RESOLUCIÓN

S/REF: 001-015684

N/REF: R/0340/2017

FECHA: 6 de octubre de 2017

[redacted]

ASUNTO: Resolución de Reclamación presentada al amparo del artículo 24 de la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno

En respuesta a la Reclamación presentada por [redacted], mediante escrito con entrada el 17 de julio de 2017, el Consejo de Transparencia y Buen Gobierno, considerando los Antecedentes y Fundamentos Jurídicos que se especifican a continuación, adopta la siguiente **RESOLUCIÓN:**

1. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, [redacted] presentó solicitud de acceso a la información, el 13 de junio de 2017, al amparo de la Ley 19/2013, de 9 de diciembre de Transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIBG), dirigida al MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN, en la que solicitaba lo siguiente:

   - *Al hilo de repetidas noticias en la prensa sobre determinadas "censuras" o "filtros" en los accesos a Internet en instituciones públicas, y preocupado por haber sufrido personalmente alguna vez el no poder acceder a algún contenido en Internet desde una conexión pública, solicito los siguientes documentos:*

     1 - Una copia del protocolo/reglamento/reglas por las que se determinan el bloqueo a determinados tipos de contenidos, dominios o IPs en las conexiones de su Ministerio que incluya tanto los criterios aplicados para decidir si una web se bloquea o no desde su conexión, como los cargos de las personas que lo deciden.

     2 - Un listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet de su Ministerio. (En caso de ser una lista dinámica en la que varíen las webs/IPs a las que se bloquea el acceso, se

[redacted]

solicita copia de la última lista con fecha anterior a un mes de la recepción de esta petición)

3 - En caso de tener distintos accesos a Internet con distintos privilegios en su Ministerio, un listado con la categorización de las distintas conexiones a Internet que tienen, así como un listado de los dominios y/o direcciones IP a los que bloquean el acceso desde cada una de sus conexiones. (En caso de ser listas dinámicas en la que varíen las webs/IPs a las que se bloquea el acceso, se solicitan copias de las últimas listas con fecha anterior a un mes de la recepción de esta petición)

- *Les ruego que la información solicitada me sea facilitada de la forma más desglosada y detallada posible, que los datos estén en formatos estructurados para que puedan ser procesados de forma automática por un ordenador, y que preferiblemente estén en un formato de archivo no propietario.*

2. Mediante Resolución de fecha 13 de julio de 2017, el MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN notificó a [redacted] lo siguiente:

- *Una vez analizada la solicitud, la Dirección General del Servicio Exterior resuelve conceder el acceso parcial a la información a que se refiere la solicitud. En relación con el punto 1 de la citada solicitud, el Ministerio de Asuntos Exteriores y de Cooperación no gestiona ninguna conexión pública a Internet, siendo la Dirección General del Servicio Exterior-Subdirección General de Informática, Comunicaciones y Redes (DGSE-SUGICYR) la Unidad competente para gestionar el acceso a Internet asociado a aquellos puestos de trabajo que lo requieren para el mejor ejercicio de las funciones que tienen asignadas.*
- *Los accesos a Internet gestionados por la DGSE-SUGICYR incorporan filtros de seguridad de acuerdo a la legislación vigente en materia de seguridad de la información, en especial el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en aplicación de la Orden AEC/1647 /2013, de 5 de septiembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores y de Cooperación.*
- *Los filtros de seguridad anteriormente citados bloquean aquellas direcciones de Internet maliciosas o que suponen un riesgo para la seguridad del Ministerio de acuerdo a los criterios de empresas de seguridad de reconocido prestigio y el Centro Criptológico Nacional. No existe en el Ministerio ningún otro criterio para el bloqueo de direcciones de Internet.*
- *En relación con los puntos 2 y 3 de la solicitud, lamentablemente no es posible atender su petición, puesto que la publicación de esos detalles supondría un menoscabo inasumible para la seguridad y el control de las redes de Ministerio. Creemos, que en estos dos puntos es de aplicación el artículo 14.1 g) de la Ley 19/2013 de 9 de diciembre.*

[redacted]

3. El 17 de julio de 2017, tuvo entrada en este Consejo de Transparencia Reclamación de [redacted], de acuerdo con lo previsto en el artículo 24 de la LTAIBG, contra la Resolución del MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN, en la que alegaba lo siguiente:

    - *En la presente petición se ha solicitado un listado de las direcciones web (dominios) a los que se prohíbe el acceso desde las conexiones públicas a internet del Ministerio.*
    - *En el escrito recibido, el Ministerio de Asuntos Exteriores y Cooperación deniega el acceso parcialmente a la información solicitada aludiendo al límite delimitado por el artículo 14.1 g) de la Ley 9/2013 de transparencia, acceso a la información pública y buen gobierno, exponiendo que el acceso a esta información supone un perjuicio para funciones administrativas de vigilancia, inspección y control, no detallando para nada cuál podría ser ese perjuicio.*
    - *No se han solicitado conocer procedimientos de seguridad o protección de las conexiones del Ministerio ni ningún otro dato que pudiera comprometer la seguridad de este servicio. Sólo un listado de webs/IPs/dominios censurados en la conexión y los criterios aplicados para ello, cosa que parcialmente se explica.*
    - *Les ruego que atiendan la presente reclamación y al Ministerio a tender los puntos 2 y 3 de mi petición, entendiendo que el derecho de acceso a información pública en este tema, que afecta a derechos fundamentales como la libertad de expresión o el derecho a recibir o emitir una información veraz prevalece sobre los argumentos expuestos por el Ministerio y teniendo en cuenta que la información a recibir no compromete para nada la operación o seguridad del Ministerio; se trata sencillamente del derecho que debemos tener a conocer qué webs/IPs/dominios se pueden visitar desde su conexión y cuáles no. No se trata de conocer ningún dato de la seguridad de sus servidores, su operativa, protección, procedimientos o cualquier otro que pudiera causar un perjuicio para la seguridad del Ministerio. Nada. Se trata sencillamente de una petición concreta en el ámbito del respeto a los mencionados derechos fundamentales.*

4. El 20 de julio de 2017, este Consejo de Transparencia trasladó al MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN la documentación obrante en el expediente para alegaciones. El escrito de alegaciones tuvo entrada el día 28 de julio de 2017, y en él se indicaba lo siguiente:

    - *Las direcciones IP constituyen un elemento de la mayor importancia para garantizar la debida seguridad de las entidades del Sector Público, toda vez que constituyen los puntos de enlace que conectan tales entidades públicas con el resto del mundo. Además de enunciarse entre los objetivos esenciales de la Estrategia Nacional de Seguridad y de concretarse en la Estrategia de Ciberseguridad Nacional, el artículo 10 de la Ley 36/2015, de 28 de*

[redacted]

septiembre, que recoge los ámbitos de especial interés para la Seguridad Nacional, señala aquellos que, por requerir una atención específica, resultan 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. Entre tales ámbitos, se menciona, expresamente y en primer lugar, la ciberseguridad.

- *Por todo ello, la decisión de bloquear o no determinadas direcciones IP (así como, en su caso y por motivos obvios, la de preservar del conocimiento no autorizado tales direcciones), fundamentadas en los criterios técnicos y de inteligencia que presiden las funciones y competencias legales del Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia, obedece a razones de seguridad pública considerándose información especialmente sensible.*
- *Asimismo, la revelación de la lista de direcciones IP bloqueadas automáticamente en función de los criterios programados por el fabricante de los equipos de seguridad de la red, supondría una infracción de los términos de la licencia de uso adquirida por el Ministerio con la consiguiente vulneración de los derechos de propiedad industrial asociados.*

II. FUNDAMENTOS □UR□DICOS

1. De conformidad con lo dispuesto en el artículo 24 de la LTAIBG, en relación 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, la Presidenta de este Organismo es competente para resolver las reclamaciones que, con carácter potestativo y previo a un eventual Recurso Contencioso-Administrativo, se presenten en el marco de un procedimiento de acceso a la información.

2. La Ley 19/2013, de 19 de diciembre, de Transparencia, acceso a la información pública y buen gobierno reconoce en su artículo 12 el derecho de todas las personas a acceder a la información pública, entendida, según el artículo 13 de la misma norma, como "*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*".

   Por lo tanto, la Ley define el objeto de una solicitud de acceso a la información en relación a información que ya existe, por cuanto está en posesión del Organismo que recibe la solicitud, bien porque él mismo la ha elaborado o bien porque la ha obtenido en ejercicio de las funciones y competencias que tiene encomendadas.

3. En cuanto al fondo del asunto, debe analizarse, en primer lugar, si resulta de aplicación el límite del articulo 14.1 g), invocado por la Administración, según el cual *el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para las funciones administrativas de vigilancia, inspección y control.*

[redacted]

Sobre la aplicación de los límites al acceso a la información, es conocido el Criterio Interpretativo nº 2 de 2015, aprobado por este Consejo de Transparencia y Buen Gobierno en cumplimiento de las funciones legalmente encomendadas por el art. 38.2 a) que se pronuncia en los siguientes términos:

Los límites a que se refiere el artículo 14 de la LTAIBG, a diferencia de los relativos a la protección de los datos de carácter personal, 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.

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.

En este sentido su aplicación no será en ningún caso automática: antes al contrario deberá analizarse si la estimación de la petición de información supone un perjuicio (test del daño) concreto, definido y evaluable. Este, además no podrá afectar o ser relevante para un determinado ámbito material, porque de lo contrario se estaría excluyendo un bloque completo de información.

Del mismo modo, es necesaria una aplicación justificada y proporcional atendiendo a la circunstancia del caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso (test del interés público).

Al acceso a la información o documentación le son de aplicación los límites contenidos en el artículo 14 de la LTAIBG y el relativo a la protección de datos de carácter personal, regulado en su artículo 15. En todo caso, la aplicación de los límites deberá ser motivada, restringida, justificada y proporcionada así como atender a las circunstancias del caso concreto, de acuerdo con los criterios contenidos en el indicado Criterio Interpretativo y en las sentencias de los Tribunales Contencioso-Administrativos.

En este sentido, debe tenerse presente que facilitar la información es la regla general y la aplicación de los limites es la excepción y hemos de tener presente que la LTAIBG, en su *Preámbulo*, afirma expresamente que el derecho de acceso a la información pública se configura de forma amplia y dicho derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información o por su entrada en conflicto con otros intereses protegidos. *"Así, la finalidad, principio y filosofía que impregna la reseñada Ley, es un acceso amplio a la información pública; y los límites a tal acceso han de motivarse, interpretarse y aplicarse de modo razonado, restrictivo y aquilatado a tenor del llamado, test de daño; a la luz de la determinación del perjuicio que el acceso a determinada información puede producir sobre el interés que se pretende salvaguardar con la limitación"* (Sentencia 85/2016, de 14 de junio de 2016, del Juzgado Central de lo Contencioso Administrativo nº 5 de Madrid. PO 43/2015).

[redacted]

4. El limite invocado por la Administración ya ha sido objeto de análisis anteriormente por este Consejo de Transparencia. Así, por ejemplo, en el procedimiento R/0482/2015, finalizado mediante Resolución de fecha 19 de enero de 2016, se razonaba lo siguiente:

   "El límite invocado por la Administración ha sido interpretado por este Consejo en el sentido de que las funciones de vigilancia, inspección y control cuyo desempeño estuviera encomendado al organismo, podrían ser perjudicadas si el procedimiento de inspección se estuviera desarrollando y el proporcionar esa información hiciera peligrar el resultado final. También, por ejemplo, en el supuesto de que, acabada la inspección o la actividad de control, se estuviera a la espera de dictar una Resolución final en base a las mismas, o que el acceso a la información fuera solicitado por la misma persona que está siendo objeto de vigilancia, inspección o control. Asimismo, este Consejo de Transparencia ha interpretado que las funciones de vigilancia, inspección y control también pudieran verse perjudicadas cuando el acceso a la información solicitada pudiera suponer que se desvelaran procedimientos o métodos de trabajo cuyo conocimiento, con carácter previo y general, pudieran comprometer el correcto desarrollo y tramitación de un concreto expediente."

   En el presente caso, no estamos ante actuaciones procedimentales de un expediente que deban ser objeto de reserva por poder afectar a actuaciones en curso o posteriores que perjudiquen futuras decisiones del Organismo o impidan realizar labores de prevención o control dentro de las funciones que legalmente tiene encomendadas. Por ello, este Consejo de Transparencia entiende que este límite no es aplicable al presente caso, pero sí lo podría ser el límite del articulo 14.1 a), de la LTAIBG, según el cual *el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para la seguridad nacional*, que se analiza a continuación.

5. En primer lugar, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional dispone que ésta se entiende como *la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos (*artículo 2*)*

   Su artículo 4 establece lo siguiente:

   1. La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.

   2. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de

[redacted]

los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.

3. La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley.

Finalmente, su artículo 11 establece que

1. En el marco del Sistema de Seguridad Nacional, las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional, estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.

2. Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico.

Igualmente, al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en la Ley de Seguridad Nacional, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema.

6. En el campo de la Ciberseguridad, el Consejo Nacional de Ciberseguridad, órgano colegiado de apoyo al Consejo de Seguridad Nacional y en concreto de asistencia al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional en el ámbito de la ciberseguridad, adoptó el Plan Nacional de Ciberseguridad, al que el Consejo de Seguridad Nacional dio su conformidad.

   Se trata del primer nivel en la planificación resultante de la Estrategia de Ciberseguridad Nacional y desarrolla, a través de planes de acción derivados, las líneas de acción previstas en la Estrategia. Estos planes derivados abordan distintos aspectos de la ciberseguridad, como incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación

ante las ciberamenazas, haciendo énfasis en la Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y otros sistemas de interés nacional, la investigación y persecución del ciberterrorismo, el ciberspionaje y la ciberdelincuencia, así como la ciberseguridad en el sector privado o la cultura de ciberseguridad.

Asimismo, la Estrategia de Ciberseguridad Nacional desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2013 en el ámbito de la ciberseguridad, fijando como objetivo global lograr que España haga un uso seguro de los sistemas de información y las telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. Seguidamente, la Estrategia fija seis objetivos específicos:

- Para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia (o capacidad para afrontar situaciones adversas);
- Para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular;
- En el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio;
- En materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio;
- En capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad;
- En lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.

7. Por tanto, el concepto de ciberseguridad nacional emana de los dos documentos estratégicos referidos, entendiendo la misma como la acción del Estado dirigida a proteger los intereses nacionales, vitales y estratégicos, referentes a:

    - Los sistemas de información y telecomunicaciones e infraestructuras comunes a todas las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés para la Seguridad Nacional.;
    - La libertad y seguridad de los ciudadanos;
    - La industria;
    - El patrimonio tecnológico.

Todo ello cumpliendo la legislación nacional y el derecho internacional, así como el respeto de las normas internacionales en cumplimiento de los compromisos adquiridos por España.

La Estrategia de Ciberseguridad Nacional establece igualmente unas *Líneas de Acción* orientadas a alcanzar los objetivos propuestos y un total de 45 medidas concretas.

Para el desarrollo efectivo de estas *Líneas de Acción*, el Consejo Nacional de Ciberseguridad propuso la elaboración del *Plan de Acción* que enmarca su desarrollo, de manera específica, para los dos próximos años.

El Plan Nacional de Ciberseguridad (PNCS), aprobado por el Consejo de Seguridad Nacional (CSN), constituye el primer nivel en la planificación de la Estrategia de Ciberseguridad Nacional que, siguiendo las directrices generales de la misma, identifica de manera más exhaustiva los riesgos y amenazas. El estado de estos riesgos y amenazas de la Ciberseguridad Nacional se concreta en el Informe Anual de Seguridad Nacional que aprueba el CSN antes de su presentación en Sede Parlamentaria, reflejo del compromiso con la necesaria transparencia e implicación de la sociedad. De este informe se desprende cómo el Sistema de Seguridad Nacional se configura para hacer frente y dar respuesta a estos desafíos.

8. La Estrategia de Seguridad Nacional, elaborada por Presidencia del Gobierno en el año 2013, dispone lo siguiente en materia de ciberseguridad:

1. *Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con apoyo en un marco jurídico operativo y eficaz. Se mejorarán los procedimientos y se impulsarán los recursos necesarios con especial énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y todos aquellos sistemas de interés nacional.*

2. *Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Se finalizar á la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio, mediante el refuerzo de las capacidades de detección y la mejora de la defensa de los sistemas clasificados. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las infraestructuras críticas. Se impulsará la normativa sobre protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.*

3. *Mejora de la seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.*

[redacted]

4. *Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.*

5. *Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.*

6. *Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.*

9. De los documentos y preceptos legales citados pueden extraerse las siguientes conclusiones:

   - La Seguridad Nacional afecta a la libertad y el bienestar de los ciudadanos, la defensa de España y sus principios y valores constitucionales.
   - La Ciberseguridad debe entenderse como la garantía del uso seguro de las redes y los sistemas de información a través del fortalecimiento de la prevención, detección y respuesta a los ciberataques.
   - La Ciberseguridad forma parte de la Estrategia de Seguridad Nacional, haciendo especial énfasis en la Administraciones Públicas. Para estas, se trata de garantizar que sus sistemas de información y telecomunicaciones, redes de comunicaciones e infraestructuras comunes poseen el adecuado nivel de seguridad y resiliencia.
   - El bloqueo a determinados tipos de contenidos, dominios o IPs en las conexiones del Ministerio, que es por lo que se interesa el Reclamante, puede incardinarse, con carácter general, dentro de la estrategia de ciberseguridad que han de adoptar las Administraciones Publicas para evitar ciberataques, puesto que permitiendo esos accesos se corre el riesgo cierto, no hipotético, de sufrir ataques externos que incidan en la seguridad de la información que maneja el Ministerio, así como en los datos personales almacenados en sus ficheros y sistemas, con el consiguiente perjuicio para los ciudadanos que tienen o han tenido relaciones con el mismo, mermando, sin duda, sus derechos y su bienestar, que es lo que se pretende proteger bajo el paraguas de la Seguridad Nacional. Todo ello, como resultado de un incidente de ciberseguridad o de un aviso previo por parte del Centro Criptológico Nacional en el que indican que se trata de dominios maliciosos.

   Sin embargo, no toda la información que se solicite relativa a bloqueo de accesos a Internet debe quedar subsumida en el límite de la Seguridad Nacional, como así lo entiende también el Ministerio, que ha dado parte de la información. Este Consejo de Transparencia entiende que la parte de la solicitud no atendida no está afectada por el límite citado, por las siguientes razones:

- Respecto a la solicitud de *copia del protocolo/reglamento/reglas por las que se determina el bloqueo a determinados tipos de contenidos, dominios o IPs*, el Ministerio ya ha contestado, informando que *Los accesos a Internet gestionados por la DGSE-SUGICYR incorporan filtros de seguridad de acuerdo a la legislación vigente en materia de seguridad de la información, en especial el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en aplicación de la Orden AEC/1647 /2013, de 5 de septiembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores y de Cooperación. Los filtros de seguridad anteriormente citados bloquean aquellas direcciones de Internet maliciosas o que suponen un riesgo para la seguridad del Ministerio de acuerdo a los criterios de empresas de seguridad de reconocido prestigio y el Centro Criptológico Nacional. No existe en el Ministerio ningún otro criterio para el bloqueo de direcciones de Internet.* Por tanto, este punto debe ser desestimado.
- Respecto al *listado de los distintos accesos a Internet*, el Ministerio no ha informado. Debe tenerse en cuenta que el bloqueo viene derivado del hecho de que el acceso a los dominios y/o direcciones IP bloqueadas puede provocar un perjuicio a las redes y sistemas, por lo que, es precisamente con el bloqueo de dichos dominios y/o direcciones IP con el que se está evitando un daño a la seguridad. Cuestión distinta es si se pide y conoce información sobre los dominios y/o direcciones IP respecto de los que se haya constatado su carácter malicioso y también sobre los efectivamente bloqueados, lo que podría permitir una comparación y la identificación de los dominios y/o direcciones IP maliciosos frente a los que no se hubiera puesto ninguna medida, que es lo solicitado en este caso. Esta última información si podría eventualmente, a nuestro juicio, producir un perjuicio a la seguridad del sistema, caso de ser conocida por terceros ajenos al mismo, ya que permitiría conocer fallos y quiebras del sistema de seguridad. No obstante, como en el supuesto anterior, sí se considera que el Ministerio debe informar de si dispone de un único perfil o de varios perfiles de acceso a Internet, que también solicita indirectamente el Reclamante. Por tanto, este punto debe ser estimado parcialmente.
- En cuanto a *los cargos de las personas que deciden si una web se bloquea o no desde su conexión,* el Ministerio no ha ofrecido contestación alguna. En este apartado, este Consejo de Transparencia entiende que debe darse la información, ya que es objetivo de la LTAIBG conocer cómo se toman las decisiones que afectan a los ciudadanos o bajo qué criterios actúan nuestras instituciones, lo que incluye conocer qué cargo toma esas decisiones con trascendencia pública, por lo que no debe aplicarse el limite invocado en este punto. La Seguridad Nacional no depende de la identificación del cargo que toma decisiones sobre ciberseguridad favorables también para la ciudadanía.

  En este sentido, debe tenerse en cuenta que lo relevante es el cargo, en el sentido de que el mismo lleva aparejada determinada responsabilidad, y no la identidad de la persona física que en un momento determinado pueda estar ejerciendo dicha responsabilidad.

[redacted]

- Lo mismo puede decirse respecto del *listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet del Ministerio,* que no ha sido proporcionado por éste. A juicio de este Consejo de Transparencia, facilitar esos datos no solo no pone en peligro las estructuras básicas del Ministerio, sino que ayuda a proteger la libertad y el bienestar de los ciudadanos, informándoles de sitios Web maliciosos a los que no es recomendable acceder, que es la finalidad de la Ley de Seguridad Nacional, por lo que tampoco debe aplicarse el límite invocado en este punto.

10. Finalmente, y respecto de lo indicado en el escrito de alegaciones en el sentido de que *la revelación de la lista de direcciones IP bloqueadas automáticamente en función de los criterios programados por el fabricante de los equipos de seguridad de la red, supondría una infracción de los términos de la licencia de uso adquirida por el Ministerio con la consiguiente vulneración de los derechos de propiedad industrial asociados* debe recordarse que, a pesar de que se solicita expresamente con ocasión de la remisión del expediente que se aporte toda documentación justificativa de las alegaciones efectuadas, la Administración no ha aportado los términos de la licencia al objeto de comprobar la previsión en las mismas de lo indicado.

    Asimismo, a nuestro juicio, la vulneración de los derechos de propiedad industrial podría producirse, en su caso, si lo que se solicitara fueran los criterios en base a los cuales se bloquearan las direcciones IP maliciosas, pero no el resultado de la aplicación de dichos criterios.

11. Por todo lo anteriormente expuesto, debe estimarse la Reclamación presentada, debiendo el Ministerio facilitar al Reclamante la siguiente información:

    - *Si dispone el Ministerio de un único perfil o de varios perfiles de acceso a Internet.*
    - *Los cargos de las personas que deciden si una web se bloquea o no desde su conexión a Internet.*
    - *El listado de los dominios y/o direcciones IP a los que bloquean el acceso desde las conexiones a Internet del Ministerio.*

    No obstante, y en relación al último punto, en la ejecución de la presente resolución, se solicita sea aportado a este Consejo de Transparencia y Buen Gobierno copia de la licencia de uso adquirida por el Ministerio y cuya vulneración ha sido alegada.

III. RESOLUCIÓN

En atención a los Antecedentes y Fundamentos Jurídicos descritos, procede

[redacted]

PRIMERO: **ESTIMAR** la Reclamación presentada por [redacted], con entrada el 17 de julio de 2017, contra la Resolución del MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN, de fecha 7 de julio de 2017.

SEGUNDO: INSTAR al MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN a que, en el plazo máximo de 10 días hábiles, remita a [redacted] la información referida en el Fundamento Jurídico 10 de la presente Resolución.

TERCERO: INSTAR al MINISTERIO DEL ASUNTOS EXTERIORES Y COOPERACIÓN a que, en el mismo plazo máximo de 10 días hábiles, remita a este Consejo de Transparencia y Buen Gobierno copia de la información remitida al Reclamante.

De acuerdo con el artículo 23, número 1, 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, 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En consecuencia, contra la presente Resolución, que pone fin a la vía administrativa, únicamente cabe, en caso de disconformidad, la interposición de Recurso Contencioso-Administrativo ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid en plazo de dos meses a contar desde el día siguiente al de su notificación, 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.

LA PRESIDENTA DEL
CONSEJO DE TRANSPARENCIA Y BUEN GOBIERNO

Fdo: Esther Arizmendi Gutiérrez

[redacted]