Expediente Nº: E/00796/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., en virtud de denuncia presentada por Don ***A.A.A.***, Doña ***C.C.C.***, Doña ***B.B.B.*** y Don ***D.D.D.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 12 de febrero de 2018 la Autoridad Catalana de Protección de Datos remite a esta Agencia escrito de Don ***A.A.A.***, Doña ***C.C.C.***, Doña ***B.B.B.*** y Don ***D.D.D.*** (en lo sucesivo, los denunciantes), en el que denuncian lo siguiente:

Con fecha 2 de febrero de 2018 han presentado, junto con otras personas, todas ellas trabajadores del Departamento de Presidencia de la Generalidad de Cataluña, una denuncia ante la entidad SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., que adjuntan a efectos de poner en conocimiento de la autoridad competente en materia de protección de datos personales los hechos recogidos en la misma.

En dicha denuncia se pone de manifiesto que, con fecha 24 de noviembre de 2017, un grupo de trabajadores del Departamento de Presidencia de la Generalidad de Cataluña suscribió una carta dirigida al ex consejero Don ***E.E.E.*** depositada en esa misma fecha en un buzón ubicado en la plaza Sant Jaume de Barcelona, con destino a la cárcel de Estremera. Dicha carta fue firmada por los trabajadores con su nombre, apellidos y DNI.

Con fecha 30 de noviembre de 2017 tuvo entrada en el Registro General del citado departamento una carta anónima manuscrita, firmada el 28 de noviembre de 2017, donde se les comunicaba que se había encontrado el sobre con la carta dirigida al señor ***E.E.E.***, abierto y sin el sello de correos, en los alrededores de la sede central de Correos de Sant Cugat del Vallés. En el mismo documento anónimo constaba que también se había encontrado otra carta dirigida al ex vicepresidente Don ***F.F.F.***.

Aportan fotografías de la carta anónima recibida junto con el sobre encontrado en la vía pública con la carta dirigida al señor ***E.E.E.***.

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 (Informe E/00796/2018), teniendo conocimiento de los siguientes extremos:

Con fecha 21 de febrero de 2018 tiene entrada en esta Agencia escrito de la SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., en el que se pone de manifiesto que fueron conocedores de los hechos denunciados mediante escrito

remitido por los denunciantes a esa entidad, habiéndoseles facilitado repuesta, que se adjunta, en la que se les informó de lo siguiente:

- El tratamiento de los envíos depositados en los buzones, que por su naturaleza de envíos ordinarios no llevan asociados trazabilidad que permita su localización y/o seguimiento, se realiza en las primeras fases a través de un procedimiento sin intervención manual de los empleados, concretamente desde su recogida en los buzones hasta la formalización de su admisión, fase que conlleva matasellado de los elementos de franqueo.

- La cancelación o matasellado cumple, asimismo, la función de dar respuesta al mandato legal de informar a los usuarios de los servicios postales cuál es la identidad del operador postal que se hace cargo del envío y de la fecha en que se produce dicho evento.

- La ausencia de elementos indiciarios que evidencien que se haya producido la admisión de dicho envío en la red postal, pues tal como se alude en el escrito y se observa en las fotografías, no consta en su cubierta la impronta que genera la cancelación del franqueo, impide acreditar que el citado envío se haya admitido en la red y, consiguientemente, que las irregularidades referidas en su escrito se hayan producido en el ámbito de gestión de dicha sociedad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora 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

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 transcrito artículo 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".*

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 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, 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 92.3, respecto de la gestión de soportes y documentos, que "*En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte*".

Por tanto, la no adopción de dicha medida de seguridad podría suponer, por parte de la entidad SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., una infracción del citado artículo 9 de la LOPD. Dicha infracción se tipifica como grave en su artículo 44.3.h), que considera como tal *"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*".

III

Por otro lado, el artículo 10 de la LOPD establece que *"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."*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11, contiene un *"…instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute 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". "Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida.*"

El deber de secreto profesional que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido, teniendo el *"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*". Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la protección de datos a que se refiere la citada Sentencia del Tribunal Constitucional 292/2000, y por lo que

ahora interesa, comporta que los datos personales 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.

En el presente caso, se le imputa a la SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., una vulneración de dicho deber de guardar secreto, que se produjo al haberse encontrado en la vía pública, abierto, el sobre que fue depositado en el buzón de la plaza Sant Jaume de Barcelona, posibilitando el acceso de terceros a los datos de carácter personal de los firmantes de la carta, en concreto, su nombre, apellidos y DNI.

El artículo 44.3.d) de la LOPD califica como infracción grave *"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.*"

IV

El artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece:

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

De las actuaciones previas de investigación llevadas a cabo por esta Agencia no se derivan elementos probatorios de los que se infiera que la sociedad denunciada resulte responsable de los hechos constitutivos de infracción que se le imputan. Tal y como alega la denunciada, en las fotografías aportadas por los denunciantes no aparece el matasellado que indicaría que el sobre había sido admitido en la red postal, por lo que no hay acreditación de que los hechos se hubieran producido en el ámbito de gestión de dicha sociedad.

En este sentido, el artículo 3.c) de la LOPD define "tratamiento de datos" como "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*". En el presente caso, no hay acreditación de que la sociedad denunciada hubiera llevado a cabo un tratamiento de datos y que, en consecuencia, debiera ser considerada como responsable del tratamiento, que se define en el artículo 3.d) de la LOPD como "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*", siendo los responsables de los ficheros y los encargados de los tratamientos quienes están sujetos al régimen sancionador establecido en la LOPD, según lo dispuesto en su artículo 43.1.

En este orden de ideas, debe tenerse en cuenta que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin

excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones. Esto, porque el ejercicio del *ius puniendi*, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

En este sentido se ha pronunciado reiteradamente el Tribunal Constitucional, entre otras en SSTC 120/1994 y 76/1990, señalando en esta última que *"… la presunción de inocencia rige sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, sean penales, sean administrativas en general o tributarias en particular".*

Expone también el Tribunal Constitucional en la Sentencia 76/1990 que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".*

Por otra parte, la Sentencia del Tribunal Constitucional de 20/02/1989 afirma que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

Así mismo, se debe tener en cuenta lo que establece el artículo 53.2 la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: "*Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables, tendrán los siguientes derechos: (…) b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario*".

En el presente caso, en aplicación del principio de presunción de inocencia, que impide imponer una sanción en el caso de que exista una falta de pruebas respecto de un hecho concreto y determinante, no procede activar un procedimiento sancionador, al no estar acreditada la comisión de las infracciones imputadas. No resulta posible, por ello, imputar las conductas típicas y antijurídicas que establece el artículo 44.3 de la LOPD en sus letras h) y d) a la SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., siendo la solución procedente en derecho el archivo de las actuaciones.

V

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

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

SE ACUERDA:

- **PROCEDER AL ARCHIVO** de las presentes actuaciones.

- **NOTIFICAR** la presente Resolución a la entidad SOCIEDAD ESTATAL CORREOS Y TELEGRAFOS, S.A., y a Don ***A.A.A.***, Doña ***C.C.C.***, Doña ***B.B.B.*** y Don ***D.D.D.***.

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

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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