contenido de los mensajes de los buzones, borrar documentos anexos o alterarlos, por lo que no era posible alterar la integridad de la información almacenada. Los mensajes recibidos y los documentos anexos a esos mensajes no pueden ser alterados incluso por los usuarios autorizados.

l. Al ser un sistema de notificaciones, la información se elimina del sistema a los 60 días desde la emisión de la notificación, no quedando información en el sistema con más antigüedad de los días señalados. El sistema no almacena expedientes completos.

m. No existía una explotación automática de los ficheros de log en el día de detección de la brecha de seguridad.

n. En relación a los resultados obtenidos de la explotación de los ficheros log en relación a qué accesos no autorizados se produjeron de los días 20 a 27 de julio de 2017, que información se accedió y qué información se descargó de la plataforma, se manifiesta lo siguiente:

    i. Se han realizado análisis de los log de esas fechas, y de semanas anteriores y posteriores a las mismas para detectar patrones de comportamiento irregulares.

    ii. Los análisis se han realizado de forma reiterada, y aunque hay un informe preliminar de fecha 30 de agosto de 2017, se está realizando un análisis más exhaustivo.

    iii. Los datos que evidencian la magnitud de la brecha en los análisis realizados a fecha de la inspección son los siguientes:

1. 284 usuarios accedieron a 692 buzones que no les pertenecían realizando 1438 visualizaciones de mensajes de forma no autorizada.
2. De ellos, 74 usuarios accedieron a 79 buzones que no les pertenecían y consultaron 432 documentos de forma no autorizada.

o. En relación a las modificaciones procedimentales introducidas para prevención de futuros errores de seguridad a raíz de la detección del incidente el día 27 de julio de 2017.

i. Se han complementado las baterías de pruebas para añadir pruebas al conjunto ejecutado sobre LexNET específicamente sobre control de acceso a buzones de usuarios.

ii. Los registros de log de acceso al sistema LexNET se han completado incluyendo más trazas de operación.

iii. Se ha implementado una solución SIEM (Security Information Event Management) para recoger, analizar y priorizar los eventos de seguridad dentro de la red.

p. Las acciones planificadas para un futuro son:

i. Implementar un Command Center, para centralizar el análisis de logs, así como la vigilancia de las aplicaciones en tiempo real y prevenir incidentes.

ii. Se está negociando un convenio con el CCN para desarrollar un SOC (Centros de Operaciones de Seguridad) entre otros en relación al sistema LexNET.

11. En la misma inspección se comprueba que en el sistema LexNET existe una opción que permite a los usuarios notificar los incidentes relativos al uso de la plataforma.

12. Con fecha 08 de noviembre de 2017 se recibe de la SGNTJ información que había quedado requerida durante la inspección presencial. De la información remitida cabe destacar:

a. La remisión de un informe de auditoría sobre el incidente de seguridad, de fecha 26 de octubre de 2017, que evidenciaba qué usuarios de LexNET accedieron a buzones que no les pertenecían visualizando mensajes de forma no autorizada; y una parte de dichos usuarios consultaron documentos de dichos buzones igualmente de forma no autorizada.

b. Los sujetos que realizaron los accesos indebidos fueron mayoritariamente abogados, a continuación procuradores y finalmente graduados sociales.

c. Los accesos indebidos se produjeron desde el 20 al 28 de julio ambos inclusive, produciéndose el mayor número de accesos indebidos el día 27 de julio de 2017.

d. Los accesos indebidos que se produjeron el 28 de julio se debieron a que el parche de seguridad del día 27 de julio a las 15:15 no fue completamente efectivo y siguieron produciéndose accesos indebidos. Por esta circunstancia, desde la SGNTJ se tuvo que poner en producción una nueva versión el 28 de julio a las 16:30.

e. Se adjunta un borrador del convenio de colaboración con el CCN en materia de ciberseguridad.

f. Se adjunta una presentación de la puesta en marcha de un Centro de Control en tiempo real de los servicios de la SGNTJ de fecha 17 de julio de 2017.

g. Se adjunta un fragmento del manual del Área de Gestión de la Demanda y Atención al Usuario en el que se establece la Vía de Contacto para gestión de incidencias, en el que se especifica una dirección web, un canal twitter privado y un número de teléfono, de fecha 18 de octubre de 2017.

h. Se adjunta un fragmento del manual de Desarrollo LexNET en el que se especifica el procedimiento de gestión de incidencias, de fecha 19 de abril de 2017, modificado el 22 de junio de 2017.

i. Se adjunta una nueva instrucción de la SGNTJ para incorporar en la fase de pruebas de un control de acceso y autorización de fecha 10 de octubre de 2017.

j. Procedimiento de gestión de incidentes en seguridad de la información de la Oficina de Seguridad de la SGNTJ de fecha 17 de julio de 2017.

13. De los datos proporcionados, se estima que el impacto de la brecha afectó a aproximadamente:

    a. Al 0,1% de los buzones de LexNET

    b. Al 0,02% de los mensajes que se intercambian en un día.

    c. Al 0,0001% de todos los mensajes que se han intercambiado en la plataforma LexNET desde el inicio de su operación.

14. Con fecha 23 de octubre de 2017 se solicitó información adicional a la Subdirección General de Nuevas Tecnologías sobre la tipología de documentos afectados por el incidente de seguridad. En su respuesta de entrada 14 de noviembre de 2017 la SGNTJ nos informa de la imposibilidad de conocer el tipo de documento, pues eso implicaría realizar un acceso para el que necesitan la autorización previa de los usuarios.

TERCERO: Con fecha 5 de diciembre de 2017**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a la Subdirección General de Nuevas Tecnologías de la Justicia, dependiente de la Secretaría General de la Administración de Justicia, Secretaria de Estado de Justicia, del Ministerio de Justicia, por la presunta infracción de los artículos 9 y 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en los artículos 44.3.h) y 44.3.d) respectivamente, de dicha norma.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, la Subdirección General de Nuevas Tecnologías de la Justicia presentó escrito matizando las cifras y plazos que fueron recogidas en el acuerdo de inicio, al haber realizado un análisis más detallado del problema. Añade que los atestados se envían por las Fuerzas y Cuerpos de Seguridad al Juzgado, utilizando la aplicación Sindepol y no a las partes. Las partes personadas que solicitan copia, la misma no se envía por LexNET, sino que se acude al órgano judicial y allí se facilita. La vulnerabilidad afectó únicamente a los mensajes existentes en el sistema intercambiados en los últimos 60 días, es decir, en el período de 21 de mayo al 28 de julio de 2017. Los buzones potencialmente expuestos son los correspondientes a los profesionales abogados, procuradores y graduados sociales. Habría que excluir los mensajes intercambiados con el resto de organismos públicos que acceden a LexNET, tales como Policía Nacional, Guardia Civil, Consejo General de la Abogacía de España, etc.

Indican que respecto de este apartado: <<El resultado es que existe una vulnerabilidad conocida en el protocolo TLS1.0 (y en versiones inferiores) utilizados en el servidor. Al no poder utilizar versiones más avanzadas, como TLS2.0 o TLS3.0, se califica el nivel de seguridad como el más bajo posible>>; quieren precisar que no existen versiones inferiores a TLS1.0, pero debido a que no se admite el uso del protocolo SSLv3 se evitan riesgos asociados al mismo y el nivel de seguridad no es el más bajo posible. El Ministerio de Justicia está trabajando en la actualización del protocolo de seguridad a la versión TLS 1.2. El incidente se ha debido a un error de programación del sistema informático y no al uso de una versión inferior de este protocolo de seguridad.

Por último, indican que por parte de esa Subdirección se han adoptado medidas de seguridad adecuadas para los datos tratados.

QUINTO: Con fecha 10 de enero de 2018, se acordó por la Instructora del procedimiento la apertura de un período de práctica de pruebas, acordándose practicar las siguientes:

Se da por reproducida, a efectos probatorios, la documentación recabada en las actuaciones previas de inspección que forman parte del expediente E/04521/2017. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento AP/00066/2017 presentadas por la S.G. NUEVAS TECNOLOGÍAS. Todo ello con su correspondiente documentación adjunta.

SEXTO: Con fecha 25 de enero de 2018, se recibió el Acuerdo adoptado por la Comisión Permanente del Consejo General del Poder Judicial, en su reunión de 28 de diciembre de 2017, respecto al procedimiento iniciado en relación con el incidente de vulnerabilidad del sistema de comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia, LexNET. El Acuerdo aprueba *"el archivo de las diligencias preliminares 1/2017 abiertas por el Centro de Documentación Judicial (CENDOJ) en cumplimiento del acuerdo adoptado por la Comisión Permanente del Consejo General del Poder Judicial en reunión extraordinaria celebrada el 28 de julio, al objeto de clarificar los hechos relativos a la*

quiebra en materia de seguridad del sistema de comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia, LexNET".

En los Fundamentos de Derecho de este Acuerdo se indica lo siguiente: *"… se desprende que se produjo una brecha de seguridad en la versión LexNET 4.10.1.0 que afectaba a la versión web, no a la versión para teléfono móvil o los web services que permitían el acceso de aplicaciones a LexNET, siendo así que el propósito de dicha versión era permitir el acceso de usuarios a sus buzones de forma más flexible.*

Ha de partirse de la consideración de que el sistema LexNET es utilizado por abogados, procuradores, graduados sociales, centros penitenciarios, funcionarios de la Oficina Judicial, la Policía Nacional, los policías locales, la Guardia Civil y hospitales que utilizan el sistema electrónico para remitir atestados o partes de lesiones, tal y como informó el Ministro de Justicia en su comparecencia en el Congreso de Diputados el 31 de agosto de 2017, pero no es utilizado por jueces y por fiscales mínimamente en pruebas piloto y solo con ocasión de aceptar notificaciones.

Del resultado de la Inspección, conforme obra en el acta de 23 de octubre de 2017, se desprende que todos los tipos de cuenta no quedaron expuestas, "sólo las correspondientes a los colectivos de abogados, procuradores y graduados sociales", en tanto que otras cuentas más sensibles, como las correspondientes a la fiscalía, juzgados, fuerzas y cuerpos de seguridad, medicina legal, abogados del estado, servicios jurídicos de las CCAA y Seguridad Social, "no estaban afectadas por el incidente".

Por otra parte, de acuerdo con los informes recabados, el acceso a un buzón ajeno no permitía realizar acciones consistentes en el acceso a expedientes completos, acceso a notificaciones no practicadas en caso de usuarios distintos a procuradores, ni realizar presentaciones de escritos en nombre de terceros ni la posibilidad de borrado manual y modificación de datos del sistema.

En este sentido, puede afirmarse que la quiebra de seguridad de la versión 4.10.1.0 ocurrida el día 27 de julio de 2017 no afectó a ficheros jurisdiccionales, cuya independencia y autonomía respecto a las comunicaciones y notificaciones electrónicas, así como a la presentación electrónica de escritos, documentos u otros medios o instrumentos y al traslado de copias (que conforma el contenido y actividad del sistema LexNET) es completa, de manera que la seguridad, tanto de los sistemas de gestión procesal como de los ficheros jurisdiccionales, ha estado siempre salvada razón por la cual, en virtud de lo dispuesto en el artículo 236 nonies, tercero de la LOPJ, procede archivar el presente expediente y dar traslado a la AEPD a fin de que prosiga con la tramitación del procedimiento, sin perjuicio de adoptar la resolución que proceda si del curso de la investigación llevada a cabo por la AEPD se desprenden nuevos indicios de los que pudiera derivar la afectación de los ficheros jurisdiccionales"

SÉPTIMO: Con fecha 19 de febrero de 2018, la Instructora del procedimiento emitió Propuesta de Resolución, en el sentido de que por la Directora de la Agencia Española de Protección de Datos se declare que la la Subdirección General de Nuevas Tecnologías de la Justicia, dependiente de la Secretaría General de la Administración de Justicia, Secretaria de Estado de Justicia, del MINISTERIO DE JUSTICIA, ha infringido lo dispuesto en los artículos 9.1 y 10 de la LOPD, tipificadas como grave en los artículos 44.3.h) y 44.3.d) de dicha norma.

OCTAVO: Con fecha 26 de febrero de 2018, el Ministerio de Justicia (Subdirección General de Nuevas Tecnologías de la Justicia) realizó alegaciones frente a la citada propuesta de resolución, trasladando un escrito del Ministerio de Energía, Turismo y Agenda Digital en la que les comunica que tras recibir información de la SGNTJ sobre el incidente de seguridad relativo al servicio no cualificado de entrega electrónica certificada LexNET, y el análisis exhaustivo del incidente y las medidas tomadas para mitigarlo y evitar situaciones similares en el futuro, la consideran adecuada y suficiente para proceder a la finalización del expediente relativo al incidente de seguridad notificado.

La SGNTJ añade un cuadro de Actuaciones, a las que ya se refirió durante las actuaciones previas de inspección y durante la tramitación del procedimiento de infracción de administraciones públicas. Se concretan en la planificación o puesta en marcha de cincuenta y ocho medidas preventivas para garantizar la no repetición del incidente de seguridad y que se agrupan en las siguientes categorías: la Oficina de Seguridad, un convenio de colaboración con el CCN, la creación de un Centro de Control, la creación de una Oficina de Gestión del Servicio, la mejora de la calidad del código, la revisión de la ejecución de comandos o el acceso a datos, la revisión de la gestión de la autenticación, el filtrado adecuado de datos, la revisión de los esquemas de autorización, la prevención de suplantación al usuario, la eliminación de la posibilidad de filtrado de datos sensibles, la actualización de los componentes software, la mejora de la configuración de seguridad de los sistemas de información, la mejora de estrategias de detección de ataques y otros aspectos organizativos y legales. Sin entrar a describir los detalles técnicos de la misma, se tiene constancia que veintisiete de dichas medidas ya se han implementado, mientras que el resto de ellas se encuentran en desarrollo o fase de pruebas.

HECHOS PROBADOS

PRIMERO: LexNET es una plataforma de intercambio seguro de información entre los órganos judiciales y múltiples operadores jurídicos que, en su trabajo diario, necesitan intercambiar documentos judiciales (notificaciones, escritos y demandas).

SEGUNDO: LexNET se implantó en el año 2007 como un sistema de envío de documentación de los Procuradores a los Juzgados y desde entonces se han ido incorporando diversos colectivos, entre ellos, los Letrados de la Administración de Justicia y, desde enero de 2016, se ha convertido en la plataforma de envío de comunicación obligatoria para todos los abogados del territorio del Ministerio de Justicia y Comunidades Autónomas, excepto Cantabria, País Vasco, y Navarra; Cataluña solo utiliza LexNET para notificar y no para presentar escritos (Ley 42/2015, de Enjuiciamiento civil).

TERCERO: LexNET está desarrollada como una nube privada del Ministerio de Justicia.

CUARTO: La identificación y autenticación del usuario de LexNET se realiza por certificado digital.

QUINTO: Los usuarios tienen que solicitar el alta en LexNET la primera vez que acceden. En el caso de los abogados, procuradores y graduados sociales solo podrán tramitar la solicitud de alta a través de su Colegio profesional, y una vez tramitado, ya

podrán acceder con su carnet colegial con firma electrónica (ACA). LexNET funciona a través de privilegios de usuario (estructurados mediante roles) que permiten acceder a un determinado tipo de información. Cada usuario tiene asignado al menos un “rol” y al menos un “buzón” espacio que permite el envío y recepción de los documentos. En caso de que un usuario tenga más de un rol, al acceder a LexNET, el Sistema le muestra, por defecto, las notificaciones correspondientes al buzón o buzones asociados al primer rol que se le asignó en el registro inicial, pudiendo el usuario elegir cualquier de los otros roles que tenga asociado.

SEXTO: Los acuses de recibo son visibles en los buzones durante 60 días y posteriormente pueden ser localizados sin restricción temporal, tras hacer una solicitud expresa y ejecutar un proceso de auditoría específico sobre el sistema LexNET. Las notificaciones también son visibles en los buzones durante el plazo que marca la normativa.

SÉPTIMO: El acceso a LexNET puede ser directamente (https://lexnet.justicia.es) o a través de aplicaciones externas desarrolladas por diferentes colectivos.Sea cual sea la ruta de acceso, el Sistema internamente utiliza el número de DNI del usuario para identificar su “rol” o “roles” y poder mostrar la información disponible en cada uno de los buzones asociados.

OCTAVO: Con fecha 28 de julio de 2017 se recibió en esta Agencia la comunicación, remitida por el Subdirector General de Nuevas Tecnologías de la Secretaría General de la Administración de Justicia, de la existencia de un incidente de seguridad en el sistema LexNET.

NOVENO: El incidente afectaba al buzón de correo de los usuarios de LexNET y consistía en que mediante la modificación deliberada de la dirección URL del navegador, cambiando los dígitos de identificación del usuario, se podía acceder a los buzones de otros usuarios.

DÉCIMO: En la Subdirección General de Nuevas Tecnologías se tuvo conocimiento del incidente de seguridad el día 27 de julio de 2017 al recibirse aviso de un usuario de LexNET. La brecha aparece en una versión de LexNET puesta en producción el 20 de julio de 2017. La primera acción que se tomo fue verificar que el incidente existía y, a continuación, se resolvió a las 5 horas desde la detección del incidente.

DÉCIMOPRIMERO: En LexNET no existen expedientes completos, sino notificaciones, que es la información que ha quedado comprometida. El tipo de acceso no autorizado habilitaba a visualizar el buzón del tercero al que pertenece el identificador, pero no abrir una comunicación que no hubiese sido previamente abierta por el usuario legítimo.

DÉCIMOSEGUNDO: En relación con los hechos, se han iniciado investigaciones internas para determinar lo sucedido.

DÉCIMOTERCERO: El día 27 de julio de 2017, a las 10:53 horas, un usuario manifestaba que había encontrado un fallo en LexNET.

DÉCIMOCUARTO: A las 15:00 horas de ese día, el Ministerio de Justicia avisaba sobre la existencia de un fallo en LexNET.

DÉCIMOQUINTO: A las 15:15 el Ministerio de Justicia avisaba de una parada técnica de LexNET.

DÉCIMOSEXTO: A las 16:25 el Ministerio de Justicia avisaba del restablecimiento del servicio.

DÉCIMOSEPTIMO: Para el acceso a un buzón del que no se es el propietario se tenía que realizar las siguientes acciones:

- Autenticarse mediante certificado digital.

- Introducir un número de diez dígitos que no tiene relación con el DNI del usuario.

DÉCIMOCTAVO: El acceso a un buzón ajeno permitía realizar las siguientes acciones:

- Acceso a las notificaciones practicadas, y traslado de escritos, demandas, notificaciones, partes hospitalarios, etc.

- Acceder a las notificaciones ya aceptadas y a los acuses de recibo de los escritos presentados previamente por el usuario.

- Acceso a las notificaciones no practicadas en caso de buzones de procuradores.

DÉCIMONOVENO: No puede realizar las siguientes acciones:

- Acceder a notificaciones no practicadas en caso de usuarios distintos a procuradores.

- Realizar presentación de escritos en nombre de terceros.

- Acceso a expedientes completos

- Borrado manual y modificar datos del sistema

VIGÉSIMO: El sistema borra los datos de forma automática en 60 días. El sistema cuenta con un sistema de auditoría que deja constancia de accesos al sistema y que permite identificar al usuario y la dirección de Internet desde el cual se realizó el acceso a un determinado buzón. Dichos registros se conservan a disposición del CGPJ.

VIGÉSIMOPRIMERO: La modificación que dio lugar a la incidencia de seguridad se realizó por las peticiones de los usuarios, que realizaban labores de sustitución legítima de otros usuarios en el sistema y por aquellos que tienen distintos roles, para que fuese posible acceder a los buzones de los sustituidos sin necesidad de cerrar la sesión del usuario y, de esta forma, consultar varios buzones de forma simultánea, incorporando un control multibuzón.

VIGÉSIMOSEGUNDO: El error de seguridad se produjo al no incorporar, en dicha modificación, una comprobación de los permisos que disponía el usuario activo en el sistema para acceder a buzones de terceros.

VIGÉSIMOTERCERO: En relación a qué accesos no autorizados se produjeron de los días 20 a 27 de julio de 2017, a qué información se accedió y qué información se descargó de la plataforma, la SGNTJ indicó que usuarios de LexNET accedieron a buzones que no les pertenecían visualizando mensajes de forma no autorizada, y una parte de los usuarios consultaron documentos de dichos buzones, igualmente, de forma no autorizada.

VIGÉSIMOCUARTO: Al detectar la brecha de seguridad, las acciones que se tomaron fueron:

- El equipo técnico evaluó, comprobó, confirmó e inició el análisis de la solución de la incidencia informada.

- La solución consistió en incorporar mecanismos de validación de permisos en los accesos a todos los elementos del sistema.

- La solución se validó para todos los tipos de buzones LexNET. Posteriormente se validó por el Personal de Pruebas y Calidad.

VIGÉSIMOQUINTO: Las modificaciones procedimentales introducidas para prevención de futuros errores de seguridad a raíz de la detección del incidente el día 27 de julio de 2017.

- Se han complementado las baterías de pruebas para añadir pruebas al conjunto ejecutado sobre LexNET específicamente sobre control de acceso a buzones de usuarios.

- Los registros de log de acceso al sistema LexNET se han completado incluyendo más trazas de operación.

- Se ha implementado una solución SIEM (Security Information Event Management) para recoger, analizar y priorizar los eventos de seguridad dentro de la red.

VIGÉSIMOSEXTO: Las acciones planificadas para un futuro son:

- Implementar un Command Center, para centralizar el análisis de logs, así como la vigilancia de las aplicaciones en tiempo real y prevenir incidentes.

- Se está negociando un convenio con el CCN para desarrollar un SOC (Centros de Operaciones de Seguridad) entre otros en relación al sistema LexNET.

VIGÉSIMOSEPTIMO: La Comisión Permanente del Consejo General del Poder Judicial, en su reunión de 28 de diciembre de 2017, adoptó respecto al procedimiento iniciado en relación con el incidente de vulnerabilidad del sistema de comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia, LexNET el Acuerdo que aprueba *"el archivo de las diligencias preliminares 1/2017 abiertas por el Centro de Documentación Judicial (CENDOJ) en cumplimiento del acuerdo adoptado por la Comisión Permanente del Consejo General del Poder Judicial en reunión extraordinaria celebrada el 28 de julio, al objeto de clarificar los hechos relativos a la quiebra en materia de seguridad del sistema de comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia, LexNET".*

FUNDAMENTOS DE DERECHO

I

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

II

La disposición de creación del fichero LexNET se encuentra en el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la

Administración de Justicia, publicado en el Boletín Oficial del Estado de 1 de diciembre de 2015, que deroga 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.

En el artículo 13 se define la naturaleza del sistema LexNET como un sistema de entrega certificada y segura para acreditar actos de comunicación.

Artículo 13. Definición y características.

> *1. El sistema LexNET es un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos.*
>
> *….*
>
> *2. El sistema LexNET tendrá la consideración de sistema de entrega electrónica certificada conforme al artículo 43 del Reglamento UE nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.*

Según dispone el artículo 236 nonies de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en su apartado 1, según redacción dada por la Ley Orgánica 7/2015, de 21 de julio, “las competencias que la Ley Orgánica 15/1999, de 13 de diciembre, atribuye a la Agencia Española de Protección de Datos, serán ejercidas, respecto de los tratamientos efectuados con fines jurisdiccionales y los ficheros de esta naturaleza, por el Consejo General del Poder Judicial”. En su apartado 2, que “los tratamientos de datos llevados a cabo con fines no jurisdiccionales y sus correspondientes ficheros quedarán sometidos a la competencia de la Agencia Española de Protección de Datos, prestando el Consejo General del Poder Judicial a la misma la colaboración que al efecto precise”.

Por lo tanto, el sistema LexNET, con relación al cumplimiento de la normativa de protección de datos, está sometido a la competencia de la Agencia Española de Protección de Datos.

III

El artículo 9 de la LOPD, 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.

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."

El art. 9 de la LOPD *establece* el principio de *"seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta a los ficheros el art. 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.
b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.
c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.
d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Es necesario analizar las previsiones que el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento define en su artículo 5.2 ñ) el *"Soporte"* como el "*objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*".

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad

de nivel alto se regulan en los artículos 101 a 104.

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.

El Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

Entre las medidas de seguridad de nivel básico, el Reglamento expone en su artículo 91, respecto al control de acceso que:

"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".

Por su parte, el artículo 93, sobre la Identificación y autenticación, dispone:

"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".

El artículo 5.2.b) del Reglamento de desarrollo de la LOPD define la "autenticación" como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la "identificación" como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o

tratamiento.

IV

La SGNTJ, debió, por ello, adoptar las medidas necesarias para impedir que los usuarios de LexNET pudieran acceder a los buzones de otros usuarios. Tales medidas no fueron adoptadas totalmente al modificar la programación del sistema informático ya que se produjeron durante unos días accesos de unos usuarios de LexNET a los buzones de otros.

En definitiva, la SGNTJ está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para el sistema LexNET, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en los mismos. En este caso, sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, por cuanto no impidió de manera fidedigna que por parte de terceros (usuarios del sistema) se pudiera acceder a buzones de distintos usuarios. En concreto, consta acreditado que unos usuarios de LexNET pudieron acceder a buzones ajenos y acceder a notificaciones efectuadas y traslado de escritos, demandas; acceder a notificaciones ya aceptadas y a los acuses de recibo de escritos presentados previamente por el usuario; acceso a notificaciones no practicadas en caso de buzones de procuradores.

Este problema de seguridad se produjo al solicitar numerosos usuarios que realizaban labores de sustitución legítima de otros usuarios y de aquellos que tenían distintos roles para que fuese posible acceder a los buzones de los sustituidos sin necesidad de cerrar la sesión del usuario; de esta forma se podrían consultar varios buzones de forma simultánea, incorporando un control multibuzón.

En la modificación que se realizó para solventar el problema de los usuarios que sustituyen legítimamente a otros usuarios no se incorporó una comprobación de los permisos que disponía el usuario activo en el sistema para acceder a buzones de terceros.

En el momento en que un usuario comunicó el incidente que se producía al acceder a LexNET, la SGNTJ dependiente del Ministerio de Justicia inició el proceso para solventar el fallo y lo solucionó a las pocas horas de ser informados del mismo. Posteriormente, incorporaron mecanismos de validación en los accesos a todos los elementos del sistema, solucionando el error de programación que produjo el incidente de seguridad.

Según consta reseñado en las actuaciones realizadas por la Subdirección General de Nuevas Tecnologías de la Justicia, se analizaron los logs de las fechas en las que se produjo el incidente, comprobando a que información se accedió, analizando las semanas anteriores y posteriores para detectar patrones de comportamiento; se realizó un informe preliminar continuando el estudio para que el análisis sea exhaustivo.

Se ha finalizado las baterías de pruebas sobre control de acceso a buzones de usuarios; los registros de log de acceso al sistema LexNET se han completado incluyendo más trazas de operación; y se ha implementado una solución SIEM (Security Information Event Management) para recoger, analizar y priorizar los eventos de seguridad dentro de la red.

Este acceso por unos usuarios a los datos personales de otros usuarios de Lexnet, supone la comisión, por parte de la Subdirección General de Nuevas Tecnologías de la Justicia dependiente de la Secretaría General de la Administración de Justicia, Secretaria de Estado de Justicia, Ministerio de Justicia, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por una deficiente implementación de las medidas de seguridad obligatorias según la naturaleza y el nivel de seguridad asignado al fichero en cuestión. En consecuencia, dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que la SGNTJ es responsable de la misma.

V

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

En Sentencia de 19/10/2010, la Audiencia Nacional considera conforme la resolución recurrida, en la que se graduó la multa tomando en consideración la existencia de medidas de seguridad. En dicha Sentencia se declara que *"La Administración le impuso, no obstante, una sanción de… utilizando los criterios de corrección del art. 45.4 de la LOPD, al haber ponderado que la empresa tenía medidas de seguridad…"*.

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso*

"que se ha empleado la diligencia que era exigible por quien aduce su inexistencia." (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."* (SAN 29de junio de 2001).

Por otra parte, ha de señalarse que es la entidad responsable la obligada última a garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

La SGNTJ en las alegaciones a la propuesta de resolución ha enunciado las cincuenta y ocho medidas preventivas planificadas para garantizar la no repetición del incidente de seguridad, y que se agrupan en las siguientes categorías: la Oficina de Seguridad, un convenio de colaboración con el CCN, la creación de un Centro de Control, la creación de una Oficina de Gestión del Servicio, la mejora de la calidad del código, la revisión de la ejecución de comandos o el acceso a datos, la revisión de la gestión de la autenticación, el filtrado adecuado de datos, la revisión de los esquemas de autorización, la prevención de suplantación al usuario, la eliminación de la posibilidad de filtrado de datos sensibles, la actualización de los componentes software, la mejora de la configuración de seguridad de los sistemas de información, la mejora de estrategias de detección de ataques y otros aspectos organizativos y legales. Sin entrar en esta resolución a describir los detalles técnicos de la misma, por evidentes motivos de seguridad, se tiene constancia que veintisiete de dichas medidas ya se han implementado, mientras que el resto de ellas se encuentran en desarrollo o fase de pruebas. La SGNTJ ha ido informando de dicho progreso durante la tramitación del procedimiento y se consideran que son medidas adecuadas para el caso que nos ocupa.

VI

El artículo 44.3.h) de la LOPD, considera infracción grave:

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, al modificar el programa de acceso de usuarios de LexNET a buzones de otros usuarios, se considera que la Subdirección General de Nuevas Tecnologías de la Justicia ha incurrido en la infracción grave descrita.

VII

El artículo 10 de la LOPD establece: "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".*

El deber de secreto profesional que incumbe a los responsables de los ficheros y a todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal, recogido en el artículo 10 de la LOPD, comporta su obligación de no revelar ni dar a conocer su contenido, así como *"deber de guardarlos".* Continúa dicho artículo añadiendo: *"obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".* Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, y por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste, precisamente, el secreto.

Este deber de sigilo resulta esencial en la sociedad contemporánea, cada vez más compleja, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de los derechos fundamentales, como el derecho a la protección de los datos personales, que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un *"instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos"* (Sentencia del Tribunal Constitucional 292/2000). Este derecho fundamental a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias de la dignidad de la persona.

En este caso concreto, se han difundido datos personales que tenían unos usuarios de LexNET y pudieron ser vistos por otros usuarios.

Se trata de valorar si se ha vulnerado el principio del deber de secreto, consagrado en el artículo 10 de la LOPD, que obliga al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal.

En este caso ha quedado acreditado que el sistema LexNET no impidió que unos usuarios accedieran a la información de otros usuarios. Como ya se ha señalado, al subsanarse el problema de seguridad que se produjo, ya se impidió que terceros accedieran a información a la que no debían tener acceso.

La conducta de la SGNTJ se incardina en el artículo 44.3.d) de la LOPD que indica como tal: "*La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley*."

De acuerdo con los fundamentos anteriores, hay que entender que por parte de la SGNTJ se ha producido una vulneración del deber de secreto, dado que se han difundido los datos de carácter personal concernientes a terceros, y que procede calificar la infracción como infracción grave.

El hecho constatado de la difusión de datos personales fuera del ámbito de los afectados, establece la base de facto para fundamentar la imputación de la infracción del artículo 10 de la LOPD.

VIII

El hecho constatado de la difusión de datos personales a terceros establece la

base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia de que la comisión de una implica necesariamente la comisión de la otra. Esto es, si una documentación que contiene información sobre datos personales sale del ámbito de la responsable de su confidencialidad, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que señala que: *"Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*", procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto calificado como grave en el artículo 44.3.d) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD por tratarse de la infracción originaria que ha dado lugar a la comisión de la otra infracción.

IX

El artículo 46 de la LOPD, *"Infracciones de las Administraciones Públicas"*, dispone:

"1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

En el supuesto objeto de este procedimiento, se considera que se han tomado las medidas adecuadas para evitar que se vuelva a producir el incidente de seguridad referido, por lo que no se requiere al responsable de LexNET a la adopción de nuevas medidas.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DECLARAR que el MINISTERIO DE JUSTICIA (Subdirección General de Nuevas Tecnologías de la Justicia) ha infringido lo dispuesto en el artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución al MINISTERIO DE JUSTICIA (Subdirección General de Nuevas Tecnologías de la Justicia).

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

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

Contra esta resolución, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la 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.

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