CLASIFICACIÓN DE INFORMACIÓN:
CT-CI/A-20-2018

INSTANCIA REQUERIDA:
DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

Ciudad de México. Resolución del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, correspondiente al **cinco de septiembre de dos mil dieciocho**.

A N T E C E D E N T E S:

I. Solicitud de información. El cinco de julio de dos mil dieciocho, se recibió en la Plataforma Nacional de Transparencia la solicitud tramitada bajo el folio 0330000135418, por la que se requirió información consistente en: "…*conocer el número de ataques cibernéticos que la dependencia federal ha recibido de enero de 2018 a la fecha. Favor de detallar por mes, tipo de ataque y lugar de origen*" [sic].

II. Prevención y su desahogo. El Subdirector General de la Unidad General de Transparencia y sistematización de la Información Judicial, mediante acuerdo de fecha seis de julio de este año, previno por única ocasión al peticionario para aclarar a que dependencia se refería.

El peticionario, con fecha nueve de julio del presente año, aclaró que requería información de este Alto Tribunal.

III. Trámite. El diez de julio de dos mil dieciocho, una vez analizada la naturaleza y contenido de la solicitud, el Subdirector General de la Unidad General de Transparencia y Sistematización de la Información Judicial con fundamento en los artículos 123 y 124 de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 7 del *"ACUERDO GENERAL DE ADMINISTRACIÓN 05/2015, DEL TRES DE NOVIEMBRE DE DOS MIL QUINCE, DEL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, POR EL QUE SE EXPIDEN LOS LINEAMIENTOS TEMPORALES PARA REGULAR EL PROCEDIMIENTO ADMINISTRATIVO INTERNO DE ACCESO A LA INFORMACIÓN PÚBLICA, ASÍ COMO EL FUNCIONAMIENTO Y ATRIBUCIONES DEL COMITÉ DE TRANSPARENCIA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN" (Lineamientos Temporales)*, determinó procedente la solicitud para abrir el expediente UT-A/0249/2018.

IV. Requerimiento de informe. Por oficio UGTSIJ/TAIPDP/1993/2018, de once de julio de dos mil dieciocho, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial requirió al Director General de Tecnologías de la Información, para que dentro del término de cinco días hábiles computados a partir de que le fuera notificado el aludido oficio, le informara en esencia: **a)** la existencia de la información y, en su caso, su clasificación; **b)** la modalidad o modalidades disponibles, ajustándose, en la medida de lo posible, a la solicitud de lo peticionado; y, **c)** en su caso, el costo de la reproducción.

V. Respuesta del área. En seguimiento, el Director General de Tecnologías de la Información, a través del oficio DGTI/DAPTI-1658-2018, de ocho de agosto del presente año, solicitó prórroga de cinco días para dar respuesta.

VI. Requerimiento de informe. Por oficio UGTSIJ/TAIPDP/2154/2018, de diez de agosto de dos mil dieciocho, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial requirió nuevamente al Director General de Tecnologías de la Información, por lo solicitado.

VII. Respuesta del área. En respuesta, el Director General de Tecnologías de la Información, en el oficio DGTI/DAPTI-1720-2018, de quince de agosto del presente año, manifestó lo siguiente:

> *"…Dar a conocer la información asociada a ciberataques en contra de la SCJN, tal como son: el número de ataques, periodo del ataque, tipo de ataque y lugar de origen, brinda a un atacante información sensible que podría comprometer la infraestructura tecnológica de la SCJN, toda vez que esta información permite conocer: - - - A. Las capacidades de la infraestructura tecnológica y de seguridad informática de la institución, mediante la cantidad de peticiones web que ha soportado hasta el momento la infraestructura tecnológica de la SCJN, la cual en caso de recibir una cantidad superior de peticiones, resultaría en la caída de los portales de Internet de la Institución. - - - B. Tipo de ataques detectados y mitigados por la infraestructura de seguridad informática de los portales de Internet, permitirían a un atacante dirigir de manera específica el tipo de ataques por eliminación, las cuales la infraestructura de seguridad informática no tiene registradas o generar peticiones web que a la fecha no se han ejecutado contra la infraestructura de la SCJN, con lo que aumentaría las probabilidad [sic] de comprometer la información de la institución. - - - C. El lugar de origen, el cual es identificado por la infraestructura de seguridad informática, con lo que los atacantes podrían coordinar ataques desde otros países y poner en riesgo la información de esta institución. - - - D. Al relacionar los ataques registrados, el atacante puede verificar que los ataques ya generados han sido registrados o mitigados por la infraestructura de seguridad informática. - - - Derivado de lo anterior y con base en el Artículo 113*

Fracción XI, de la Ley General de Transparencia y Acceso a la Información Pública, la información se clasifica como reservada...”

VIII. Remisión del expediente a la Secretaría del Comité de Transparencia de la Suprema Corte de Justicia de la Nación. A través del oficio UGTSIJ/TAIPDP/2219/2018, el diecisiete de agosto de dos mil dieciocho, el Titular de la Unidad General de Transparencia y Sistematización de la Información Judicial remitió el expediente a la Secretaría del Comité de Transparencia de la Suprema Corte de Justicia de la Nación, a efecto de que conforme a sus atribuciones le diera el turno correspondiente a fin de que se elaborara el proyecto de resolución respectivo, por parte del Comité de Transparencia.

IX. Acuerdo de trámite. Mediante proveído de veinte de agosto de dos mil dieciocho, el Presidente del Comité de Transparencia de este Alto Tribunal ordenó su remisión al Secretario Jurídico de la Presidencia de esta Suprema Corte de Justicia de la Nación, en su carácter de integrante de dicho órgano, para que conforme a sus atribuciones procediera al estudio y propuesta de resolución respectiva, en términos de lo dispuesto en los artículos 44, fracción II, de la Ley General; 23, fracción II, y 27 de los Lineamientos Temporales.

X. Prórroga. Durante el trámite del presente asunto, en sesión del veintidós de agosto del año dos mil dieciocho, el Comité de Transparencia autorizó prórroga de plazo extraordinario.

C O N S I D E R A N D O:

I. Competencia. El Comité de Transparencia de la Suprema Corte de Justicia de la Nación es competente para confirmar, modificar o

revocar la determinación de clasificación de información, de conformidad con los artículos 6° de la Constitución Política de los Estados Unidos Mexicanos; 44, fracciones I y II, de la Ley General; 65, fracciones I y II, de la Ley Federal; 23, fracciones I y II, y 37, de los Lineamientos Temporales.

II. Análisis. Como se vio en el capítulo de antecedentes, la petición que propició la integración del presente asunto se centra en diversa información sobre posibles ataques cibernéticos que este Alto Tribunal hubiere recibido a partir de enero de este año a la fecha.

Al enfrentarse a tal solicitud; el Director General de Tecnologías de la Información entendió que la divulgación de esa información podría comprometer, en distintos aspectos, la infraestructura tecnológica de este Alto Tribunal; de ahí que procedió a su reserva en términos del artículo 113 fracción XI, de la Ley General.

Sobre esa base, el punto a dilucidar a través del caso que nos ocupa radica en determinar si sobre la información requerida se actualiza o no la reserva identificada por el área instada a su divulgación y, en su caso, si aquella puede o no ser proporcionada en los términos solicitados.

Ahora, antes de llevar a cabo el análisis correspondiente, es importante recordar que en el esquema de nuestro sistema constitucional, el derecho de acceso a la información encuentra cimiento a partir de lo dispuesto en el artículo 6º, apartado A, de la Constitución, cuyo contenido deja claro que, en principio, todo acto de autoridad (todo

acto de gobierno) es de interés general y, por ende, es susceptible de ser conocido por todos.

Sin embargo, como lo ha interpretado el Pleno del Alto Tribunal en diversas ocasiones, el derecho de acceso a la información no puede caracterizarse como uno de contenido absoluto, en tanto su ejercicio se encuentra acotado en función de ciertas causas e intereses relevantes, así como frente al necesario tránsito de las vías adecuadas para ello[1].

Así, precisamente en atención al dispositivo constitucional antes referido, se obtiene que la información que tienen bajo su resguardo los sujetos obligados del Estado encuentra como excepción aquella que sea temporalmente reservada o confidencial en los términos establecidos por el legislador federal o local, cuando de su propagación pueda derivarse perjuicio por causa de interés público y seguridad nacional.

---

[1] ***DERECHO A LA INFORMACIÓN. SU EJERCICIO SE ENCUENTRA LIMITADO TANTO POR LOS INTERESES NACIONALES Y DE LA SOCIEDAD, COMO POR LOS DERECHOS DE TERCEROS***. *El derecho a la información consagrado en la última parte del artículo 6o. de la Constitución Federal no es absoluto, sino que, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto a los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura jurídica del secreto de información que se conoce en la doctrina como "reserva de información" o "secreto burocrático". En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, el mencionado derecho no puede ser garantizado indiscriminadamente, sino que el respeto a su ejercicio encuentra excepciones que lo regulan y a su vez lo garantizan, en atención a la materia a que se refiera; así, en cuanto a la seguridad nacional, se tienen normas que, por un lado, restringen el acceso a la información en esta materia, en razón de que su conocimiento público puede generar daños a los intereses nacionales y, por el otro, sancionan la inobservancia de esa reserva; por lo que hace al interés social, se cuenta con normas que tienden a proteger la averiguación de los delitos, la salud y la moral públicas, mientras que por lo que respecta a la protección de la persona existen normas que protegen el derecho a la vida o a la privacidad de los gobernados. Época: Novena Época. Registro: 191967. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000. Materia(s): Constitucional*
Tesis: P. LX/2000. Página: 74)

Trasladado al caso, como se vio en el apartado de antecedentes, para sustentar la reserva debatida, el área manifestó expresamente que divulgar lo solicitado pondría en riesgo la información de la institución porque:

- Revelar la cantidad de peticiones web podría evidenciar la capacidad de la infraestructura tecnológica y de seguridad, y en su caso, la posibilidad de recibir mayores ataques, con la consecuente caída de los portales de Internet de la Institución;
- Identificar el tipo de ataques detectados, permitiría dirigir éstos de manera específica por vía de eliminación;
- Dar a conocer el lugar de los ataques podría generar otros coordinados desde distintos lugares.

En ese sentido, la instancia entendió que la información se encontraba **reservada**, al estimar actualizada la hipótesis dispuesta en el artículo 113, fracción XI, de la Ley General, en virtud de que se podrían poner en riesgo cuestiones de seguridad informática y, con ello, de la conducción de expedientes judiciales o procedimientos administrativos seguidos en forma de juicio.

El referido dispositivo establece:

> ***"Artículo 113.*** *Como información reservada podrá clasificarse aquella cuya publicación:*
> *…;*
> *XI. Vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;.."*

Al respecto, el contraste entre la justificación proporcionada por el área requerida y los supuestos contenidos en el precepto transcrito, permiten evidenciar que dicha motivación resulta indebida, ya que si bien es cierto que, en principio, como este Comité ha sostenido en otros asuntos[2], la posible afectación de los sistemas tecnológicos de este Alto Tribunal podría generar un acceso no controlado y no permitido a la información de los expedientes judiciales o procedimientos administrativos seguidos en forma de juicio, también lo es que junto a la tarea sustantiva de este Tribunal Constitucional, que se traduce en la emisión de sentencias dentro de los diversos expedientes de los que toca conocer, prevalecen múltiples actividades administrativas para su debido desarrollo, sobre cuya vigencia, en este caso, no podría entenderse actualizada la hipótesis ya descrita.

En efecto, como se dijo al resolver la clasificación de información CT-CI/A-3-2018, en sesión de dieciocho de abril del presente año, "*no todo el cúmulo de herramientas o instrumentos tecnológicos con los que opera la Suprema Corte de Justicia de la Nación se encuentran vinculados o referenciados con los expedientes judiciales, sino que también prevalecen sistemas orientados a la gestión de su administración (recursos humanos, adquisiciones, contabilidad, etcétera)",* de ahí que, por tal motivo, en estos casos la materialización de la causa de reserva no puede predicarse de manera general o abstracta, siendo que, además, tal supuesto se limita al espacio de los expedientes judiciales.

En otro orden de ideas, esas consideraciones dan cuenta que, para efectos del acceso a la información, la supuesta alteración del

[2] Tal como fue el CT-CI/A-7-2018, de treinta de mayo de este año.

esquema de seguridad de los sistemas tecnológicos sobre los que puede descansar la dinámica de comunicación y operación de los diversos sujetos obligados debe justificarse de manera concreta y estricta, sin que la mera posibilidad de ataques sea suficiente para ello.

Sobre todo porque el acceso a la información no puede entenderse sustentado en un principio de riesgo futuro o de malicia de quien acude a su ejercicio, de ahí que su eficacia no deba verse obstaculizada a partir de supuestas categorías y datos técnicos generales e hipotéticos, sino que, por el contrario, para su posible limitación se exige la precisión de datos objetivos que, dentro de un marco racional específico, demuestren de modo real y excepcional el daño que la divulgación de la información representaría, en términos de los artículos 104 y 113 de la Ley General, lo que no aconteció en la especie, sin que este Comité, en este momento, pueda pronunciarse al respecto.

Ello, de conformidad con lo dispuesto en los artículos 100, último párrafo de la Ley General[3], en relación con el 17, párrafo primero, de los Lineamientos Temporales[4], en tanto es competencia del titular de la instancia que tiene bajo su resguardo la información requerida, determinar su disponibilidad y clasificarla conforme a los criterios establecidos en la normativa aplicable, además de que es la única área técnica que cuenta con el personal especializado para velar por la

---

[3] ***"Artículo 100.*** *…*
…
Los titulares de las Áreas de los sujetos obligados serán los responsables de clasificar la información, de conformidad con lo dispuesto en esta Ley, la Ley Federal y de las Entidades Federativas."

[4] ***"Artículo 17***
De la responsabilidad de los titulares y los enlaces
En su ámbito de atribuciones, los titulares de las instancias serán responsables de la gestión de las solicitudes, así como de la veracidad y confiabilidad de la información…"

seguridad de la información y de los sistemas tecnológicos del Alto Tribunal, en términos de lo dispuesto por el artículo 27, fracción XI del Reglamento Orgánico en Materia de Administración de la Suprema Corte de Justicia de la Nación[5].

Luego, conforme a lo anterior, ante la evidencia de la necesidad de proteger información que pudiere generar afectación a los sistemas de seguridad informática, que pudieren incidir en accesos no controlados ni permitidos de la información, tanto jurisdiccional como administrativa, de este Alto Tribunal, se exigiría que se precise y justifique de forma suficiente, desde la especifica prueba de daño, la reserva de información a que se ha venido haciendo mención o alguna otra.

Junto a lo anterior, y solo a manera de ejemplo, se tiene que algunos sujetos obligados, como es el caso del Banco de México[6] y el Centro de Investigación y Seguridad Nacional "Cisen"[7], han informado,

---

[5] *"**Artículo 27.** El Director General de Tecnologías de la Información tendrá las siguientes atribuciones:*
…
XI. Ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento;…"

[6] *Este sujeto obligado ha dado a conocer diversos en diversos momentos datos sobre los ataques cibernéticos a participantes del Sistema de Pagos Electrónicos Interbancarios (véase el siguiente link de Internet: http://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf), así como propios (se desprende del punto 2 del boletín que se encuentra en la siguiente página electrónica: http://www.banxico.org.mx/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf)*

[7] *En este caso, se puede consultar la resolución del recurso de revisión 155/11 resuelto por el entonces Instituto Federal de Acceso a la Información y Protección de Datos Personales, en la cual se observa que el CISEN, en la etapa de alegatos, informó a ese Instituto el número de ataques informáticos detectados por el órgano desconcentrado en su contra en el periodo de dos mil nueve a dos mil diez; dando por resultado, en lo que importa, que se instruyera al sujeto obligado a comunicar al peticionario el dato referido.*
Dicha resolución está visible en la siguiente liga:
file:///D:/Users/lfuentesm/Downloads/155%20(1).pdf

en mayor o menor medida, sobre los ciberataques de los que han sido objeto, lo que refuerza la idea de que se explique con mayor precisión, para cada punto planteado en la solicitud de acceso, porqué podría determinarse la reserva, o bien, porqué sería factible la divulgación.

Por tanto, de conformidad con lo dispuesto por el artículo 37, párrafos primero y segundo, de los Lineamientos Temporales[8], se **requiere** al Director General de Tecnologías de la Información, para que, en el plazo de cinco días hábiles, computados a partir del día siguiente al en que surta sus efectos la notificación de la presente resolución, justifique, desde la especifica prueba de daño, la reserva de información, de acuerdo a la causal o hipótesis respectiva de las encausadas en el artículo 113 de la Ley General.

Por lo expuesto y fundado; se,

R E S U E L V E:

ÚNICO. Se requiere al Director General de Tecnologías de la Información, en términos de lo expuesto en esta resolución.

Notifíquese al solicitante y a la instancia.

Así, por unanimidad de votos, lo resolvió el Comité de Transparencia de la Suprema Corte de Justicia de la Nación, y firman

---

[8] *"**Artículo 37***
Del cumplimiento de las resoluciones
Las resoluciones del Comité que ordenen acciones concretas a las instancias, deberán cumplirse dentro del plazo de cinco días hábiles a partir de su notificación.
Además del cumplimiento, las instancias deberán informar al Secretario y, en su caso, remitirle las constancias que lo acrediten dentro del plazo establecido en el párrafo anterior..."

los licenciados Alejandro Manuel González García, Secretario Jurídico de la Presidencia, Presidente; Magistrado Constancio Carrasco Daza, Titular de la Unidad General de Enlace con los Poderes Federales; y Juan Claudio Delgado Ortiz Mena, Contralor del Máximo Tribunal, integrantes del Comité, ante el Secretario del Comité, que autoriza y da fe.

LICENCIADO ALEJANDRO MANUEL GONZÁLEZ GARCÍA
PRESIDENTE DEL COMITÉ

MAGISTRADO CONSTANCIO CARRASCO DAZA
INTEGRANTE DEL COMITÉ

LICENCIADO JUAN CLAUDIO DELGADO ORTIZ MENA
INTEGRANTE DEL COMITÉ

LICENCIADO LUIS RAMÓN FUENTES MUÑOZ
SECRETARIO DEL COMITÉ