Resolución 473/2021

S/REF: 001-056485

N/REF: R/0473/2021; 100-005333

Fecha: La de firma

Reclamante [redacted]

Dirección: [redacted]

Administración/Organismo: Ministerio de Trabajo y Economía Social

Información solicitada: Incidente de seguridad en el Servicio Público de Empleo Estatal

Sentido de la resolución: Estimatoria parcial

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el interesado, al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[1] (en adelante LTAIBG), con fecha 3 de mayo de 2021, solicitó al MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL la siguiente información:

    - *Causas del ciberataque, identidad de los atacantes y pretensiones, así como información de los datos que se pusieron en peligro.*

2. Mediante resolución de fecha 17 de mayo de 2021, el SERVICIO PÚBLICO DE EMPLEO ESTATAL (SEPE) del MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL contestó al solicitante lo siguiente:

    De acuerdo con la letra d) del apartado 1 del artículo 14 de la citada Ley 19/2013, de 9 de diciembre, el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para la seguridad pública.

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887

Conviene precisar, que los límites a que se refiere el artículo 14 de la Ley 19/2013, de 9 de diciembre, no se aplican directamente, sino que de acuerdo con la literalidad del texto del número 1 del mismo, "podrán" ser aplicados. De esta manera, los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación a los contenidos.

De este modo, la invocación de motivos de interés público para limitar el acceso a la información deberá estar ligada con la protección concreta de un interés racional y legítimo y deberá analizarse, para su aplicación, si la estimación de la petición de información supone un perjuicio concreto, definido y evaluable.

Una vez analizada la solicitud, esta Dirección General considera que, en este caso, es aplicable el límite de la letra d) del apartado 1 del artículo 14 de la citada Ley 19/2013, de 9 de diciembre. En este sentido, el Servicio Público de Empleo Estatal (SEPE), el día 9 de marzo, fue objeto de un incidente de seguridad durante el cual se vio afectada la disponibilidad de sus sistemas de información y comunicaciones, que se fueron restableciendo, de forma progresiva, bajo la supervisión del Centro Criptológico Nacional y en coordinación con la Secretaría General de Administración Digital, que es el órgano encargado de impulsar la coordinación de las tecnologías de la información y de las comunicaciones, incluida la seguridad e interoperabilidad, en el ámbito de la Administración General del Estado y sus Organismos Públicos.

Hacer público, como se deduce de la presente solicitud, las causas del ciberataque, la identidad de los atacantes y pretensiones, así como la información de los datos que se pusieron en peligro, proporcionaría información sobre el sistema de Tecnologías de la Información y Comunicaciones de este Organismo, y de aspectos comunes de seguridad de la Administración General del Estado, así como desvelaría aspectos que pudieran suponer un riesgo para la seguridad. Ello haría aún más complicado, e incluso invalidaría, la labor de defensa de unas infraestructuras tecnológicas que dan soporte a un servicio esencial como es la gestión del sistema de protección por desempleo.

En consecuencia, con fundamento en lo dispuesto en la letra d) del apartado 1 del artículo 14 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, se deniega la solicitud de acceso a la información pública respecto a la información descrita en los párrafos anteriores.

[redacted]

3. Ante esta respuesta, con fecha de entrada el 18 de marzo de 2021, el interesado presentó, al amparo de lo dispuesto en el artículo 24[2] de la LTAIBG, una reclamación ante este Consejo de Transparencia, con el siguiente contenido resumido:

   Que el SEPE se niega a aportar información sobre el ciberataque y sobre si los algún tipo de dato ha sido vulnerado, aduciendo un riesgo a la seguridad que no es real, al no haberse solicitado información sobre los sistemas de defensa o de reparación, ni ningún dato de carácter técnico.

   Dicha denegación no viene amparada por asuntos de seguridad pública, si no de imagen de la propia institución, careciendo de toda transparencia.

   Solicito se conceda el acceso a la información solicitada de la que el SEPE dispone, al ser una información de interés público.

4. Con fecha 20 de mayo de 2021, el Consejo de Transparencia y Buen Gobierno remitió el expediente al MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, al objeto de que pudiera hacer las alegaciones que considerase oportunas, contestando el SERVICIO PÚBLICO DE EMPLEO ESTATAL lo siguiente:

   Tal y como se señaló en la citada resolución, se considera que conceder el derecho de acceso en esta solicitud supondría un perjuicio para la seguridad pública, al darse información que forma parte de las actuaciones de mitigación y restablecimiento de la normalidad tras el incidente de seguridad del pasado 9 de marzo.

   El contenido solicitado se incardina plenamente en la información de carácter reservado que se integra en el supuesto de limitación de acceso. Como ya se señaló, no se considera procedente conceder al acceso a la información sobre las causas del ciberataque, identidad de los atacantes y las pretensiones, así como la información de los datos que se pusieron en peligro, por afectar a la propia seguridad tecnológica del SEPE, y del conjunto de la Administración General del Estado.

   Como ya se indicó en la resolución, el restablecimiento de los sistemas de información se ha realizado bajo la supervisión del Centro Criptológico Nacional (Centro Nacional de Inteligencia), y en coordinación con la Secretaría General de Administración Digital, siendo evidente que se trata de información que está sometida a limitaciones en el derecho de acceso, por los riesgos que pudiera entrañar su divulgación en la seguridad de la infraestructura tecnológica de gestión del sistema de protección por desempleo.

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

[redacted]

Desde el SEPE se han seguido las indicaciones pertinentes para la contención del incidente, la investigación de las causas y la correcta restauración de los servicios.

Estos ámbitos se considera que se encuentran plenamente integrados en la limitación al derecho de acceso en que se fundamentó la resolución.

De la misma forma, es preciso señalar que los beneficiarios de prestaciones por desempleo no se vieron afectados por esta situación de control, recuperación y estabilización del incidente de ciberseguridad.

II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 24 de la LTAIBG[3], en conexión con el artículo 8 del Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno[4], el Presidente de esta Autoridad Administrativa Independiente es competente para resolver las reclamaciones que, con carácter potestativo y previo a su eventual impugnación en vía contencioso-administrativa, se presenten frente a las resoluciones expresas o presuntas recaídas en materia de acceso a la información.

2. La LTAIBG, en su artículo 12[5], reconoce el derecho de todas las personas a acceder a la información pública, entendiendo por tal, según dispone su artículo 13 "*los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*".

   De este modo, la Ley delimita el ámbito material del derecho - a partir de un concepto amplio de información, que abarca tanto documentos como contenidos específicos y que se extiende a todo tipo de "*formato o soporte*", a la vez que acota su alcance exigiendo la concurrencia de dos requisitos vinculados con la naturaleza "*pública*" de las informaciones: (a) que se encuentren "*en poder*" de alguno de los sujetos obligados por la ley, y (b) que hayan sido elaboradas u obtenidas "*en el ejercicio de sus funciones*".

3. La solicitud de acceso de la que trae causa la presente reclamación versa sobre determinada información relacionada con un incidente de seguridad producido en el Servicio Público de

[3] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[4] https://www.boe.es/buscar/act.php?id=BOE-A-2014-11410&tn=1&p=20141105#a8
[5] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

[redacted]

Empleo Estatal, en concreto: causas del ciberataque, identidad de los atacantes, pretensiones y datos que se pusieron en peligro.

La Administración deniega la solicitud de acceso alegando que "*proporcionaría información sobre el sistema de Tecnologías de la Información y Comunicaciones de este Organismo, y de aspectos comunes de seguridad de la Administración General del Estado, así como desvelaría aspectos que pudieran suponer un riesgo para la seguridad. Ello haría aún más complicado, e incluso invalidaría, la labor de defensa de unas infraestructuras tecnológicas que dan soporte a un servicio esencial como es la gestión del sistema de protección por desempleo.*

En consecuencia, con fundamento en lo dispuesto en la letra d) del apartado 1, del artículo 14, de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, se deniega la solicitud de acceso a la información".

4. Corresponde por tanto examinar la pertinencia de la aplicación al presente caso del límite legal de la "*seguridad pública*" invocado. Junto a ello, no cabe desconocer que, a pesar de no haber sido alegado por la Administración, el acceso a la información solicitada puede afectar también al límite previsto en la letra a) del artículo 14.1 de la LTAIBG relativo a la "*seguridad nacional*". Habida cuenta de que, según ha manifestado el Tribunal Supremo, este Consejo, al resolver una reclamación, "*actúa como entidad que fiscaliza en vía administrativa la legalidad de la decisión adoptada por el órgano ante el que se presentó la solicitud, y su reclamación tiene la consideración de un recurso administrativo*", y de que "*el ejercicio de esta función puede revisar y resolver todas las cuestiones, tanto de fondo como de forma*" (STS 890/2021 - ECLI:ES:TS:2021:890, FJ.2º), se considera pertinente incluir también en el objeto de enjuiciamiento la aplicabilidad de este segundo límite.

   La estrecha conexión de la ciberseguridad con la seguridad pública y con la seguridad nacional ha sido proclamada por el Tribunal Constitucional en la Sentencia 142/2018, de 20 de diciembre de 2018, en la que formuló, entre otras, las siguientes consideraciones sobre el particular:

   "La ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública, así como en las telecomunicaciones. A partir de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan, fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo que se proyecta específicamente sobre el concreto ámbito de la protección de las redes y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas. El uso cotidiano de las tecnologías de la información y la comunicación ha provocado que se conviertan en un elemento esencial para el desarrollo económico y las relaciones sociales. No

[redacted]

obstante, es también un hecho constatado que las amenazas a la seguridad de la red comportan un riesgo que afecta a los ámbitos más diversos, por cuanto pueden afectar a la disponibilidad, integridad y confidencialidad de la información.

En el ATC 29/2018, de 20 de marzo, FJ 5, ya se constató la conexión existente entre ciberseguridad y seguridad nacional «incluida como dice expresamente la Ley 36/2015, en los títulos competenciales de las materias 4 y 29 del artículo 149.1 CE» (STC 184/2016, FJ 3), pues la Ley 36/2015, de 28 de septiembre, de seguridad nacional, identifica en su artículo 10 la ciberseguridad como uno de los «ámbitos de especial interés de la seguridad nacional... que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales». También la Ley 8/2011, de 28 abril, de medidas para la protección de las infraestructuras críticas, dictada al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29 CE, hace referencia a la ciberseguridad. El artículo 2 de esta Ley define las infraestructuras estratégicas como «las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales». Tales servicios esenciales son los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las Administraciones públicas.

A mayor abundamiento, el mantenimiento de la ciberseguridad es una de las funciones propias del Centro Nacional de Inteligencia, según establece el artículo 4 b) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Además, la ciberseguridad es uno de sus objetivos, conforme a la estrategia de seguridad nacional 2017, aprobada por Real Decreto 1008/2017, de 1 de diciembre, […]

Esta relación entre ciberseguridad y seguridad nacional se confirma en la Orden PCI/870/2018, de 3 de agosto, por la que se publica el acuerdo del Consejo de Seguridad Nacional, por el que se aprueba el procedimiento para la elaboración de una nueva estrategia de ciberseguridad nacional que sustituya a la actualmente vigente." (FJ 4º).

Resulta por tanto indiscutible que el acceso a la información relativa a un incidente de ciberseguridad como el que nos ocupa puede verse restringido por los límites de la seguridad nacional y la seguridad pública establecidos, respectivamente, en las letras a) y d) del artículo 14.1 de la LTAIBG. Sin embargo, como este Consejo viene señalando reiteradamente, la eventual afectación de alguno de los bienes o intereses públicos protegidos por los límites al derecho de acceso consagrados en la LTAIBG no necesariamente implica que los mismos prevalezcan en todo caso ni, menos aún, que ello

[redacted]

impida un acceso parcial a la información con arreglo a lo previsto en el artículo 16 de la LTAIBG.

5. A la hora de examinar la procedencia de la aplicación de los límites legales al derecho de acceso en un supuesto concreto es preciso tener presente que, al igual que sucede con las causas de inadmisión del artículo 18 de la LTAIBG, los límites del artículo 14 LTAIBG enuncian restricciones a un derecho de rango constitucional y, por tanto, deberán ser objeto de interpretación estricta y su aplicación habrá de ser proporcionada y estar justificada, atendiendo a las circunstancias de cada caso concreto. Así lo ha establecido el Tribunal Supremo en su Sentencia 3530/2017, de 16 de octubre (ECLI: ES:TS:2017:3530), en la que fijó la siguiente doctrina:

   "*La formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva, tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1 de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1, sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información*. […]

   Asimismo, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración o entidad a la que se solicita información, pues aquél es un derecho reconocido de forma amplia y que sólo puede ser limitado en los casos y en los términos previstos en la Ley" (F.J. 6º)

   Doctrina jurisprudencial que, en lo concerniente a los límites, ha sido completada por el Alto Tribunal, entre otras, en la más reciente Sentencia 574/2021, de 25 de enero (ECLI:ES:TS:2021:574), en la que precisó lo siguiente:

   "*La aplicación de los límites al derecho de acceso a la información está sujeta a determinados requisitos y condiciones. Al respecto, el artículo 14.2 LTAIBG de la LTAIBG señala lo siguiente:*

   > *2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.*

   Por tanto, el precepto legal no permite una aplicación genérica de las limitaciones como justificación de una denegación del acceso a la información pública, válida para todos los procedimientos de una determinada materia, por ejemplo, la protección de las relaciones exteriores o la protección de la investigación y sanción de los ilícitos penales en los

[redacted]

procedimientos de extradición, sino que exige una aplicación justificada y proporcionada de las limitaciones en relación al caso concreto, debiendo hacerse una ponderación de los intereses en juego, el de acceso a la información pública, por un lado, y el protegido por la limitación de que se trate.

[…]

El juicio de proporcionalidad requerido por el articulo 14.2 LTAIBG también es exigible en la aplicación del artículo 16 de la LTAIBG, que prevé como se ha indicado la posibilidad de un acceso parcial a la información, en los casos en los que la aplicación de alguno de los límites del articulo 14 LTAIBG no afecte a la totalidad de la información solicitada." (FJ, 4º)

Como puede apreciarse, el Tribunal Supremo no sólo subraya la necesidad de justificar la aplicación de los límites ponderando caso por caso, sino que deja claro que la decisión sobre el alcance material de la denegación de acceso ha de regirse también por el principio de proporcionalidad, de modo que su extensión se circunscriba a la parte de la información que resulte afectada por límite correspondiente, de acuerdo con lo establecido en el artículo 16 LTAIBG.

6. Pues bien, la aplicación de esta doctrina jurisprudencial al caso que nos ocupa lleva a este Consejo a concluir que no existe una justificación suficiente que ampare la denegación del acceso a la información solicitada.

   En primer lugar, porque la Administración se limita a justificar la denegación total del acceso con una inespecífica referencia al impacto que la revelación de la información solicitada tendría sobre la seguridad tecnológica del organismo afectado y de la Administración General del Estado, sin mayores concreciones, y sin llevar a cabo el juicio de ponderación exigido por el artículo 14.2 de la LTAIBG.

   En segundo término, porque el carácter genérico de la información solicitada -que, recordemos, versa sobre las causas del ciberataque, la identidad de los atacantes, sus pretensiones y los datos que se pusieron en peligro- permite, en lugar de contestar con una denegación absoluta, modular el alcance de la respuesta de modo que, una vez realizado el juicio de ponderación requerido por el artículo 14.2 de la LTAIBG y con la debida justificación de la aplicación de los límites concurrentes, se conceda el acceso, de acuerdo con el artículo 16 LTAIBG, a aquella parte de información cuyo conocimiento público no suponga un perjuicio real para la seguridad pública y la seguridad nacional. Buena prueba de que este deslinde es factible la ofrece el hecho de que la propia ministra de Trabajo y Economía Social, en su comparecencia en la sesión de la Comisión de Trabajo, Inclusión, Seguridad Social y Migraciones del Congreso de los Diputados celebrada el 22 de marzo de

[redacted]

2021, proporcionó determinada información sobre los aspectos que han sido objeto de la solicitud de información pública denegada por su Departamento ministerial (v. Diario de Sesiones del Congreso de los Diputados, núm. 331, 2021).

En virtud de lo hasta aquí razonado, la presente reclamación debe ser estimada parcialmente.

III. RESOLUCIÓN

En atención a los antecedentes y fundamentos jurídicos descritos, procede

PRIMERO: ESTIMAR parcialmente la reclamación presentada por [redacted] frente a la resolución del SERVICIO PÚBLICO DE EMPLEO ESTATAL del MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL, de fecha 17 de mayo de 2021.

SEGUNDO: INSTAR al SERVICIO PÚBLICO DE EMPLEO ESTATAL del MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL a que, en el plazo máximo de 10 días hábiles, remita al reclamante la siguiente información, relacionada con el incidente de seguridad en sus instalaciones:

- *Causas del ciberataque, identidad de los atacantes y pretensiones, así como información de los datos que se pusieron en peligro.*

De esta información podrán excluirse aquellos aspectos que resulten afectados por los límites previstos en las letras a) y d) del artículo 14.1 de la LTAIBG, cuya aplicación habrá de motivarse en los términos exigidos por el artículo 14.2 de la citada ley.

TERCERO: **INSTAR** al SERVICIO PÚBLICO DE EMPLEO ESTATAL del MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL a que, en el mismo plazo máximo, remita a este Consejo de Transparencia copia de la información enviada al reclamante.

De acuerdo con el artículo 23, número 1[6], de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, la Reclamación prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de conformidad con lo dispuesto en el artículo 112.2 de la Ley 39/2015, de 1 de octubre[7], del Procedimiento Administrativo Común de las Administraciones Públicas.

[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a23
[7] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a112

[redacted]

Contra la presente Resolución, que pone fin a la vía administrativa, se podrá interponer Recurso Contencioso-Administrativo, en el plazo de dos meses, ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid, de conformidad con lo previsto en el artículo 9.1 c) de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa[8].

EL PRESIDENTE DEL CTBG

Fdo: José Luis Rodríguez Álvarez

[8] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&tn=1&p=20181206#a9

[redacted]