MINISTERIO
DE HACIENDA
Y FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE HACIENDA

Solicitud de Acceso a la Información

Nº Expediente: 001-074122

[redacted]

Asunto: robo datos hacienda.

Estimado [redacted]:

Con fecha 22 de noviembre de 2022 tuvo entrada en la Unidad de Información de la Transparencia Ministerio de Hacienda y Función Pública la solicitud de acceso a la información pública al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que quedó registrada con el número de expediente 001-074122.

Con fecha 22 de noviembre de 2022 la citada solicitud se recibió en la Unidad gestora del derecho de acceso a la información pública de la Secretaría de Estado de Hacienda, fecha a partir de la cual empieza a contar el plazo de un mes para su resolución, según lo previsto en el artículo 20.1 de la Ley 19/2013, de 9 de diciembre.

Su solicitud pretende el acceso a la siguiente información:

"Quisiera conocer si es cierto que ha sucedido un robo de datos personales por un hackeo a Hacienda. Quiero conocer también quién es la persona responsable y la calidad y cantidad de datos robados, así como sospechosos de haber robado.".

En este sentido, se asume que la solicitud de transparencia se refiere al ataque informático sufrido por el Punto Neutro Judicial (PNJ) que ha sido hecho público por el Consejo General del Poder Judicial (CGPJ) en la siguiente nota de prensa:

https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Oficina-de-Comunicacion/Notas-de-prensa/El-Punto-Neutro-Judicial--afectado-por-un-ciberataque-a-las-redes-de-las-Administraciones-Publicas-espanolas

Una vez estudiada su solicitud, se resuelve DENEGAR el acceso:

De acuerdo con el artículo 14.1 de esa Ley 19/2013:

> "*1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:*
>
> *a) La seguridad nacional.*
>
> *(…)*
>
> *d) La seguridad pública.*

CORREO ELECTRÓNICO:
se.hacienda@hacienda.gob.es

CÓDIGO DIR3: E05029601

ALCALÁ. 9. 1ª Planta
28014 MADRID
TEL.: 91 595 80 95
FAX: 91 595 84 73

e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.

(…)".

En este sentido, debe señalarse que la ciberseguridad tiene una íntima relación con la seguridad pública y la seguridad nacional, como ha sido reconocido por la sentencia 142/2018, de 20 de diciembre de 2018, del Tribunal Constitucional. En concreto, realizó las siguientes afirmaciones en el fundamento jurídico cuarto:

"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 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.".

De acuerdo con lo ya indicado por la nota de prensa del CGPJ, se está investigando el ataque que se realizó a través del PNJ, por lo que no se puede revelar en este momento ningún tipo de información al respecto, incluyendo las instituciones que han sido efectivamente atacadas a través de dicho PNJ, puesto que dicha información puede inferirse el grado de avance en la investigación, los métodos de investigación, los sistemas de seguridad utilizados para detectar el ataque, el tipo de información que se haya podido ver comprometida y demás información que afecta al conjunto de sistemas de seguridad de todas las instituciones a las que se puede acceder a través del PNJ.

Más aún, revelar esta información podría facilitar la realización de nuevos ataques a dicho PNJ u otras instituciones públicas, al inferirse los sistemas de seguridad utilizados, los procedimientos para la investigación y prevención de tales ataques, etc.

Incidiendo en lo ya mencionado anteriormente, la comunicación de los datos que solicita el interesado puede afectar a la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios. En efecto, dicha información permitiría al responsable o los responsables conocer el grado de avance de las investigaciones, los cauces por los que se están desarrollando y demás información que pudiera servirles para dificultar o, incluso, eludir su identificación y, en su caso, detención.

Igualmente, debe recordarse que la resolución 412/2022 del Consejo de Transparencia y Buen Gobierno, establece que detallar la información que hipotéticamente ha podido ser obtenida a través de un robo podría llevar a dicho responsable o responsables a no utilizarla en un ámbito público o con apariencia de legalidad, lo cual también podría dificultar, no solo la identificación de ese o esos sujetos, sino también la posibilidad de incautar esa información hipotéticamente obtenida. Asimismo, eso impediría mitigar los daños que esa hipotética información pudiera causar al ser utilizada por sujetos que no tienen derecho a ella.

Finalmente, debe señalarse que la Audiencia Nacional ha abierto unas diligencias previas para investigar el ataque al PNJ, de acuerdo con la siguiente nota de prensa:

https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Audiencia-Nacional/Noticias-Judiciales/La-Audiencia-Nacional-investiga-el-ciberataque-al-Punto-Neutro-Judicial-del-CGPJ

Así, de acuerdo con la misma:

"Como primera medida, el juez ha acordado el secreto de las actuaciones por el periodo de un mes y solicitar sendos informes a la Agencia Tributaria y al Centro Criptológico Nacional sobre el alcance de los hechos denunciados.".

De acuerdo con el artículo 299 de la Ley de Enjuiciamiento Criminal (LECrim), aprobada por el Real Decreto de 14 de septiembre de 1882:

> *"Constituyen el sumario las actuaciones encaminadas a preparar el juicio y practicadas para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos.".*

Por su parte, según el artículo 301 de esa LECrim:

> *"Las diligencias del sumario serán reservadas y no tendrán carácter público hasta que se abra el juicio oral, con las excepciones determinadas en la presente Ley.*
>
> *El abogado o procurador de cualquiera de las partes que revelare indebidamente el contenido del sumario, será corregido con multa de 500 a 10.000 euros.*
>
> *En la misma multa incurrirá cualquier otra persona que no siendo funcionario público cometa la misma falta.*
>
> *El funcionario público, en el caso de los párrafos anteriores, incurrirá en la responsabilidad que el Código Penal señale en su lugar respectivo.".*

A su vez, según el artículo 302 de la LECrim:

> *"(…)*
>
> *No obstante, si el delito fuere público, podrá el Juez de Instrucción, a propuesta del Ministerio Fiscal, de cualquiera de las partes personadas o de oficio, declararlo, mediante auto, total o parcialmente secreto para todas las partes personadas, por tiempo no superior a un mes cuando resulte necesario para:*
>
> *a) evitar un riesgo grave para la vida, libertad o integridad física de otra persona; o*
>
> *b) prevenir una situación que pueda comprometer de forma grave el resultado de la investigación o del proceso.*
>
> *El secreto del sumario deberá alzarse necesariamente con al menos diez días de antelación a la conclusión del sumario.".*

En consecuencia, el acceso a esta información no es posible siquiera antes de que se produzca la apertura de juicio oral con carácter general, so pena de incurrir en las infracciones y responsabilidades penales previstas por el artículo 301 anteriormente citado, por lo que no podría revelarse, en ningún caso, ningún tipo de información.

Más aún, en el caso concreto, como indica la nota de prensa, el juez ha declarado el secreto de sumario, por lo que el contenido del sumario ni siquiera es público para las partes personadas. Dicha limitación se ha impuesto, previsiblemente, porque el juez ha considerado necesario "*prevenir una situación que pueda comprometer de forma grave el resultado de la investigación o del proceso*", por lo que concurre la causa de denegación anteriormente citada del artículo 14.1.e) de la LTBG.

Contra la presente resolución, que pone fin a la vía administrativa, podrá interponerse recurso contencioso-administrativo ante la Audiencia Nacional (Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa), en el plazo de dos meses o, previa y potestativamente, reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de un mes; en ambos casos, el plazo se contará desde el día siguiente al de la notificación de la presente resolución.

El Secretario de Estado de Hacienda

Jesús Gascón Catalán

firmado electrónicamente