- **Procedimiento nº.: PS/00626/2014**

Recurso de reposición Nº RR/00312/2022

Examinado el recurso de reposición interpuesto por SINDICATO DE POLICÍAS DE CATALUÑA contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00626/2014, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 26/04/2022, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00626/2014, en virtud de la cual se imponía a la entidad SINDICATO DE POLICÍAS DE CATALUÑA una sanción de de 40.001 euros (cuarenta mil un euros), por la vulneración de lo dispuesto en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 05/05/2022, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la LOPDGDD, y supletoriamente en la LPACAP, en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00626/2014, quedó constancia de los siguientes:

*"1. En el Registro General de Protección de Datos, a fecha 23/12/2013, figuraba inscrito el fichero automatizado denominado "***FICHERO.1", cuya titularidad correspondía a la entidad SPC.* ***(…)***

2. La entidad SPC es titular de varias páginas web. Entre ellas, la página "spc-me.cat". Según declaraciones (…) ante la Direcció General de la Policía, del Departament d'Interior de la Generalitat de Catalunya, de fecha 25/10/2013, esta página cuenta con información sindical a la que acceden los afiliados mediante usuario y contraseña.

3. Según las manifestaciones realizadas por los representantes de la entidad SPC a los Servicios de Inspección de la AEPD, en octubre de 2013 el sistema de información de dicha entidad se encontraba alojado en un único servidor de la empresa que en ese momento le prestaba servicio de hosting.

(…).

(…)

(…)

4. Con fecha 23/10/2013, el servidor que alojaba el sistema de información de la entidad SPC sufrió un ataque informático llevado a cabo por terceros desconocidos. En visita de inspección de fecha 04/06/2014, los Servicios de Inspección de la AEPD pudieron acceder a un log del sistema atacado, de 23/10/2013, ***(…).***

En la declaración efectuada (…) ante la Direcció General de la Policía, del Departament d'Interior de la Generalitat de Catalunya, de fecha 25/10/2013, se dio cuenta de la intrusión al servidor del día 23/10/2013, a las 19:00 horas.

Los representantes de la entidad SPC manifestaron a los Servicios de Inspección de la AEPD que ***(…)*** *y que del análisis de los logs del servidor web, se comprobó que* ***(…)****.*

5. En la declaración efectuada (…) ante la Direcció General de la Policía, del Departament d'Interior de la Generalitat de Catalunya, de fecha 25/10/2013, se dio cuenta de la publicación en la dirección ******URL.1*** *de información contenida en la base de datos del servidor que alojaba la información de la entidad SPC. Se indica que* ***(…)*** *comprobó el acceso ilícito y la obtención de la información publicada en* ***"(…)"****.*

Asimismo, los representantes de la entidad SPC manifestaron a los Servicios de Inspección de la AEPD ***(…)****. Informaron, además, que la entidad SPC denunciaba estas publicaciones, con el fin de que los datos fuesen eliminados, como así ocurría en cada ocasión.*

6. ***(…).***

TERCERO: Con fecha 02/06/2022, dentro del plazo establecido, se ha interpuesto recurso de reposición por la entidad SINDICATO DE POLICÍAS DE CATALUÑA (en lo sucesivo SPC o la recurrente) contra la resolución reseñada en el Antecedente Primero, de fecha 26/04/2022, en el que solicita que se declare la inexistencia de infracción conforme a las consideraciones siguientes:

1. En primer término, ratifica las alegaciones formuladas durante la tramitación del procedimiento que dio lugar a la resolución impugnada.

2. No se especifican las medidas que hipotéticamente debía adoptar la entidad SPC; no existe negligencia o incumplimiento; el supuesto de hecho no es subsumible en la infracción tipificada en el artículo 44.3.h) de la LOPD ni hay incumplimiento reglamentario alguno.

"…la administración trata de imponer una responsabilidad prácticamente objetiva, cuando el precepto no establece tal cosa, sin que a través de la regulación reglamentaria indicada posteriormente, sea capaz de precisar qué disposiciones reglamentarias o de cualquier tipo puede haber infringido mi representada, o cuando las precisa, observamos que no se adapta a este supuesto.

La expresión medidas de seguridad adecuadas al estado de la tecnología, a la tipología de los datos, a la naturaleza, se han de referir sin duda a un situación común

u ordinaria del acceso, de usuario cuya acción no revista un dolo y conocimientos técnicos o de hackeo, precisamente enfocados a cometer un ilícito penal para acceder a los mismos.

Es decir, si el acceso pudiera haber sido realizado por cualquier persona que sin conocimiento ni uso de programas de hackeo, o los medios necesarios para el mismo tuviera acceso o pudiera acceder a los datos por falta de seguridad de la web de SPC, podría al menos discutirse la sanción impuesta, pero acreditada tal circunstancia a través del proceso penal, por la que precisamente las actuaciones han estada paralizadas, hasta constar que efectivamente se produjo dicho ataque y la manera en que se produjo, es evidente que acredita que no existe imprudencia ni acción negligente por mi representada.

No hay infracción de los artículos 91 y 93 que se indican, sino todo lo contrario. El sindicato tenía implantado el sistema de seguridad, con contraseñas, periodicidad y cambios.

La referencia a un sistema de detección de reiteración de accesos no autorizados, (que existía), no se refiere a ataques por parte de terceros con conocimientos técnicos, que permitan asaltar webs y sistemas con inyección de código especifico, actuación diametralmente opuesta a accesos en condiciones de seguridad normales o medias, de cualquier usuario. El precepto regula la obligación de proteger los datos de personas que no tengan como finalidad delictiva la apropiación de datos y precisamente su publicación, y de accesos no autorizados ordinarios.

Y lo que no puede hacer esta agencia, a efectos recaudatorios, es no valorar un proceso penal y una sentencia con hechos probados, que ha suspendido ella misma, porque los hechos estaban conectados y que acredita la forma del ataque, independientemente que en algunos de ellos se haya condenado o identificado al autor, alegando que la misma no tiene relación o no tiene efectos sobre su decisión, cuando consta la forma de ataque, que evidentemente afecta a su decisión sancionadora al ser un hecho distinto de los regulados y que motivan en la resolución definitiva, y que suponen la inexistencia de responsabilidad".

Por último, la entidad SPC, en su mismo escrito de recurso, para el caso de que éste sea desestimado, solicita la suspensión cautelar de la resolución firme en vía administrativa en tanto anuncia la interposición de recurso contencioso-administrativo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 48.1 de la LOPDGDD.

II

En relación con las manifestaciones efectuadas por la recurrente, que reproducen,

básicamente, las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que ya fueron analizadas y desestimadas en los Fundamentos de Derecho II a VI de la Resolución recurrida, de fecha 26/04/2022, en la que se considera que la misma incumplió lo dispuesto en el artículo 9 de la LOPD y se detalla suficientemente la valoración de las pruebas que han permitido determinar dicho incumplimiento y el alcance otorgado al mismo, así como las circunstancias tenidas en cuenta para la graduación de la sanción impuesta. En dichos Fundamentos de Derecho se indica lo siguiente:

"II

La entidad SPC ha alegado la prescripción de la infracción señalando que la AEPD paralizó el procedimiento innecesariamente por unos hechos que no tenían relevancia para la existencia de infracción, toda vez que la Agencia considera que "el ataque informático es indiferente, pues lo fundamental es que no se hubieran adoptado herramientas adecuadas para evitar los intentos reiterados de a usuarios no autorizados al sistema". Entiende, por ello, la reclamada que esta Agencia ya tenía esa información antes de proceder a la suspensión y que ésta no procedía.

En este caso, se imputa a SPC una infracción calificada como grave, por vulneración de lo establecido en el artículo 9 de la LOPD. Sobre las infracciones graves, el artículo 47 de la citada Ley Orgánica establece que prescribirán a los dos años, contados desde el día en que la infracción se hubiera cometido. Según este precepto, la iniciación del procedimiento sancionador, con conocimiento del interesado, interrumpe la prescripción, reanudándose el cómputo del plazo si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Lo mismo se establece en el artículo 132.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), según el cual, "El plazo de prescripción de las infracciones comenzará a contarse desde el día que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador".

En el presente caso, los hechos valorados en las presentes actuaciones, relacionados con un acceso por parte de terceros a la base de datos personales de la entidad SPC, tuvieron lugar en fecha 23/10/2013.

Así, considerando que el plazo de prescripción comienza a contarse el día en que se cometió la presunta infracción, en el presente caso el "dies a quo" del cómputo prescriptivo debe fijarse en día 23/10/2013, resultando que la posible infracción denunciada, considerando su calificación, no había prescrito en el momento en que se notificó a SPC la apertura del presente procedimiento sancionador, en fecha 12/11/2014, al no haber transcurrido el plazo de dos años dispuesto en el mencionado artículo 47.1 de la LOPD para la prescripción de las infracciones graves.

*No obstante, durante las actuaciones previas de investigación se tuvo conocimiento de las Diligencias Previas seguidas por los mismos hechos en el Juzgado de Instrucción núm. X de ***LOCALIDAD.1,* ***señaladas con el número (...)****.*

Fueron los propios representantes de la entidad reclamada los que informaron a los Servicios de Inspección que la entidad SPC formuló una denuncia en fecha 25/10/2013, dos días después del acceso a la base de datos, y aportaron la declaración efectuada en esa fecha por ***(…)*** *ante la Direcció General de la Policía, del Departament d'Interior de la Generalitat de Catalunya, en la que se da cuenta de la intrusión al servidor del día 23/10/2013, a las 19:00 horas, y de la publicación en la dirección* ******URL.1*** *de información contenida en la base de datos del servidor del sindicato.*

Aportaron, asimismo, un documento que hace referencia a las actuaciones seguidas en el citado Juzgado y a su objeto (ataque informático sufrido por el servidor que aloja las webs del SPC), que consta incorporado al Acta de Inspección de fecha 04/06/2014. En concreto, se trata de una solicitud de personación como acusación particular que dirige al Juzgado una entidad tercera (la responsable del funcionamiento de dichas webs).

*Con este motivo, se acordó suspender el procedimiento sancionador y dirigir al Juzgado de Instrucción núm. X de ***LOCALIDAD.1 la consulta a la que se refiere el artículo 7.1 del Reglamento del procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto, vigente en el momento de producirse los hechos y en la apertura del procedimiento ("En estos supuestos, así como cuando los órganos competentes tengan conocimiento de que se está desarrollando un proceso penal sobre los mismos hechos, solicitarán del órgano judicial comunicación sobre las actuaciones adoptadas").*

Hasta en seis ocasiones se consultó al Juzgado de Instrucción indicado y al Juzgado de lo Penal al que se remitieron las Diligencias para su enjuiciamiento sobre el estado de tramitación de las actuaciones y las decisiones adoptadas, así como los detalles sobre la identidad de sujeto, hecho y fundamentos entre la presunta infracción administrativa y la infracción penal que pudiera corresponder. Ninguna respuesta se recibió a estas consultas, salvo la remisión de copia de la sentencia judicial firme recaída, que consta reseñada en el Antecedente Séptimo.

En ese momento se acordó levantar la suspensión del procedimiento y reanudar su tramitación de acuerdo con lo estipulado en el artículo 7.2 del citado Reglamento del procedimiento para el ejercicio de la potestad sancionadora, interpretado contrario sensu, que determina: "(...) y si se estima que existe identidad de sujeto, hecho y fundamento entre la infracción administrativa y la infracción penal que pudiera corresponder, el órgano competente para la resolución del procedimiento acordará su suspensión hasta que recaiga resolución judicial".

De acuerdo con lo expuesto, la alegación efectuada por SPC sobre la prescripción de la infracción debe ser desestimada.

III

Se imputa a la entidad SPC el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

El Artículo 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Artículo 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que

presente el tratamiento y con la naturaleza de los datos que deban protegerse".

La LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46/CE. En el artículo 9 de la citada LOPD se 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 la 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 trascrito artículo 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 dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado" por parte de terceros.

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 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.

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.

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros "...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

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.

*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. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal contenidos en el fichero "***FICHERO.1" del que es responsable la entidad SPC, correspondiendo adoptar las de nivel alto en atención al tipo de información que contiene, tal como se especifica en el artículo 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.*

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, del Reglamento de desarrollo de la LOPD. Según el artículo 81.3 del citado Reglamento, a los ficheros de nivel de seguridad alto se aplicarán las medidas de nivel alto, además de las medidas de nivel básico y medio. (…)

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, se refieren al acceso a los ficheros y establecen lo siguiente:

"Artículo 91. Control de acceso.
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".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.
1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento 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.

A partir del nivel medio de seguridad, "el responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información" (artículo 98 del Reglamento de desarrollo de la LOPD).

Por otra parte, también para los ficheros con nivel medio y alto, el artículo 96 "Auditoría" del citado Reglamento establece lo siguiente:

"1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.
Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas".

En definitiva, la entidad SPC está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para sus ficheros, 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, al haberse constatado la posibilidad de acceder, por parte de terceros no interesados, a datos personales registrados en su sistema de información, ***(…)***

Los representantes de la entidad reclamada han manifestado que la base de datos y la información sindical contenida en su sistema es accesible para los afiliados mediante usuario y contraseña.

Sin embargo, en fecha 23/10/2013, una o varias personas no identificadas accedieron al único servidor que alojaba el sistema de información de la entidad SPC. Así lo han reconocido los propios representantes de la citada entidad.

Este acceso no autorizado fue el resultado de un ataque informático llevado a cabo mediante comandos SQL incrustados en las peticiones recibidas por el servidor. Los Servicios de Inspección de la AEPD pudieron comprobar un log del sistema atacado en el que aparecen estos comandos.

Se trata de un ataque por "SQL Injection" que persigue violar las medidas de seguridad y

acceder de una forma no legítima a la información. Para ello, el ciberatacante introduce en el sistema un código malicioso propio que le posibilita controlar el sitio, de modo que la información queda a su merced para disponer de ella o suprimirla.

En este caso, los representantes de la entidad SPC manifestaron a los Servicios de Inspección de la AEPD que se vieron comprometidos ***(…).***

Este tipo de ataques se produce cuando el "saneamiento de entrada" de datos es inadecuado, es decir, se produce con éxito aprovechando siempre las vulnerabilidades de seguridad del sistema, las cuales deben detectarse mediante las auditorías que la reclamada estaba obligada a realizar periódicamente o en cada modificación sustancial del sistema; y se evita con las herramientas de filtración adecuadas para detectar si el acceso se pretende por un usuario no autorizado y estableciendo mecanismos para limitar los intentos reiterados de accesos no autorizados al sistema de información (artículo 98 del Reglamento de desarrollo de la LOPD).

Prueba de ello son las medidas adoptadas por la entidad SPC una vez tuvo conocimiento del acceso que ha motivado las presentes actuaciones, las cuales constan reseñadas en el Hecho Probado Sexto, dirigidas a prevenir incidencias similares en el futuro.

En consecuencia, en contra de lo señalado por la reclamada, en este caso, el acceso no autorizado a la base de datos no es solo el resultado de un ataque informático, sino que se trata de un supuesto en el que la entidad reclamada no atendió sus obligaciones de seguridad estableciendo los mecanismos que hubiesen impedido aquel acceso, a pesar del ataque informático. Existe una relación entre el acceso y la inexistencia o ineficacia de las medidas, con independencia de las técnicas intrusivas empleadas.

Así, los datos personales reseñados resultaron accesibles a terceros, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Dado que ha existido vulneración del "principio de seguridad de los datos", se considera que SPC ha incurrido en infracción por incumplimiento de lo establecido en el artículo 9 de la LOPD, en relación con lo dispuesto en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley Orgánica.

La vulneración de los preceptos citados aparece tipificada como infracción grave en el artículo 44.3.h) de la LOPD, 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", pudiendo ser sancionada con multa de 40.001 a 300.000 euros, de conformidad con lo establecido en el artículo 45.2 de la citada Ley Orgánica.

En su escrito de alegaciones a la propuesta de resolución, la entidad SPC no realiza manifestación alguna sobre lo expuesto en el presente Fundamento de Derecho, limitándose a señalar que el artículo 44.3.h) de la LOPD no se refiere a ataques por parte de terceros. Se trata de una cuestión que no incide en la configuración del tipo infractor, que se determina por la existencia o no de medidas de seguridad adecuadas y, según ha quedado expuesto, en el presente caso consta que los sistemas de información de la entidad SPC resultaron vulnerables por una falta de medidas de seguridad que impidieran el acceso a la información por parte de terceros no autorizados.

IV

El "principio de seguridad de los datos" exige que la entidad responsable del tratamiento adopte las medidas necesarias y adecuadas para garantizar que la información no sea accedida por parte de terceros, tomando en consideración el estado de la tecnología y la naturaleza de los datos de carácter personal en cuestión, según doctrina de nuestro Tribunal Supremo (Sentencia 188/2022, de 15 de febrero; Rec. 7359/2020).

En este caso, se tiene en cuenta, por un lado, que la seguridad de los datos personales

sometidos a tratamiento exige medidas de nivel alto y, por otro, que el ataque sufrido empleó una tecnología de uso frecuente en las fechas en que se produjo el acceso y que dicho ataque era evitable con las herramientas disponibles en aquel momento.

En consecuencia, se entiende que las medidas adoptadas por SPC eran insuficientes y que la conducta de esta entidad no fue diligente.

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 29 de junio de 2001).

Finalmente, ha de señalarse que es la entidad SPC la responsable del fichero y, por tanto, la obligada última a garantizar la seguridad de los datos, asegurando la efectividad de las medidas adoptadas.

V

El artículo 45.2 y 4 LOPD establece lo siguiente:

"2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros".

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora".

En cuanto a la graduación de la sanción, según los criterios establecidos en el artículo 45.4, se tiene en cuenta, por un lado, la vinculación de la actividad de la entidad infractora con la realización de tratamientos de datos de carácter personal especialmente protegidos (datos de afiliación sindical); el volumen de datos personales accedidos (la información aportada por la reclamada se refería a (…), pero la base de datos comprometida tenía más de 11.000); que los hechos denunciados se producen por una falta de medidas de seguridad de los datos que posibilitó el acceso a los datos personales indicados, y no por un fallo puntual de las que hubiesen adoptado, sin perjuicio de que SPC hubiese adoptado otras medidas como el establecimiento de accesos mediante usuario y contraseña, y que la entidad SPC no comunicó espontáneamente los hechos a esta Agencia; y por otro lado, el volumen de negocio o actividad del infractor, la ausencia de intencionalidad, las acciones realizadas para evitar la divulgación de los datos, denunciando las publicaciones aparecidas, y las medidas adoptadas para evitar incidencia similares.

En base a estos criterios y circunstancias, procede la imposición de una multa por el importe mínimo establecido para las infracciones graves, fijado en 40.001 euros.

VI

Consta en las actuaciones que el acceso a la base de datos de la entidad SPC fue realizado por terceros no autorizados, los cuales recabaron información contenida en el sistema de aquella entidad que fue posteriormente divulgada.

Estos hechos son constitutivos de infracción a la normativa de protección de datos personales. Sin embargo, las actuaciones no han permitido identificar el origen real de la intrusión y la consiguiente acreditación de la autoría de los hechos, de modo que no es posible realizar imputación alguna por tales hechos.

Consta en las actuaciones una Sentencia que condena a una persona por hechos similares. Pero esta Sentencia esta referida a un acceso indebido a la base de datos de la entidad SPC distinto al que ha motivado el presente procedimiento sancionador".

III

En su escrito de recurso, SPC se limita a reproducir los argumentos expuestos en los escritos de alegaciones presentados durante la tramitación del procedimiento que dio lugar a la resolución impugnada, sin considerar los hechos constatados y los fundamentos que determinaron el acuerdo adoptado, en los que, además, se analizan ampliamente las circunstancias puestas de manifiesto por dicha entidad y se exponen las razones que determinaron su desestimación.

Por tanto, los alegatos contenidos en el recurso quedan sobradamente rebatidos con los argumentos transcritos, que se consideran válidos y suficientes para rechazar la declaración de inexistencia de infracción solicitada. En tales argumentos se exponen sobradamente las normas vulneradas, las circunstancias que permiten calificar como negligente la conducta de SPS, o la correspondencia entre los hechos comprobados y el tipo infractor

Se considera oportuno, no obstante, precisar que la normativa exige la adopción de medidas adecuadas para evitar los accesos no autorizados, sin distinguir el tipo de acceso, que puede ser automatizado o no; y se establece un tipo infractor consistente en mantener los ficheros *"carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos"*, de

modo que no se excluyen aquellos accesos que puedan llevarse a cabo intencionadamente por personas con conocimientos técnicos.

En este caso, no se niega que el sistema de información de la recurrente fuese objeto de un ataque informático realizado por persona o personas con conocimientos técnicos, pero se estimó como determinante que dicho sistema carecía de las medidas de seguridad que pudieron evitar que dicho ataque informático tuviese éxito y que la información de carácter personal pudo ser accedida como consecuencia de las vulnerabilidades del sistema de SPS.

Como ya se indica en la resolución, *"en este caso, el acceso no autorizado a la base de datos no es solo el resultado de un ataque informático, sino que se trata de un supuesto en el que la entidad reclamada no atendió sus obligaciones de seguridad estableciendo los mecanismos que hubiesen impedido aquel acceso, a pesar del ataque informático. Existe una relación entre el acceso y la inexistencia o ineficacia de las medidas, con independencia de las técnicas intrusivas empleadas".*

Por último, cabe reiterar que la resolución impugnada no tuvo en cuenta la sentencia penal que consta reseñada en sus Antecedentes porque está referida a un ataque informático distinto al que motivó el procedimiento administrativo sancionador. Si bien, esto no modifica los fundamentos de la citada resolución.

En consecuencia, en virtud de cuanto antecede, en el presente recurso de reposición la recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada, de fecha 26/04/2022, en la que se acordó imponer a la misma una sanción por la infracción de lo establecido en el artículo 9 de la LOPD.

IV

La entidad recurrente solicita en su escrito de recurso la suspensión cautelar de la ejecutividad de la presente resolución, para el caso de que sea desestimatoria, en tanto anuncia la interposición de recurso contencioso-administrativo.

Se trata de una posibilidad prevista en el artículo 90.3 de la LPACAP, que consta reseñada en la parte dispositiva del presente acto. Según se indica, para que esta suspensión pueda decretarse, el interesado deberá comunicar formalmente su intención de interponer recurso contencioso-administrativo mediante escrito dirigido a esta Agencia Española de Protección de Datos.

Vistos los preceptos citados y demás de general aplicación,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por SINDICATO DE POLICÍAS DE CATALUÑA contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 26 de abril de 2022, en el procedimiento sancionador PS/00626/2014.

SEGUNDO: NOTIFICAR la presente resolución a la entidad SINDICATO DE

POLICÍAS DE CATALUÑA.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-050422

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