



Expediente Nº: E/05316/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **DIRECCION GENERAL GUARDIA CIVIL** en virtud de denuncia presentada por D. **C.C.C.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 27 de junio de 2013, tuvo entrada en esta Agencia escrito de D. **C.C.C.**, en el que denuncia que, ejerciendo funciones de Secretario Jurídico de Asociación Unificada de la Guardia Civil –AUGC-, tiene la responsabilidad del asesoramiento jurídico en los expedientes disciplinarios que se tramitan a los asociados de AUGC HUELVA y como consecuencia tiene contacto habitual durante toda la tramitación de los expedientes con los guardias civiles encartados. Que desde el pasado año 2012, coincidiendo con el destino del Comandante D. **D.D.D.** a la Comandancia de Huelva y ser el instructor encargado de la mayoría de los expedientes por falta grave que se tramitan en la Comandancia, ha venido recibiendo quejas, de que, la mayoría expedientes disciplinarios, son entregados a los encartados sin ningún tipo de confidencialidad, bien, por el Jefe más inmediato del encartado, o por algún mando o guardia civil, quejándose los mismos de la publicidad que tienen dichos expedientes, llegándose a enterar en alguna ocasión antes los guardias civiles del Puesto, que los propios encartados o bien, teniendo conocimiento de ello, incluso algunos guardias o mandos que posteriormente tendrían que declarar en el mismo.

Tras recibir estas quejas, la AUGC ha realizado una investigación con los propios guardias que han sido encartados en los expedientes y algunos de ellos han coincidido, en que el expediente disciplinario así como los documentos, pliego de cargos, propuesta de resolución, alegaciones, informaciones reservadas, resoluciones sancionadoras, etc, se está enviando por e-mail, desde el Negociado de Expedientes de la Comandancia de Huelva, por parte del Instructor de los mismos, a las Compañías territoriales y estos a su vez, lo remiten por el mismo procedimiento al Puesto donde pertenece el encartado, de forma tal, que puede ser visto, por los guardias civiles destinados en la Oficina de la Compañía de Plana Mayor de cada Compañía, por el propio Capitán, que muchas veces tiene que manifestar con posterioridad y desde aquí, al Puesto, donde cualquier guardia civil puede tener acceso al expediente ya que se remite sin ninguna confidencialidad, se ha dado el caso incluso, que ha sido llevado por dos guardias civiles al mismo domicilio del encartado, cuando ya ni siquiera pertenecía a la Unidad de esos guardias civiles.

Tras hablar con todos los encartados que son asociados de AUGC HUELVA, en concreto con los que se relacionan a continuación estos han señalado lo siguiente:

-Expediente por falta grave núm. ****1/12, instruido al Sargento D. **O.O.O.**

Expediente por falta grave núm. ****1/12 instruido al Cabo 1º D. **K.K.K.**

Expediente por falta grave núm. ****1/12, instruido al Guardia Civil D. **M.M.M.**

Estos Guardias Civiles están destinados en el Puesto Principal de Ayamonte, los expedientes y los documentos posteriores, fueron remitidos por e-mail al correo de la Compañía de la Plana Mayor y estos a su vez, al Puesto, donde podo ser visto por el guardia de servicio burocrático, por el propio Comandante de Puesto, que era parte implicada en el expediente, que posteriormente tenía que declarar y por cualquier guardia civil que tuviera acceso, toda vez, que muchos de ellos poseen las claves para ver el correo electrónico del Puesto.

Así mismo, se tiene conocimiento que incluso fue impreso alguno de ellos por el Comandante de Puesto y entregado a los encartados, varios días después, el mismo trámite ha llevado el pliego de Cargos, la propuesta de resolución y la resolución siempre por e-mail, siendo vistos por personal que no debería verlo.

-Expediente por falta grave núm. ****1/12, instruido al Guardia Civil D. **III.**

Este guardia civil está destinado en el Puesto de Chiva de la Comandancia de Valencia y también le han sido remitidos los documentos sin ninguna confidencialidad, siendo visto por personal del Puesto y de la oficina de la Unidad, que no deberían tener conocimiento al ser la instrucción de dichos expedientes confidencia.

Expediente por falta grave núm. ****2/12 instruido al Guardia Civil DON **L.L.L.**

Este Guardia Civil está destinado en el Puesto de Rociana del Condado, fue denunciado por el Sargento Comandante de Puesto, en la instrucción del mismo, tenían que declarar el Sargento, Cabo y algunos Guardias Civiles, fue remitido por e-mail desde el negociado de expedientes a la Compañía de La Palma del Condado y de este al Puesto, allí fue abierto el correo por un guardia civil, posteriormente- por el Sargento que lo entregó al encartado, después de imprimirlo y dejarlo un tiempo en la bandeja de los documentos, todos los guardias del puesto tenían conocimiento del expediente.

-Expediente por falta grave núm. ****3/12 instruido al Guardia Civil DON **L.L.L.**

Siguió el mismo procedimiento que el anterior, todos los documentos fueron enviados por email sin confidencialidad ninguna y pudiendo ser visto por el Comandante de Puesto que era quien lo denunciaba y otros documentos como pliego de cargos y propuesta de resolución fue entregado incluso por algún guardia en su domicilio del Acuartelamiento.

Este Guardia Civil presentó escrito solicitando la confidencialidad.

-Expediente por falta grave núm. ****4/12 instruido al Guardia Civil D. **J.J.J.**

A este Guardia Civil se le ha enviado por email desde el Negociado de Expediente de la Comandancia de Huelva, al Puesto de Sevilla por email, para que allí fuera entregado por el Comandante de Puesto, diversa documentación como pliego de cargos, propuesta de resolución, resolución sancionadora, no preservando la confidencialidad.

-Expediente por falta grave núm. ****5/12, instruido al Guardia Civil D. **Q.Q.Q.**

Al igual que el anterior expediente y documentación se ha remitido por email desde el Negociado de Expedientes al email del Puesto de Sevilla, sin confidencialidad, para ser entregado por el Comandante de Puesto

-Expediente por falta grave núm. ****6/12 instruido al Guardia Civil D. **E.E.E.**

Este Guardia Civil, está destinado en el Puesto de Torre la Higuera, y la documentación le ha llegado también por email, sin confidencialidad ninguna, y en la misma, se encontraba en su interior informaciones reservadas, así mismo se le remitió por el mismo sistema todas las resoluciones propuestas y todo el expediente.

-Expediente por falta grave núm. ****7/13, instruido al Guardia Civil D. **N.N.N.**

Este Guardia Civil, se encontraba pendiente de asignación de destino y su domicilio era en la localidad de Corrales, distante 5 kms. de la Comandancia de Huelva, el expediente fue remitido a su anterior destino el Servicio Marítimo Provincial de Huelva, allí fue impreso y se le entrego a dos guardias civiles de dicha Unidad para que se lo entregaran en su domicilio, sin ningún tipo de confidencialidad, sobre cerrado, ni nada que preservara que no tuvieran



conocimiento del mismos los guardias civiles que lo llevaban y los que estaban en la oficina de la Plana Mayor, a pesar que en el mismo tenían que declarar el Capitán Jefe del Servicio Marítimo Provincial, un Sargento y un Cabo, al poder tener conocimiento del mismo estos guardias civiles que lo transportaron y los de la oficina se vulneró la confidencialidad, así mismo otros dos guardias civiles le entregaron el pliego de cargos.

Este guardia civil presentó escrito para que se preservara su intimidad y se le ofrecieran explicaciones por el tramite seguido, que obra en el expediente disciplinario, después de esto, le han sido entregado otros documentos en sobre cerrado con el sello de confidencial.

-Expediente por falta muy grave núm. ****8/13 instruido al Guardia Civil D. **H.H.H.**

Al igual que los anteriores y a pesar que está destinado en el Puesto de Punta Umbría distante 14 kms de la Comandancia, el expediente fue remitido por e-mail a la compañía de la Plana Mayor de Moguer y posteriormente por el mismo sistema al puesto, se dio la circunstancia que fue informado por compañeros de la Unidad, antes de que le fuera entregado el mismo, porque ya se tenía conocimiento al haberlo recibido por email, sin confidencialidad ninguna.

Este se está tramitando pero es de suponer que el resto de documentos seguirá el mismo procedimiento.

-Expediente por falta grave núm. ****9/13, instruido al Guardia Civil D. **P.P.P.**

Este Guardia Civil se encuentra destinado en el Destacamento del Seprona de Doñana, fue su propio comandante de Puesto el que lo denunció, declaró un Cabo 1º y además el suboficial, pues el expediente le fue entregado por este mismo Suboficial y así se ha realizado con el resto de documentos, también se está tramitando por lo que es de suponer que seguirá los mismos trámites y que pliego de cargos, propuesta de resolución y resolución se envíen por email y que pueda ser visto por el Suboficial que probablemente será nuevamente llamado a declarar y por algún miembro de la Unidad y también tendrá que declarar.

-Expediente por falta grave núm. ***10/13, instruido a los Guardias Civiles D. **F.F.F.** y D. **G.G.G.**

Estos Guardias Civiles están destinados en el Puesto de Isla Cristina y ha sido remitido el expediente por email desde el Negociado de Expediente de la Comandancia de Huelva al email de la Compañía de Plana Mayor, donde ha podido ser visto, por el Capitán que emitió el parte disciplinario, por el Brigada y por dos guardias civiles allí destinado que no deberían tener conocimiento del expediente.

El expediente fue remitido al Puesto de Isla Cristina y estos Guardias Civiles tuvieron conocimiento de la apertura del expediente por sus propios compañeros, cuando todavía ni siquiera había sido entregado por su Comandante de Puesto, prueba evidente que con el sistema que se está utilizando se está vulnerando la intimidad de los Guardias Civiles encartados en los expediente.

Este también se está tramitando pero es de suponer que seguirá el mismo trámite que los anteriores.

Así se han ido remitiendo durante todo el año 2012 y 2013, los expedientes disciplinarios en la Comandancia de Huelva

Estos hechos se están produciendo desde el año 2012, porque con anterioridad o bien los guardias civiles eran citados al negociado de expedientes donde se les entregaban los documentos por parte del instructor o el secretario o bien eran remitidos a la Unidad, en sobre cerrado con el sello de confidencial, que el Jefe de la Unidad entregaba al encartado y este firmaba el recibí de dicho sobre, con lo que se respetaba escrupulosamente la



confidencialidad de los mismos.

Consideran también que con el sistema que se está utilizando actualmente, además de la intimidad de los encartados, se les está produciendo una indefensión, porque sus expedientes pueden ser vistos por guardias civiles que no tienen la necesidad de verlos y porque pueden ser vistos también por aquellos que hayan sido los denunciados o por los que posteriormente declararan como testigos.

Así mismo, existen documentos dentro del expediente, como citaciones para declarar que no necesitan confidencialidad, pero nadie salvo el instructor y el secretario debe tener conocimiento de las alegaciones presentadas de lo que declaran los testigos y de pliego de cargos, propuestas de resoluciones o de las sanciones.

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 y con fecha 23 de junio de 2014, la Dirección General de La Guardia Civil, ha remitido a esta Agencia, informe de su Asesoría Jurídica en relación con los hechos denunciados, en el que se pone de manifiesto que:

1. El denunciante, aunque dice actuar como Secretario Jurídico Provincial de AUGC, no acredita por ningún medio válido en derecho dicha representación ni el cargo que manifiesta ostentar.

2. El denunciante tampoco acredita que en todos y cada uno de los expedientes disciplinarios que relaciona él haya sido designado por los encartados para ejercitar su derecho de defensa, ni que cuente con el consentimiento expreso de los encartados para divulgar los datos confidenciales de sus expedientes disciplinarios, lo que podría determinar su responsabilidad y la de la Asociación a la que dice pertenecer por infracción a la Ley de Protección de Datos.

3. El Comandante Instructor, D. **D.D.D.**, a quien se alude en el escrito de denuncia, ha informado que las comunicaciones o notificaciones efectuadas por el órgano instructor a los interesados con ocasión de los procedimientos disciplinarios que, contra ellos se dirigen, se suelen realizar indistintamente mediante correo ordinario o correo electrónico oficial corporativo Groupwise, siempre con el tratamiento de información confidencial, haciendo uso de sobres cerrados para dicho tratamiento y dirigidos para ser abiertos exclusivamente por sus destinatarios en el caso de correo ordinario, o bien haciendo uso del medio telemático oficial corporativo reseñado, con expresa advertencia en su contenido de la especial protección de los datos contenidos o adjuntos y los correspondientes avisos legales que ello supone. Las notificaciones y comunicaciones se suelen cursar siempre por conducto de las Compañías territoriales de cada una de las Unidades de destino de los interesados, en las que el acceso a la información cuenta con mayor grado de restricción y reserva por hallarse limitado el personal que asume las funciones de recepción de la información.

4. Así mismo, el citado Comandante, que fue destinado a la Comandancia de Huelva el 27 de noviembre de 2011, ha informado que el procedimiento de notificación y comunicación a los interesados de los diferentes expedientes disciplinarios empleado desde su destino, no difiere del empleado por otros instructores en otros procedimientos disciplinarios de dicha Comandancia, ni tampoco difiere del que se venía usando por los instructores y secretarios de procedimientos disciplinarios con anterioridad a su incorporación.

5. En el caso concreto del Expediente Disciplinario FG****1/12, indica que se hallaban encartados cuatro componentes del Cuerpo, tres de ellos destinados en el Puesto Principal de Ayamonte de la Comandancia de Huelva, uno de los cuales se hallaba realizando el curso de acceso a la Escala de Suboficiales en la Academia de Baeza (Jaén), y el último en el Puesto de Chiva, de la Comandancia de Valencia. Dicha



disparidad geográfica junto a la complejidad de la instrucción, hacían aconsejable para evitar su caducidad el uso de las nuevas tecnologías para los trámites de comunicación de los distintos momentos procesales a los interesados, siempre sin que ello suponga merma de las medidas de seguridad inherentes a los datos de carácter disciplinario tratados.

6. La denuncia interpuesta no cuestiona el buen uso del correo ordinario en la tramitación de los expedientes disciplinarios, centrandó única y exclusivamente lo hechos denunciados en el uso de medios ofimáticos y telemáticos, no obstante la utilización de estos medios está expresamente prevista en el artículo 45.2 de la Ley Disciplinaria, al disponer que: "las comunicaciones entre las autoridades, mandos y órganos que intervengan en la tramitación se efectuarán directamente, sin traslados intermedios. Estas comunicaciones y las que deban tener lugar con los interesados se lleven a cabo, en lo posible, a través de medios ofimáticos y telemáticos, siempre que reúnan los requisitos exigidos en materia de comunicaciones electrónicas", siendo en MINISTERIO muchas ocasiones su utilización absolutamente imprescindible para poder resolver la notificación de los expedientes en el plazo de 6 meses establecido en el artículo 65 de la misma Ley.

7. En caso de sobrepasarse el plazo de 6 meses, se produce la caducidad del expediente disciplinario, lo que no impide la instrucción de uno nuevo si la infracción apreciada no hubiere prescrito, con los consiguientes perjuicios también para los interesados que se tratan de evitar con el uso de los medios electrónicos para efectuar las comunicaciones y' notificaciones, asegurando siempre la debida confidencialidad, lo que también se hace en la Comandancia de Huelva

8. Respecto a la gestión de la documentación a la que se hace referencia en la denuncia, la Comandancia de Huelva, ha informado de lo siguiente:

a) La remisión de la misma, se ha realizado, en todos los casos, por medio de correo electrónico denominado Groupwise, cuyo uso está regulado por la Orden General núm. 14, de 2 de julio de 2001, sobre Normas para la implantación y empleo del Correo Electrónico en el Cuerpo.

b) El artículo 1 de dicha norma tiene por objeto *"Regular la implantación y empleo del correo electrónico en las comunicaciones internas entre las UCO,s de la Guardia Civil y serán de aplicación a todos los usuarios de cuentas de correo electrónico de la red intranet del Cuerpo y a los mensajes que se cursen a través de la misma. Se tendrán cuentas de Unidad, de Cargo o de Función"*.

c) Por otra parte, el artículo 45.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establece que *"Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes."*

d) Por tanto, el empleo del medio electrónico (correo interno) está plenamente respaldado por la citada normativa.

9. Respecto a las medidas de seguridad implantadas sobre la transmisión de documentos mediante correo electrónico se detallan en la Instrucción Técnica del Correo Electrónico Corporativo, de noviembre de 2002 (modificada en junio de 2006) señala que "la plataforma de correo interno, al estar basada en una plataforma propietaria, utiliza una encriptación tanto en las comunicaciones a través de la red, como en el almacenamiento de los mensajes, por lo que aumenta el grado de seguridad del sistema. El uso de certificación y firma digital en aquellas comunicaciones que lo requieran, complementa la citada seguridad".



10. Así mismo, la Orden General núm. 11, de 8 de mayo de 2000, sobre tramitación y transmisión de mensajes indica, en el apartado sexto, relativo a materiales clasificados, que "los escritos y mensajes, que en su caso correspondan, deberán ser calificados en cuanto a su seguridad, por la persona que autorice su transmisión, con uno de los conceptos de "SECRETO", "RESERVADO" o "CONFIDENCIAL", de acuerdo con los criterios establecidos en las Instrucciones de 14 de octubre de 1988 y 1 de febrero de 1991, del Secretario de Estado de Seguridad y cumplimentados con las formalidades establecidas en la misma".

11. Respecto a la dependencia de la gestión de la cuenta de correo asignada a una Unidad, se detalla en la Orden General número 14/2001, que establece que *"Es la asociada de forma inequívoca a una Unidad, Centro u Organismo del Cuerpo: Existirán dos cuentas de este tipo:*

a) De registro

b) De servicio.

c) Se creara una cuenta de UNIDAD-Registro en todas aquellas UCO,s que dispongan actualmente de registro de correspondencia, ya sea registro general o auxiliar, siendo su encargado el responsable de dicha cuenta de correo, el cual deberá abrir y distribuir los mensajes dirigidos a la misma, así como registrar y archivar los enviados y recibidos, devolviendo al remitente aquellos erróneamente recibidos, con indicación en su caso, de las acciones realizadas con los mismos.

12. Por tanto, el medio utilizado para la transmisión de la documentación relativa a expedientes disciplinarios es adecuado por cumplir los requerimientos de seguridad establecidos al efecto. Además, la referida normativa determina la persona con responsabilidad por el debido tratamiento de la información transmitida.

13. De esta forma, el medio utilizado por el Negociado de Expedientes de la Comandancia de Huelva se ajusta plenamente a la normativa relacionada con la custodia de soportes del artículo 108 del R.D. 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos, que establece que *"mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada"*.

14. Respecto a las normas dadas a las distintas Unidades, en la Intranet Corporativa, en la página del Servicio de Innovación Tecnológica y Seguridad de la Información (SiTy SI), dependiente de la Jefatura de los Servicios Técnicos de la Subdirección General de Apoyo, se encuentra la Normativa de Seguridad de los Sistemas de Información y Comunicaciones, entre las que se recogen las siguientes:

Normas Básicas de Seguridad DSEG-A064-V05.

Normativa Seguridad del Correo Electrónico PSEG-A034-V04

15. Por todo lo expuesto en el informe, manifiestan que desde el año 2012 no ha existido ninguna variación en el procedimiento de notificación y comunicación a los interesados de los diferentes expedientes disciplinarios en la Comandancia de Huelva, en contra de lo manifestado por el denunciante, y el empleado no difiere del utilizado por otros instructores en otros procedimientos disciplinarios de dicha Comandancia, ni tampoco difiere del que se venía usando por los instructores y secretarios de procedimientos disciplinarios con anterioridad a la incorporación del citado Comandante.



16. Así mismo, consideran que la afirmación hecha por el denunciante de que el sistema actual, además de afectar a la intimidad de los encartados, les produce indefensión porque sus expedientes pueden ser vistos por guardias civiles que no tienen necesidad de verlos y porque pueden ser vistos también por aquellos que hayan sido los denunciados o por los que posteriormente declararán como testigos, no deja de ser una aseveración genérica que no se ajusta a la realidad, al garantizar debidamente el procedimiento establecido la confidencialidad de la documentación transmitida, así como la identificación de los responsables del tratamiento.

17. Consideran además, que en el hipotético supuesto de que pudiera producirse alguna de dichas vulneraciones en un expediente disciplinario en concreto, el encartado o su letrado la podrían invocar en los distintos trámites del mismo, lo que redundaría en perjuicio de la propia Institución que lo ha ordenado incoar y que tiene interés en corregir las conductas contrarias a la disciplina de sus miembros.

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

Con carácter previo, se observa que el denunciante se irroga una representación, Secretario Jurídico Provincial de la AUGC, que no justifica, y basa la denuncia en la falta de “confidencialidad” que impera en la Comandancia de Huelva a causa del medio de comunicación utilizado el correo electrónico en las comunicaciones de las diferentes actuaciones de los expedientes disciplinarios a los afectados que causan accesos injustificados por terceros, así como la revelación de datos de los expedientados a miembros del Cuerpo de dicha Comandancia, conducta que la atribuye al inicio de sus funciones del actual Comandante .

En forma análoga, se observa respecto a la formulación de los diferentes hechos denunciados la “generalidad” con que se formulan relativos a los procedimientos disciplinarios que se relacionan ya que no se justifica los motivos por los que la utilización del correo electrónico (por cierto, “corporativo” que no se menciona) para traslado de comunicaciones de actuaciones de expedientes comporta el acceso indebido por terceros (miembros del cuerpo) como tampoco justifica que desde el punto de vista organizativo de la Comandancia de Huelva el conducto utilizado para las comunicaciones a la Compañía de la Plana Mayor , a la Compañía Territorial y al Jefe del Puesto se califiquen de accesos indebidos sin razonar los motivos por los que el traslado de las actuaciones a través de unidades orgánicas suponen revelación de datos a terceros ajenos.

III

El contenido de los hechos denunciados plantean, de un lado la falta de “confidencialidad” en la Comandancia de la G.C en la provincia de Huelva por la utilización indebida del “correo electrónico corporativo” para la comunicación de las actuaciones en los expedientes disciplinarios seguidos a los miembros del cuerpo y, por otro lado, el acceso injustificado a consecuencia del traslado de las actuaciones a través de la Compañía de Plana Mayor, Dirección Territorial y Puesto de mando de la GC por miembros que deben ser ajenos al conocimiento de los expedientes. Es decir, denuncia que se viene produciendo a partir del año 2012 y 2013 una generalizada la falta de “confidencialidad” en la instrucción de los expedientes disciplinarios que redundan revelaciones de datos de expedientes disciplinarios a terceros ajenos y ello porque en la tramitación de los expedientes disciplinarios se incumplen las *medidas de seguridad* implantadas.

El artículo 10 de la LOPD, recoge

“ 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 aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”.

Y el artículo 9 de la LOPD dispone lo siguiente:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las



condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.”

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Para poder delimitar cuáles son 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 al concepto de “*fichero*” el artículo 3.b) de la LOPD lo define como “*todo conjunto organizado de datos de carácter personal*”, con independencia de la modalidad de acceso al mismo condición que reúne el expediente disciplinario ya sea soporte papel o automatizado.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la “*comunicación*” o “*consulta*” de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Sintetizando las previsiones legales citadas 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, regulado en normas reglamentarias.

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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, 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 el artículo 81.1 del mismo Reglamento señala 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, correspondiendo a los ficheros que contengan datos sobre infracciones administrativas y penales el nivel medio .

Esta necesidad de especial diligencia en la custodia de la documentación por el



responsable del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11 de diciembre de 2008 (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 adopten 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”*.

Esta Agencia se ha manifestado respecto a la utilización del correo electrónico como medio de notificación de actuaciones administrativas, con cita de la Ley 30/1992, de 26/11, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –LRJPAC- en su artículo 45 que señala lo siguiente:

“1. las Administraciones Públicas, impulsaran el empleo y aplicación de las técnicas y medios electrónicos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes”

Y el artículo 59 dispone lo siguiente:

“ Las notificaciones se practicarán por cualquier medio que permita tener constancia de la recepción por el interesado o su representante, así como de la fecha. La identidad y el contenido del acto notificado. La acreditación de la notificación se incorporará al expediente”.

Por su parte, la Ley 11/2007, de Acceso Electrónico de los ciudadanos a los servicios públicos, establece en su artículo 1 que:

“2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.”

Y el Artículo 27 “ Comunicaciones electrónicas”, dispone

“7. Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes”.

A mayor abundamiento, la Guardia Civil acredita disponer de diversa normativa que regulan el uso de las comunicaciones telemáticas. La Ley Disciplinaria de la G.C en el artículo 45.2 dispone que:

“las comunicaciones entre las autoridades, mandos y órganos que intervengan en la tramitación se efectuarán directamente, sin traslados intermedios. Estas comunicaciones y las que deban tener lugar con los interesados se lleven a cabo, en lo posible, a través de medios ofimáticos y telemáticos, siempre que reúnan los requisitos exigidos en materia de comunicaciones electrónicas”,

La Orden General núm. 14, de 2 de julio de 2001, sobre Normas para la implantación y empleo del Correo Electrónico en el Cuerpo su artículo 1 establece como objeto *“Regular la implantación y empleo del correo electrónico en las comunicaciones internas entre las UCO,s de la Guardia Civil y serán de aplicación a todos los usuarios de cuentas de correo electrónico de la red intranet del Cuerpo y a los mensajes que se cursen a través de la misma. Se tendrán cuentas de Unidad, de Cargo o de Función”*.



Y respecto a las medidas de seguridad implantadas sobre la transmisión de documentos mediante correo electrónico se detallan en la Instrucción Técnica del Correo Electrónico Corporativo, de noviembre de 2002 (modificada en junio de 2006) que señala *"la plataforma de correo interno, al estar basada en una plataforma propietaria, utiliza una encriptación tanto en las comunicaciones a través de la red, como en el almacenamiento de los mensajes, por lo que aumenta el grado de seguridad del sistema. El uso de certificación y firma digital en aquellas comunicaciones que lo requieran, complementa la citada seguridad"*.

Así mismo, la Orden General núm. 11, de 8 de mayo de 2000, sobre tramitación y transmisión de mensajes indica, en el apartado sexto, relativo a materias clasificadas, que *"los escritos y mensajes, que en su caso correspondan, deberán ser calificados en cuanto a su seguridad, por la persona que autorice su transmisión, con uno de los conceptos de "SECRETO", "RESERVADO" o "CONFIDENCIAL", de acuerdo con los criterios establecidos en las Instrucciones de 14 de octubre de 1988 y 1 de febrero de 1991, del Secretario de Estado de Seguridad y cumplimentados con las formalidades establecidas en la misma"*. Y respecto a la dependencia de la gestión de la cuenta de correo asignada a una Unidad, se detalla en la Orden General número 14/2001, que establece que *"Es la asociada de forma inequívoca a una Unidad, Centro u Organismo del Cuerpo: Existirán dos cuentas de este tipo:*

- a) De registro
- b) De servicio.
- c) Se creara una cuenta de UNIDAD-Registro en todas aquellas UCO,s que dispongan actualmente de registro de correspondencia, ya sea registro general o auxiliar, **siendo su encargado el responsable de dicha cuenta de correo, el cual deberá abrir y distribuir los mensajes dirigidos a la misma, así como registrar y archivar los enviados y recibidos, devolviendo al remitente aquellos erróneamente recibidos, con indicación en su caso, de las acciones realizadas con los mismos.**

Por tanto, de acuerdo con la normativa citada se puede concluir que el medio utilizado para la transmisión de la documentación relativa a expedientes disciplinarios es adecuado por cumplir los requerimientos de seguridad establecidos al efecto **y además, la referida normativa determina la persona con responsabilidad por el debido tratamiento de la información transmitida.** De esta forma, el medio utilizado por el Negociado de Expedientes de la Comandancia de Huelva se ajusta a la normativa relacionada con la custodia de soportes del artículo 108 del R.D. 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos, que establece que *"mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada"*. y de acuerdo a la normativa citada el traslado en la Comandancia de Huelva entre sus unidades, Compañía de la Plana Mayor, Dirección Territorial y el Puesto de destino, cuando utiliza el correo electrónico está habilitado para utilizar dicho telemático.

IV

La Sentencia de la Audiencia Nacional de 28 de junio de 2013, recurso nº 00024/2012, se refiere a las Medidas de Seguridad previstas en el artículo 9 de la LOPD en el Fundamento de Derecho Cuarto al recoger:

<<El artículo 9.1 LOPD, que traspone el artículo 17 de la Directiva 9546/CE, recoge en su apartado 1 la necesidad de la adopción de medidas técnicas y organizativas necesarios para



garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, obligación que impone al responsable del fichero y, en su caso, al encargado del tratamiento.

En interpretación del artículo 9 de la LOPD, esta Sala ha señalado en múltiples sentencias, (SSAN, Sec. 1ª, de 13 de junio de 2002, Rec. 1517/2001; 7 de febrero de 2003 Rec. 1182/2001; 25-1-2006 Rec. 227/2004; 28 de junio de 2006 Rec. 290/2004 etc), que la obligación que dimana del artículo 9 de la LOPD no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, en concreto recoge " Se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva ... la recurrente es, por disposición legal, una deudora de seguridad en materia de datos ... y puesto que ... es una deudora de seguridad en materia de datos ... es insuficiente, según se desprende de la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad ... también es responsable de que las mismas se cumplan y ejecuten con rigor. En definitiva toda responsable de un fichero (o encargada de tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica, sin que bajo ningún concepto, datos bancarios o cualesquiera otros de carácter personal puedan llegar a manos de terceras personas".

(...) El artículo 91 dispone, entre otros particulares, que los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones, el responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. El 113, por su parte, establece: 1. El acceso a la documentación se limitará exclusivamente al personal autorizado; 2. Se establecerán mecanismos que permitan identificar en el caso de documentos que puedan ser consultados por varios, y 3. El acceso de personas no incluidas en el párrafo anterior deberá quedar debidamente registrado de acuerdo con el procedimiento establecido.

(...) La cuestión en la que discrepan la AEPD y la actora se refiere, esencialmente, a que tienen acceso a la caja fuerte, situada en el sótano de la entidad en la que se guarda la documentación médica, no solo el Director médico, sino también los Directores Generales. Para la AEPD, el que estos Directores puedan tener acceso al lugar en que se guarda dicha documentación supone una vulneración del principio de seguridad, aunque no se haya demostrado que se haya producido ningún acceso a la repetida documentación médica. Para la actora, la documentación médica está separada del resto de la documentación de la entidad, según el documento de seguridad no están autorizadas personas distintas del Directo Médico para acceder a dicha documentación y, además, se encuentra en soporte papel guardada en sobres cerrados, identificados con el anagrama del Centro médico Creu Blanca, y depositada en compartimentos (estanterías) debidamente separados de otros en los que se guarda otro tipo de documentación a la que sí pueden acceder los Directores Generales. Finalmente, añade la actora que existe un registro de accesos a la citada caja fuerte y no consta que se haya producido ningún acceso indebido o pérdida de documentación.

En el caso concreto, aunque las medidas de seguridad puedan ser objeto de mejora, no cabe entender vulnerado el principio de seguridad del artículo 9.1 de la LOPD, respecto los datos de salud de los trabajadores de la Mutua que figuran en los citados documentos médicos, porque dichos datos están guardados en sobres cerrados, perfectamente identificados y separados del resto de documentación, como así se comprobó en la inspección



practicada, estando limitado el acceso a los mismos al Director Médico, según el documento de seguridad, y según lo manifestado por el Dr... en vía administrativa, A.A.A., quedando registrado el acceso de las personas que acceden a la citada caja fuerte”.

En el caso analizado, ha quedado probado que la utilización del correo electrónico corporativo es apto para la realización de comunicaciones administrativas; que existe un responsable de la recepción de los correos y su distribución sin que se haya probado el acceso a las actuaciones de los expedientes disciplinarios por personas ajenas a la G.C ; que los miembros que acceden a las comunicaciones están sujetos al deber de confidencialidad de los hechos que conozcan por razón de su cargo; y que, asimismo, el traslado de las actuaciones a los responsables de las unidades orgánicas, Compañía de Plana Mayor; Dirección territorial y Puesto de Mando del afectado no suponen revelaciones indebidas sino el seguimiento de la cadena orgánica que quienes forman parte están sujetos al deber de secreto.

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 las presentes actuaciones.

2 **NOTIFICAR** la presente Resolución a la **DIRECCION GENERAL GUARDIA CIVIL** y a D. **C.C.C..**

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