República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal

GERSON CHAVERRA CASTRO
Magistrado Ponente

SP135-2026
Radicación n° 69521
Acta No 073

Bogotá D.C., once (11) de marzo de dos mil veintiséis (2026).

ASUNTO

La Sala, con el fin de garantizar el principio de doble conformidad, examina la sentencia del 25 de marzo de 2025, emitida por la Sala Penal del Tribunal Superior de Bogotá. Con dicho fallo se revocó la decisión dictada el 20 de agosto de 2024, por el Juzgado Cincuenta y Cuatro Penal del Circuito con Funciones de Conocimiento de esta ciudad para, en su lugar, declarar a Luis Alberto Luengas Calle responsable por la comisión del delito de espionaje.

HECHOS

Entre los años 2018 y 2019, la Fuerza Aérea Colombiana tenía vigente un contrato con la ETB para efectos de recibir soporte en temas informáticos, entre ellos el relacionado con ciberseguridad. Para efectos de cumplir con esta labor, la ETB subcontrató a la empresa Ona Systems S.A.S., entidad que asignó a Luis Alberto Luengas Calle como el ingeniero de soporte que se encargaría de instalar, implementar y poner en marcha las herramientas de ciberseguridad al interior de esa fuerza armada.

Con ocasión de lo anterior y, con la intención de que pudiera cumplir con sus labores, la Fuerza Aérea Colombiana le entregó a Luengas Calle información secreta relativa a nombres de equipos y usuarios, así como direcciones IP de computadores asignados a altos mandos de esa institución, radares y del Centro de mando y Control de la FAC, entre otros datos.

Dicha información fue compilada por Luis Alberto Luengas Calle en un solo archivo Excel que denominó «*Estaciones de trabajo Fac*». En el mes de octubre de 2018, este documento fue publicado por Luengas Calle en las plataformas de internet «*SCRIBD*» y «*EDOC*», desde donde fue descargado en 14 ocasiones y visualizado 108 veces, permitiendo así que personas indeterminadas tuvieran acceso a datos que constituían secreto militar, dejando expuesta la seguridad del Estado en su componente aéreo.

ANTECEDENTES

1. El 28 de enero de 2020, ante el Juzgado Veintitrés Penal Municipal con Función de Control de Garantías de Bogotá, la Fiscalía le formuló imputación a Luis Alberto Luengas por la comisión del delito de espionaje (artículo 463 del Código Penal), cargo que no fue aceptado por el referido ciudadano.

Dado que no hubo solicitud en tal sentido, el imputado no fue afectado con ningún tipo de medida de aseguramiento.

2. El 1 de julio de 2020 la Fiscalía radicó escrito de acusación en contra del prenombrado, conservando los términos en los cuales le fuera formulada la imputación.

La actuación fue asignada al Juzgado Cincuenta y Cuatro Penal del Circuito con Funciones de Conocimiento de Bogotá, autoridad ante la cual, el 20 de octubre de 2020, se llevó a cabo la audiencia donde se verbalizó la acusación, sin que se registrara variación o aclaración respecto de los términos de la imputación.

3. La audiencia preparatoria se desarrolló en dos sesiones los días 31 de marzo y 19 de julio de 2023. El juicio oral se instaló el 14 de noviembre de ese mismo año, prolongándose hasta el 20 de agosto de 2024.

4. En vista pública del mismo 20 de agosto de 2024, el Juzgado Cincuenta y Cuatro Penal del Circuito con Funciones

de Conocimiento de Bogotá, dio lectura a la sentencia absolutoria proferida en favor de Luis Alberto Luengas Calle.

5. Dicha providencia fue objeto del recurso de apelación por parte de la delegada de la Fiscalía y la representación de víctimas, quienes solicitaron la revocatoria de la decisión para, en su lugar, proferir condena en contra del procesado por el delito que le fuera endilgado.

6. Con sentencia del 25 de marzo de 2025, la Sala Penal del Tribunal Superior de Bogotá resolvió revocar la providencia apelada y declaró a Luis Alberto Luengas Calle como autor responsable del delito de espionaje, imponiéndole una sanción de 72 meses de prisión e inhabilidad para el ejercicio de derechos y funciones públicas por ese mismo lapso. Aunado a lo anterior, le negó al condenado la suspensión condicional de la ejecución de la pena y la prisión domiciliaria, por expresa prohibición del artículo 68 A del Código Penal.

7. Tal decisión habilitó la interposición del recurso de impugnación especial para el acusado, y el de casación para las demás partes e intervinientes, interponiéndose únicamente el primero por parte del defensor del procesado, en tanto que, las demás partes, guardaron silencio.

SENTENCIA DE PRIMERA INSTANCIA

Tras presentar un recuento de la actividad probatoria y elaborar un marco teórico en torno al delito de espionaje, el *A*

quo consideró que, en el presente asunto, la Fiscalía no había logrado demostrar más allá de toda duda razonable la existencia del delito endilgado.

Partió por destacar que, durante el juicio oral, se demostró la vinculación laboral de Luis Alberto Luengas Calle con la empresa ONA System S.A.S., subcontratista de la ETB, empresa encargada de brindar seguridad informática a la Fuerza Aérea Colombiana FAC.

Adujo que se acreditó la existencia de un archivo denominado «*Estaciones de trabajo Fac*», el cual fue creado por el acusado en desarrollo de su actividad laboral dentro de la FAC, ello con el objetivo de tener un control sobre los equipos «*gestionados*» por él y los que ya contaban con una activación del antivirus. Afirmó tener por probado que ese documento fue consignado, entre los años 2018 y 2019, en dos «*reposarios de información*» de libre acceso, denominados «*SCRIBD*» y «*EDOC*», desde donde se calcula fue descargado por personas desconocidas, al menos, unas 40 veces.

Indicó que, pese a lo anterior, la Fiscalía no logró demostrar, primero, que quien publicó el documento denominado «*estaciones de trabajo FAC*», fue el procesado. Tampoco se acreditó que el contenido de ese archivo constituía secreto militar, ni que su divulgación puso en riesgo la seguridad nacional. Señaló que, si bien hubo un ataque direccionado a algunos correos electrónicos de la FAC, esta no podía vincularse con Luengas Calle.

Resaltó que no se demostró cuál fue el rédito obtenido por el acusado con la acción que le fuera endilgada; ni se descartó que la misma fuera ejecutada por un tercero, desde el equipo de cómputo de Luis Alberto Luengas. Desestimó que unas direcciones IP constituyeran secreto militar, toda vez que estas, por sí solas, no contienen información sensible.

En cuanto a la tipicidad de la conducta, aseguró que esta no se hallaba acreditada, pues no se demostró que la información publicada hubiera ido a parar a manos de un Estado enemigo o de una fuerza beligerante, poniendo así en riesgo la seguridad estatal. Sostuvo que, aun acogiendo la hipótesis de la Fiscalía, no se avizora un proceder doloso por parte del procesado, por cuanto desconocía que la información puesta en sus manos para el desarrollo de su trabajo, constituía secreto militar.

Así las cosas, consideró que había una duda razonable frente a la responsabilidad de Luis Alberto Luengas Calle en la comisión del delito de espionaje y, por tanto, se imponía la necesidad de proferir sentencia absolutoria en su favor.

DECISIÓN IMPUGNADA

Como primera medida, el *Ad quem* aseguró que, contrario a lo afirmado por el juez de primera instancia, las pruebas de cargo se ofrecen «*consistentes y coherentes*», por lo que logran colmar el estándar probatorio requerido para emitir una sentencia de carácter condenatorio.

Aseguró que, el caudal probatorio aportado por la Fiscalía, evidenciaba que la información contenida en el archivo denominado «*estaciones de trabajo FAC*», publicado en los portales de «*SCRIBD*» y «*EDOC*», sí tenía la potencialidad de atentar contra la seguridad nacional, pues unas pruebas ejecutadas por personal uniformado de la FAC, demostraron que los datos allí consignados permitían incursionar en el correo del oficial a cargo de entregar semanalmente la coordinación operacional de la Fuerza Aérea.

Agregó que, la información revelada era de tal nivel de sensibilidad para la seguridad nacional, que el Estado se vio en la obligación de incurrir en grandes costos a fin de mitigar el daño causado, debiendo cambiar direcciones IP, realizando encriptaciones, renovando equipos y dictando nuevas capacitaciones al personal de la FAC. Todo lo anterior porque, los datos publicados, podían llegar a manos de personas indeterminadas alrededor del mundo.

Indicó que, contrario a lo sostenido por el *A quo*, la jurisprudencia en torno al delito de espionaje no da cuenta sobre la necesidad de individualizar al destinatario de la información revelada, ni exige acreditar la existencia de algún tipo de provecho por parte de quien la publicó para de ese modo tener por demostrada la tipicidad del hecho.

En ese sentido, aseguró que lo realmente necesario en estos eventos es establecer la calidad de sensible de los datos publicados, como en efecto ocurrió en el *sub judice*, donde se

demostró que la información expuesta estaba relacionada con la infraestructura técnica de la FAC, quedando así expuesta, a nivel global, la seguridad nacional en su componente aéreo.

Explicó que, con ocasión de la libertad probatoria, no existe tarifa legal en torno a la demostración de lo que es o no secreto militar. En consecuencia, no puede esperarse a que exista un listado taxativo con los temas que ingresan en esa categoría, siendo suficiente apreciar el contenido de la información para, a partir de ello, determinar si se está o no ante un secreto militar.

Desde esa perspectiva, aseguró que no era difícil para el procesado y la empresa a la cual prestaba sus servicios, saber que la información entregada constituía secreto militar, pues su labor consistía en brindar «*soporte de software y hardware de toda la plataforma* ***de seguridad informática adquirida por la FAC***»; razón por la cual todos los empleados de Ona System S.A.S. debían suscribir cláusula de confidencialidad. Agregó que, además, Luengas Calle no era novato en el ejercicio de sus funciones, pues su experiencia abarcaba el manejo de datos sensibles desde el año 2013 en varias entidades del estado.

Destacó que, según la prueba técnica allegada, fue posible establecer que el documento con la información secreta fue publicado en las plataformas «*SCRIBD*» y «*EDOC*» desde un usuario llamado «*Alberto Calle*». Dicho acto de publicación, según el perito de la Fiscalía, implicaba el previo

agotamiento de varios pasos, de modo que no se trataba de una tarea simple. Y esa labor se cumplió desde el computador de trabajo asignado a Luis Alberto Luengas Calle.

A partir de lo anterior, el Tribunal resaltó:

> «*Y es que no podía dejarse en grado de coincidencia, que aunado a lo anterior: i) quien aparece como usuario responsable de su exhibición se denominó "Alberto Calle", datos que se ajustan al segundo nombre y segundo apellido del aquí acusado; ii) la plataforma visualizaba una fotografía del usuario que señalaron los testigos, se corresponde con el acusado, iii) el documento que aparecía en Scribd, concuerda con la información que debía contar Ona System, para el desarrollo del contrato, empresa de la cual, el procesado era contratista, iv) en juicio oral el procesado renunció a su derecho de guardar silencio, aceptó que era usuario de Scribd y de Facebook, v) que una vez fue requerido por la empresa, afirmó que bloqueó la visualización del archivo, lo que sugiere un dominio de claves, vi) el equipo asignado por Ona System contaba con un usuario y contraseña y vii) no señaló los nombres de otras personas que tuvieron acceso al equipo.*»

Finalmente, tras realizar una síntesis sobre el contenido de las pruebas de descargo, el *Ad quem* concluyó que estas no lograban desvirtuar a las ofrecidas por la Fiscalía, las cuales permitieron acreditar que la autoría del hecho investigado estuvo en cabeza del procesado.

Destacó que, incluso, los testimonios entregados por los testigos de la defensa permitían corroborar que, la información manejada por el procesado en el ejercicio de sus funciones era sensible, por tratarse de datos relacionados con la «*seguridad del conjunto equipos* (sic) *que preservan información*

relacionada con las funciones constitucionales que cumple el cuerpo armado».

DE LA IMPUGNACIÓN ESPECIAL

La defensa de Luis Alberto Luengas Calle formuló dos cargos concretos en contra de la sentencia de segundo grado.

1. Como primer reproche, el recurrente aseguró que en el presente caso se produjo una «*Violación del principio universal de in dubio pro reo (C.P.P. Art. 7) y la garantía constitucional de presunción de inocencia (C.N. Art. 29), por cuanto dentro del proceso penal, no se encuentra suficientemente probada la materialización del delito de espionaje.*»

Explicó que, para concretar el tipo penal de espionaje, la norma exige que el sujeto activo «*indebidamente revele secreto militar relacionado con la seguridad del Estado*». Señaló que, en el presente caso, no resulta claro que el documento revelado por Luis Alberto Luengas se clasifique en esa modalidad de información, ya que su contenido, por sí solo, «*no era suficiente para estructurar un ataque cibernético, sino que eran necesarios otros insumos*», como bien lo revelaron los testigos Juan Manuel Rodríguez López y Khristian Jaffet Morales Vargas.

Resaltó que, desde el punto de vista técnico, posible es sostener que la sola información contenida en el documento denominado «*Estaciones de trabajo FAC*», el cual compila unos nombres de usuarios y unas direcciones IP, no permite acceder a los correos electrónicos de la referida fuerza

armada. Agregó que, «*el documento "Estaciones de Trabajo FAC", no contiene datos que permita el acceso no autorizado a sistemas críticos, ni contraseñas activas, claves cifradas, tokens, direcciones de correos electrónicos, ni rutas vulnerables a intrusión externa*».

Indicó que, ese archivo, tan solo registra «*los nombres de sistema, el estado gestionado, la dirección IP, el nombre del usuario, y el tipo de sistema operativo, datos que por sí solos no permiten estructurar un ataque cibernético*». Agregó que, si en un momento determinado el Mayor Juan Manuel Rodríguez López pudo ingresar a un correo electrónico valiéndose de esa información, fue porque la complementó con datos externos, unos que no estaban allí consignados, aspecto que fue soslayado por el *Ad quem*.

Manifestó que, en ese sentido, la aludida información no puede ser considerada como secreto militar. Que esa categoría le fue atribuida tan solo porque se produjo su publicación en dos portales web, lo cual resulta contraria al principio de legalidad estricta, ya que los datos allí vertidos no pueden ser catalogados como un secreto militar.

Señaló que en el presente asunto no se demostró quién fue el beneficiario o receptor de la información divulgada. Tampoco se acreditó que la seguridad del estado se hubiera visto comprometida, ya que «*en primer lugar el Estado Colombiano no se encontraba inmerso en un conflicto internacional para la fecha de ocurrencia de los hechos materia de investigación, y en segundo lugar, el ente acusador no probó que el documento intitulado "Estaciones de Trabajo FAC", hubiera sido descargado por las fuerzas de seguridad de un Estado enemigo del Estado Colombiano*».

2. Como segundo cargo el impugnante planteó la existencia de una atipicidad en la conducta. Aseguró, primero, que de acuerdo con las manifestaciones efectuadas por el testigo Juan Manuel Rodríguez López, no se pudo establecer quién fue el destinatario de la información publicada. Y, segundo, cuestionó que el Tribunal hubiera restado importancia a esa temática para, de manera equivocada, pasar a sostener que no era relevante llegar a determinar quién era el destinatario de los datos revelados.

Adujo que, al ser un tipo de peligro, el delito de espionaje sí exige establecer quién es el destinatario de la información publicada, siendo irrelevante si al final la misma es o no usada por su receptor, ya que ahí radica precisamente la tipicidad de la conducta: en la puesta en peligro de la seguridad estatal por parte de un estado enemigo.

Bajo esa lógica, indicó que «*si el adversario no recibe la información, sencillamente la seguridad del Estado no se pone en riesgo, y por lo tanto no hay delito, ya que el delito se configura cuando se transmite información secreta al adversario, situación que le da una ventaja en el campo de las hostilidades y por lo tanto se pone en riesgo la seguridad del Estado*».

Insistió en señalar que, en todo caso, la información contenida en el archivo denominado «*Estaciones de trabajo Fac*», no era clasificada, por cuanto la misma no revelaba «*información personal, correos electrónicos, contraseñas activas, claves cifradas, tokens, que permitiera el acceso no autorizado a sistemas*

críticos de la Fuerza Área Colombiana y que por ende comprometiera la seguridad del Estado Colombiano».

INTERVENCIÓN DE LOS NO RECURRENTES

1. El representante legal de las víctimas solicitó confirmar la sentencia condenatoria proferida en contra de Luis Alberto Luengas Calle, en virtud de las siguientes consideraciones:

Indicó que, en Colombia, existen dos categorías para limitar el acceso a la información, denominadas «*información calificada*» e «*información clasificada*», las cuales están reguladas, respectivamente, en las leyes 1712 de 2014 y 1621 de 2013.

En lo que atañe a la primera legislación, explicó que «*la "información calificada" se refiere a aquella que, debido a su naturaleza, ha sido sujeta a restricciones específicas por razones de seguridad, defensa nacional, o por la protección de derechos fundamentales*»: Por su parte, la Ley 1621 se refiere a la protección de la información en el marco de actividades de Inteligencia y Contrainteligencia. Así, aseguró, «*La "información clasificada" bajo esta ley, tiene un enfoque más específico en cuanto a la protección de la información, dado que la misma deriva del ejercicio de ejecución de actividades de organismos públicos que llevan a cabo actividades de inteligencia y contrainteligencia*».

En lo que respecta al Secreto Militar, afirmó que se trata de «*información cuya divulgación podría poner en riesgo la seguridad y d*

e

fensa de la nación».

Con fundamento en la anterior explicación, el apoderado de las víctimas señaló que el recurrente incurrió en yerros conceptuales que impiden acceder a sus pretensiones, pues, finalmente, la información revelada por el procesado sí constituye secreto militar, ya que incorpora datos sensibles relacionados con la seguridad aérea del estado colombiano.

2. El delegado de la Fiscalía presentó un extenso escrito donde, básicamente, consignó los apartes probatorios que consideró más relevantes para la resolución del asunto, presentando junto a ellos un análisis de ellos.

Señaló que, el memorial de impugnación especial se centró en tres aspectos relevantes: *i)* naturaleza y clasificación del documento divulgado; *ii)* peligro real y potencial de la divulgación, y; *iii)* ausencia de información personal en el archivo divulgado.

Resaltó que el impugnante, al limitarse a esos puntos, dejó de lado otros temas discutidos a lo largo del juicio, como que el archivo fue publicado por una misma persona en dos plataformas digitales diferentes; que dicho acto fue ejecutado por el procesado; la existencia de un compromiso de confidencialidad quebrantado por Luengas Calle, entre otros, aspectos todos estos relevantes cuyo análisis conjunto permitió inferir la responsabilidad del acusado en los hechos objeto de juzgamiento.

Destacó que, en la actualidad, el tipo penal de espionaje no contempla como elemento constitutivo el verificar que la información sustraída fuera entregada a una «*potencia enemiga*» en medio de un estado de guerra, como sí acontecía en legislaciones anteriores. En la actual redacción, dicha conducta sólo reclama verificar que se haga pública una información de carácter secreto proveniente del ámbito político, económico y militar. Además, exige verificar que, tal divulgación, ponga en riesgo la seguridad del Estado.

En virtud de lo anterior, señaló que se equivoca la defensa cuando pretende desestimar el actuar del procesado asegurando que no hay prueba en torno a determinar quién fue el destinatario de la información publicada, ya que ese aspecto resulta irrelevante al momento de demostrar la existencia del delito de espionaje.

Afirmó que, contrario a los sostenido por el impugnante, las pruebas practicadas en juicio sí permitieron demostrar que la información publicada por el procesado en dos portales web sí ponía en riesgo la seguridad aérea del estado, pues los datos allí detallados mostraban la ubicación de al menos 9 radares civiles y militares.

En suma, señaló que las pruebas practicadas en juicio oral permiten determinar la responsabilidad de Luis Alberto Luengas Calle en el delito de espionaje y, por tanto, solicitó confirmar la sentencia condenatoria dictada en su contra por ese reato.

CONSIDERACIONES

1. La Sala es competente para conocer de la impugnación interpuesta por el defensor de Luis Alberto Luengas Calle, contra la sentencia emitida por la Sala Penal del Tribunal Superior de Bogotá el 25 de marzo de 2025, de conformidad con lo dispuesto en el numeral 7º del artículo 235 de la Constitución Política de Colombia, modificado por el Acto Legislativo 01 de 2018 y el criterio mayoritario plasmado en la decisión CSJ AP1263-2019 del 3 de abril de 2019.

2. De acuerdo con la sustentación del recurso impetrado, la Sala deberá estudiar: *i)* Si la conducta endilgada a Luis Alberto Luengas Calle logra materializar el punible de espionaje, como lo sostuvo la Fiscalía en el acto de acusación y; *ii)* si existen elementos de convicción suficientes en virtud de los cuales se pueda deducir, más allá de toda duda razonable, la responsabilidad penal del referido ciudadano en la comisión del aludido delito.

3. Del espionaje.

3.1. Concepto.

Desde la etimología, *los términos espía o espionaje derivan de la raíz indoeuropea spek-, que significa «observar». De esta raíz derivan varios términos como los latinos species (vista, apariencia) y -specio (mirar, de dónde a su vez «espectáculo», «aspecto»), los griegos sképtomai (examinar, de dónde «escéptico») y skópos (que vigila, y de ahí «calidoscopio», «telescopio» o «epíscopo» u obispo) o el germánico spehon,*

de donde provienen nuestras palabras «espía» y «espionaje». En definitiva, «espionaje» significa «observación»[1].

Congruente con lo anterior, la Convención de La Haya de 1907, donde se recoge el «*Reglamento sobre las leyes y costumbres de la guerra terrestre*», señaló que «*Sólo puede considerarse espía a una persona cuando, actuando clandestinamente o con falsos pretextos, obtiene o intenta obtener información en la zona de operaciones de un beligerante, con la intención de comunicarla a la parte hostil. (…)*».

En ese sentido, la RAE, definió la palabra espionaje como la «*actividad secreta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad defensiva y ofensiva*».

En consecuencia, puede sostenerse entonces que el espionaje es aquella actividad clandestina desplegada por una persona que, a partir de la observación, busca recaudar y compartir información que comprometa la seguridad de un Estado.

3.2. Recuento histórico del delito de espionaje en Colombia[2].

Diversas han sido las variaciones que, a través del tiempo y las legislaciones penales, ha sufrido el delito de espionaje en nuestro país. Todas ellas, relacionadas con un

[1] Ruiz Miguel Carlos, Servicios de Inteligencia y Seguridad del Estado Constitucional. Editorial Tecnos. 2002.
[2] Sobre el particular, consultar CSJ SP del 28 de noviembre de 2007, Rad. 27650.

contexto histórico del momento, así como con las posturas dogmáticas propias de la época.

Tras la expedición de la Constitución de 1886 y, con ella, el retorno de un régimen centralista a Colombia, el legislador profirió la Ley 19 de 1890[3], que, en su Libro Segundo, agrupó los «*Delitos que afectan principalmente a la Nación o a la sociedad, o que sean cometidos por empleados públicos*»; encargándose el Título Primero de los «*Delitos contra la Nación*», centrándose el Capítulo Primero en la «*Traición y otros delitos semejantes*».

Si bien en aquél entonces el legislador no tipificó de manera expresa el delito de espionaje, sí recogió en los artículos 150 y 153 del aludido compendio normativo, una serie de supuestos fácticos equiparables a ese punible, indicando que:

> «*Art. 150. Son reos de grave delito de traición, en guerra exterior, los colombianos que ejecuten alguno de los siguientes hechos: (…)*
> *3. Servir de espías al enemigo, o acoger, proteger, ocultar o auxiliar, voluntariamente y a sabiendas, a dichos espías, para que puedan desempeñar su encargo en perjuicio de la Nación;*
> *4. Comunicar a los enemigos algún plan, instrucción o cualesquiera avisos o noticias importante, acerca de la mala situación política, económica o militar de la Nación, con el objeto de que le hagan la guerra o se aperciban para ella, o la continúen ventajosamente; o bien suministrar, procurar o facilitar a dichos enemigos, recursos, auxilios, socorros, planos de fortificaciones, de puertos o arsenales, o cualesquiera otros medios importantes para los fines expresados; (…)*

[3] Codigo (sic) Penal de la República de Colombia Ley 19 de 1890 (de 19 de octubre). Universidad del Rosario.

Art. 153. Son reos de delito menos grave de traición en guerra exterior los colombianos que ejecuten alguno de los siguientes hechos: (…)
4. Entregar, a sabiendas, a los Agentes de alguna potencia extranjera neutral, planos o diseños de fortificaciones, puertos o arsenales de que estén encargados por razón de su destino, o descubrirles el secreto de alguna negociación o expedición, de que se hallan instruidos oficialmente, por su ministerio; (…)»

El artículo 154 del Código Penal de 1890, establecía que también incurrían en las anteriores conductas «*los extranjeros que ejecuten los hechos referidos, siendo empleados públicos o estando al servicio del Gobierno*».

Como puede evidenciarse, en aquél entonces la conducta de espionaje estaba ligada a que, ante el escenario de una «*guerra exterior*», nacionales colombianos o extranjeros al servicio del gobierno, suministraran al enemigo -entiéndase otro Estado según el contexto de guerra- información que pudiera poner en condición de desventaja al Estado colombiano.

Ahora bien, hacia la segunda década del siglo XX empezaron a llegar a Colombia las influencias de lo que se conoció como «*La Escuela Positivista del Delito*», cambio dogmático que finalmente derivó en la promulgación de un nuevo Código Penal, el cual se conoció como la Ley 95 de 1936.

El Título Primero, del Libro Segundo de esa obra, se denominó «*Delitos Contra la Existencia y la Seguridad del Estado*» y, su Capítulo Primero, se dedicó a los «*Delitos de Traición a la patria*». Dentro de este último, el artículo 122 establecía:

> «*El colombiano, aunque haya perdido la calidad de nacional, o el extranjero que deba obediencia a Colombia a causa de su empleo o función pública, que revele los secretos políticos, diplomáticos o militares referentes a la seguridad del Estado, ya comunicando o publicando los documentos, dibujos, planos u otros datos relativos al material, fortificaciones u operaciones militares o cualquiera otro asunto esencial para la defensa de los intereses del país, ya facilitando de otra manera su divulgación, está sujeto a presidio, de dos a cuatro años, y multa de trescientos a mil pesos.*»

La misma norma consideraba que esa conducta se agravaba cuando los secretos eran revelados a: *i)* gobierno de otra nación; *ii)* un Estado que se hallara en guerra con Colombia; o cuando *iii)* la revelación llevara a que se interrumpieran o turbaran las relaciones amistosas de Colombia con otra nación y; *iv)* si el responsable había conocido los secretos por su condición de funcionario, o si había acudido al uso de la violencia o el fraude para obtener el conocimiento.

En este estadio histórico logra advertirse que, aun cuando todavía no se adopta el *nome iuris* de espionaje, en tanto la conducta descrita aún se denomina traición a la patria, la revelación de secretos deja de constituir, como sucedía en el Código de 1890, un delito típico de guerra exterior. Asimismo, esta legislación introdujo el concepto de «*Seguridad del Estado*», como bien jurídico penalmente tutelado, y abandonó aquella concepción según la cual, el delito en comento sólo podía ser cometido en favor de otra nación, adoptando una visión más amplia, donde se punía el simple acto de revelación de secretos, siendo apenas una causal de

agravación el que el destinatario de la información fuera otro Estado.

El 23 de enero de 1980, el Gobierno Nacional promulgó el Decreto Ley 100 de ese año, por cuya virtud se adoptó un nuevo estatuto penal. Acá, el Título I del Libro Segundo se ocupó de los «*Delitos contra la Existencia y Seguridad del Estado*» y, dentro de este, se destinó el Capítulo Primero para condensar los «*delitos de traición a la patria*», en tanto que el Capítulo Segundo se ocupó de los «*delitos contra la seguridad del estado*». Dentro de esta última categoría, por primera vez, se tipificó el espionaje como conducta autónoma, bajo los siguientes términos:

> «*Artículo 119. Espionaje. El que indebidamente obtenga, emplee o revele secreto político, económico o militar, relacionado con la seguridad del Estado, incurrirá en prisión de tres a doce años.*»

Como se puede notar, a partir de esta codificación, el espionaje dejó de considerarse como un acto de traición a la patria, para ser tenido como una conducta que atentaba contra la seguridad del Estado. En virtud de lo anterior, se adoptó una visión absolutamente amplia con respecto al modo como podía materializarse ese punible, abandonando por completo el clásico supuesto fáctico que ubica a otro Estado como el beneficiario de la labor de espionaje.

Así, a partir de ese entonces, lo relevante no era determinar quién era el destinatario de la información obtenida, empleada o revelada por el espía, sino determinar que la misma, además de constituir secreto político,

económico o militar, pusiera en riesgo la seguridad del Estado.

Finalmente, la Ley 599 de 2000, en su Libro Segundo, Título XVII -Delitos contra la existencia y seguridad del Estado-, Capítulo Segundo -Delitos contra la seguridad del Estado-, tipificó la conducta de espionaje en el artículo 463, conservando en su integridad la redacción contenida en el Decreto Ley 100 de 1980.

Como se puede apreciar, hoy en día el delito de espionaje presenta una connotación muy distinta a la que motivó su inicial vinculación delictuosa a fines del siglo XIX y durante gran parte del siglo XX, ya que, tras concluir la segunda guerra mundial, la revelación de secretos militares, económicos o políticos no conservó en nuestro país la trascendencia que originalmente vinculó el hecho con la existencia o seguridad exterior del estado, al punto que se desligó del *nomen iuris* de traición a la patria, para pasar a verificar el daño dentro de un ámbito más focalizado como es el de la seguridad nacional, entendiendo que esa revelación de información reservada, que nutre dentro de la concepción patria la conducta punible examinada, más que beneficiar hipotéticas confrontaciones externas, afecta la estabilidad misma del Estado.

3.3. Del delito de espionaje en la Ley 599 de 2000.

El artículo 463 de la aludida legislación, tipifica el delito en comento bajo los siguientes términos: «*El que indebidamente*

obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado».

En ese sentido, se tiene entonces que la aludida descripción típica presenta la siguiente estructura dogmática: *i)* un sujeto activo indeterminado; *ii)* el sujeto pasivo lo constituye el Estado, ya que el bien jurídico penalmente tutelado es, precisamente, el de su seguridad; *iii)* presenta tres verbos rectores alternativos: obtener, emplear o revelar; *iv)* exige que la ejecución de sus verbos rectores se verifique bajo el criterio de «*indebidamente*», esto es, de forma ilícita, irregular, subrepticia o tramposa; *v)* integra como ingredientes normativos los conceptos de: secreto político, económico, militar y seguridad del Estado; *vi)* es un tipo penal de resultado y peligro presunto, al tiempo que su ejecución es instantánea y; *vii)* se trata de una conducta eminentemente dolosa.

En punto de los ingredientes normativos, pertinente es señalar que, de acuerdo con la RAE, la primera acepción del vocablo secreto corresponde a «*Cosa que cuidadosamente se tiene reservada y oculta*», en tanto que la segunda, hace referencia a «*reserva, sigilo*».

Así las cosas, puede asegurarse entonces que el concepto de secreto político, económico y militar, hace referencia a la reserva que el Estado impone a cierta y determinada información que, por su delicadeza, debe ser manejada con sigilo a fin de no comprometer la estabilidad de sus instituciones, la confiabilidad de sus finanzas y la

capacidad de defensa o ataque armado; de ahí que esos conceptos se encuentren íntimamente ligados con el de seguridad del Estado, el cual se puede definir como aquel conjunto de medidas o acciones adoptadas por el aparato gubernamental con el objeto de prevenir, contener y enfrentar cualquier tipo de amenaza, interna o externa, que ponga en riesgo la existencia del Estado, su soberanía, la integridad del territorio, la seguridad de sus ciudadanos y su estabilidad económica o política.

De ahí que dicho concepto involucre, principalmente, aspectos relacionados con los órdenes: *i)* Militar. Relativo a la capacidad del Estado para ejercer, mediante el uso de la fuerza, la protección de su territorio y de sus ciudadanos; *ii)* Político. Enfocado en mantener una estabilidad institucional que permita el pacífico desarrollo de la Nación, y; *iii)* Económico. Orientado a asegurar una estabilidad de orden financiero que contribuya con el crecimiento y fortalecimiento del poder estatal[4].

Ahora bien, nótese que, de acuerdo con la evolución histórica surtida en torno al modo como se tipifica la conducta de espionaje, en la actualidad la legislación penal colombiana no condiciona la materialización de la conducta al hecho de verificar si, el secreto obtenido, empleado o revelado por el sujeto agente, tenía como destinataria una persona o entidad determinada, sino que tan solo exige

[4] Al respecto consultar «*El concepto de Seguridad en América Latina hasta la segunda década del siglo XXI*» de Alejandro Cerón Rincón. Escuela Superior de Guerra General Rafael Reyes Prieto.

constatar si la consumación de alguno de los verbos rectores descritos en el tipo penal, comprometió la seguridad del Estado en alguna de las vertientes allí detalladas.

En ese sentido, irrelevante resulta cualquier discusión en torno a establecer si, el secreto irregularmente sustraído, tuvo o no un destinatario específico; o si el mismo fue o no efectivamente usado por alguna persona, entidad o Estado, en contra de Colombia; así como también resulta superfluo determinar si se produjo un daño real y efectivo a la seguridad nacional. Lo anterior porque, se insiste, la conducta descrita en el artículo 463 del Código Penal, pune el simple hecho de poner en riesgo la seguridad del Estado a partir de la obtención, empleo o revelación de un secreto político, económico o militar.

4. De la información pública y militar, su clasificación y manejo.

4.1. Con el objeto de regular el derecho de acceso a la información pública, los procedimientos para su ejercicio y las excepciones a la publicidad de información, el Legislador colombiano expidió la Ley 1712 de 2014, la cual, según su artículo 5, es aplicable a:

> «*a) **Toda entidad pública**, incluyendo las pertenecientes a todas las Ramas del Poder Público, **en todos los niveles de la estructura estatal**, central o descentralizada por servicios o territorialmente, **en los órdenes nacional**, departamental, municipal y distrital.*

b) Los órganos, organismos y entidades estatales independientes o autónomos y de control. (…)» (Resaltado fuera de texto)

Mediante sentencia C-274 de 2013[5], la Corte Constitucional declaró inexequible el Parágrafo 2 de ese artículo, el cual pretendía exceptuar de la aplicación de esa legislación a «*la información, documentos, bases de datos y contratos relacionados con defensa y seguridad nacional, orden público y relaciones internacionales*». En consecuencia, los conceptos, regulaciones y restricciones contenidos en la mencionada Ley, resultan aplicables a las Fuerzas Armadas.

Ahora bien, el artículo 6 de la Ley 1712 de 2014 señala que información es «*un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen*». Asimismo, establece que la categoría denominada «*información pública reservada*» es «*aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley*».

Congruente con lo anterior, el canon 19 del mentado compendio normativo clasifica como «*información exceptuada por daño a los intereses públicos*», a aquella que previamente ha sido catalogada como «*pública reservada*» y guarda relación, entre otros temas, con: a) la defensa y seguridad nacional; b) la seguridad pública y; c) las relaciones internacionales. La restricción de acceso a este tipo de información, debe estar

[5] Control de constitucionalidad previo a los Proyectos de Ley 228 de 2012 Cámara, 156 de 2011 Senado, posteriormente conocidos con Ley 1712 de 2014.

contenida, bien sea en la Constitución Política de Colombia, ora en algún tipo de normatividad que así lo establezca.

4.2. Ahora bien, mediante la expedición de la Ley 1621 de 2013, el Congreso de la República reguló las actividades de inteligencia y contrainteligencia del país, norma que, en su artículo 37, le impuso al Gobierno Nacional la obligación de reglamentar los «*niveles de clasificación de la información*». Esta temática fue abordada en el artículo 11 del Decreto 857 de 2014, cuyo tenor literal, en lo que interesa para el caso, es el siguiente:

> «*Niveles de clasificación de la información. Los niveles de clasificación de seguridad de la información que goza de reserva legal serán los siguientes:*
> *(…)*
> *d) Restringido. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan* ***información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia****, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes. (…)*» (Resaltado de la Sala).

4.3. De acuerdo con el anterior marco normativo, posible es asegurar que, en la actualidad, existe información de carácter público que, obedeciendo a diversos criterios, entre los que se encuentra la defensa y seguridad nacional, goza de algún grado de restricción para su divulgación.

En ese sentido, acertado es sostener que toda aquella información relacionada con la infraestructura física y

tecnológica de las Fuerzas Armadas de Colombia, se halla protegida mediante la imposición de algún grado de reserva legal, ello, con la única finalidad de garantizar la seguridad del Estado.

Lo anterior, se vio reflejado en la emisión, por parte del Comandante de la Fuerza Aérea Colombiana, de la Disposición 018 de 2015, documento de carácter clasificado mediante el cual se adoptó el «*Manual de Ciberdefensa y Ciberseguridad*»[6], donde se consigna, entre otros aspectos, la identificación de aquellos elementos considerados como «*infraestructura crítica y especial*» de ese órgano armado, reclamando una particular protección de estos, así como de los «*activos tecnológicos y de información de la Fuerza Aérea*».

Así las cosas, el hecho de que al interior de la Fuerza Aérea Colombiana exista un «*Manual de Ciberdefensa y Ciberseguridad*», cuyo contenido es de carácter clasificado y, por ende, secreto para el público en general por razones de seguridad nacional, hace que cualquier dato o información relacionada con los activos críticos allí relacionados, también adquieran esa naturaleza, surgiendo así una restricción para su divulgación en razón al riesgo que supone a la infraestructura militar y, por ende, a la seguridad del Estado.

5. Del caso concreto.

De acuerdo con la acusación formulada por la Fiscalía, el 10 de octubre de 2018, Luis Alberto Luengas Calle publicó

[6] Disposición vigente para el momento de los hechos y modificada con posterioridad a su ocurrencia.

en las plataformas abiertas de internet denominadas «*SCRIBD*» y «*EDOC*», un documento tipo Excel denominado «*Estaciones de Trabajo Fac*», el cual contenía 5306 líneas con nombres de equipos, direcciones IP, nombres de usuario, tipos de sistemas operativos de terminales de cómputo y radares de la FAC.

Dado que esa información se considera secreto militar, por guardar relación con la seguridad aérea de Colombia, el ente acusador estimó que la acción ejecutada por Luengas Calle era constitutiva del delito de espionaje -verbo rector revelar-, ya que con ella puso en riesgo la seguridad del Estado, al suministrar a personal indeterminado insumos que podían derivar en ataques cibernéticos que comprometieran la infraestructura crítica aeronáutica.

En contraposición, el defensor de Luis Alberto Luengas Calle aseguró que, la Fiscalía, no pudo demostrar la materialidad de la conducta endilgada a su representado por cuanto: *i)* no probó que fue Luengas Calle quien publicó el documento denominado «*Estaciones de Trabajo Fac*»; *ii)* no acreditó la condición de secreta de la información revelada; *iii)* no estableció quién era el destinatario de la publicación y su contenido y; *iv)* no demostró cuál fue el rédito obtenido por el procesado con ese proceder.

Aseguró que, en todo caso, la información revelada resulta insuficiente para, por sí sola, permitir la ejecución de un ataque informático, razón por la cual la seguridad del

Estado no estuvo en riesgo. Así las cosas, consideró que, en el presente evento, se está ante el juzgamiento de una conducta que se ofrece como atípica.

Tomando como punto de partida las teorías que del caso formularon Fiscalía y defensa, la Sala procederá a realizar la correspondiente valoración probatoria con el objeto de determinar cuál de las dos se encuentra debidamente acreditada.

5.1. Del análisis y la valoración probatoria.

5.1.1. Con el objeto de demostrar su teoría del caso, la Fiscalía trajo al juicio oral los testimonios del Coronel Iván Darío Paipa Moscoso, Subdirector de Ciberseguridad de la FAC para los años 2018 y 2019; el Mayor Juan Manuel Rodríguez López, Subdirector de Ciberdefensa Aérea de la FAC en ese mismo periodo y del ingeniero de sistemas Juan Camilo Palacios, suboficial de la Fuerza Aérea para la época de los hechos.

Los mencionados testigos recordaron que, hacia finales del mes de enero de 2019, fueron informados sobre la existencia de una serie de correos electrónicos remitidos a varios funcionarios de esa fuerza armada en Cali, donde se les indicaba que su seguridad había sido comprometida, razón por la cual les era posible enviar ese mensaje desde su propio usuario. Además, en el mismo correo, se amenazaba

a los destinatarios con publicar imágenes comprometedoras si no pagaban determinada suma de criptoactivos.

Los mencionados correos fueron sometidos a un análisis por parte del Técnico Cuarto Juan Camilo Palacio y el Mayor Juan Manuel Rodríguez, quienes encontraron que el tráfico de la información se originó en los servidores de la FAC. Coincidieron en indicar los deponentes, que con el nombre específico del servidor identificado, se adelantó una búsqueda sencilla en internet, encontrando que el mismo se hallaba «*atado*» a la página web «*SCRIBD*», la cual es un «*repositorio*» de información de público acceso, donde encontraba publicado un documento denominado «*Estaciones de trabajo Fac*», el cual registraba entre 30 y 40 descargas.

Señalaron que el referido documento contenía alrededor de cinco mil registros relacionados con direccionamientos IP, nombre de usuario y máquina, la *mac* del computador y el sistema operativo; información relevante que se constituía en insumo para un ataque cibernético de gran escala.

Explicaron que, los datos divulgados hacen parte de la «*infraestructura crítica de la Fuerza Aérea*», la cual puede ser definida como aquella que les permite «*volar, cumplir operacionalmente y adelantar operaciones militares*». Indicaron que un ciberataque pudo comprometer la operatividad de los radares y, con ello, afectar la seguridad aérea de todo el país, tanto en su componente militar, como en el civil.

Destacaron que, el contenido del documento divulgado se encuentra directamente relacionado con la operación estratégica de la FAC. Los datos allí consignados permitían «*acceder a información de operaciones, inteligencia, estrategia, que no es normal que sea pública ni que cualquier persona pueda acceder a ella*». Aseguraron que, dentro de la información revelada, se encontraba el direccionamiento IP del Centro de Comando y Control de la Fuerza Aérea, el cual se encarga de manejar información sensible de seguridad.

Indicaron que, tras advertir la exposición de la información, procedieron a buscar quién fue la persona encargada de ejecutar dicho acto. Así, partieron por ubicar el nombre del usuario que divulgó el documento en la plataforma «*ESCRIBD*» y luego verificaron si al interior de la FAC había algún funcionario con acceso a esa información. El resultado de esas pesquisas los llevó a Luis Alberto Luengas Calle, empleado de la empresa Ona Systems, subcontratista de la ETB, persona jurídica que celebró con la Fuerza Aérea un contrato para brindarles asistencia en temas de seguridad, soporte y tecnología informática.

El Coronel Paipa Moscoso explicó que, Luengas Calle, era una de las personas a cargo de cumplir con el objeto del contrato celebrado con la ETB, encargándose de brindar soporte en seguridad informática. En ese sentido, tenía acceso al Cuartel General de la FAC, en el CAN; conocía las herramientas de seguridad de la Fuerza Aérea y su funcionamiento; estaba al tanto del inventario de activos de esa fuerza y contaba con acceso a la información que fue

revelada. En concreto, conocía toda la infraestructura cibernética de la FAC.

Señaló que, a fin de proteger su información frente a terceros, la Fuerza Aérea Colombiana hace suscribir a sus contratistas unos acuerdos de confidencialidad. Para el caso, los mismos fueron firmados con la ETB, que a su vez se los impuso a Ona Systems, que luego los trasladó a Luis Alberto Luengas Calle. Así las cosas, asegura, todos los antes mencionados sabían con suficiencia que la información confiada a ellos para efectos de la ejecución del mencionado contrato tenía el carácter de reservado, dada su importancia estratégica.

Finalmente explicó que, aun cuando desconoce si existe algún tipo de acto administrativo por cuyo conducto se haya catalogado como secreta la información revelada, no puede desconocerse que la misma sí gozaba de esa condición dada su incidencia en la seguridad nacional.

A su turno, el Mayor Juan Manuel Rodríguez López precisó que los correos electrónicos remitidos a los funcionarios de la FAC en Cali, fueron sometidos a una serie de pruebas, encontrando que estos lograban evadir el primer filtro de seguridad, relativo al antispam.

Puntualizó que, los datos divulgados hacían parte de la infraestructura crítica de la Fuerza Aérea Colombiana, como: *i)* los radares, los cuales constituyen el activo crítico de mayor

importancia de la FAC, por cuanto son la primera línea de defensa aérea del país; *ii)* el mando y control, que es un sistema que permite a los oficiales comandantes de batalla, ejercer control sobre las unidades desplegadas por ellos. Este sistema se centraliza en Bogotá; *iii)* cuentas y usuarios de algunos Generales, y; *iv)* información de ciertos servidores.

Indicó que esa información no es de carácter público. Agregó que la reserva de esa información está fijada en los manuales de Ciberdefensa y Ciberseguridad, los cuales definen cuál es la infraestructura crítica de la Fuerza Aérea.

Explicó que, con la información hallada, realizaron una «*prueba de concepto*», la cual consiste en simular un ataque informático para lograr determinar hasta dónde se puede penetrar en el sistema. Ese ejercicio los llevó a acceder al correo del oficial encargado de remitir la comunicación que resulta de la reunión operativa que se celebra todos los miércoles, donde se suministra detalles relacionados con las características operacionales de la fuerza a lo largo de la semana.

Aseguró que la información divulgada está directamente relacionada con la seguridad nacional, porque a partir de ella es posible elaborar un diagrama de red que permita determinar dónde se encuentran localizados los sistemas de la FAC, brindando así un panorama amplio a cualquier hacker que pretenda vulnerar los sistemas de la Fuerza, comprometiéndose así la defensa del Estado.

Por último, explicó que el secreto militar no radica en ocultar la existencia de la infraestructura, sino la manera como la misma funciona. En consecuencia, revelar las direcciones IP de los equipos radar, pone en riesgo su operatividad, luego esos datos constituyen secreto militar.

El Ingeniero de Sistemas Juan Camilo Palacios, además de referirse a la calidad de la información, su procedencia e importancia, el modo como fue hallada y los resultados de la «*prueba de concepto*», indicó que a su cargo estuvo corroborar si los datos divulgados realmente correspondían a la FAC, encontrando que ello era así.

Durante su intervención en el juicio oral, le fue exhibida la «*prueba de concepto*» realizada por él y el Mayor Juan Manuel Rodríguez López, identificando allí los radares que fueron expuestos en el documento publicado.

5.1.2. Adicionalmente, el delgado de la Fiscalía trajo a juicio el testimonio del General (R) Henry Quintero Barrios, quien para la época de los hechos se desempeñaba como Jefe de la Jefatura de Tecnologías de la Información de la FAC, quien recordó la existencia de un contrato entre esa fuerza y la ETB para la configuración y estructuración del área y plataforma de seguridad de la Fuerza Aérea.

Remembró que, en desarrollo de ese contrato, se presentó un riesgo de seguridad por fuga de información, ya que los datos suministrados para la ejecución del contrato,

los cuales estaban bajo el dominio de la empresa subcontratista Ona Systems, aparecieron divulgados en un portal abierto de internet.

Indicó que, dentro de los datos divulgados, se encontraban unas direcciones IP de radares y del Centro de Comando y Control de la FAC, dos componentes importantes del sistema de defensa aérea nacional. Explicó que, los primeros, constituyen el sistema de alerta temprana frente a incursiones aéreas, en tanto que, el segundo, es el «*cerebro*» de la fuerza, al encargarse de recaudar información y administrar lo relativo a radares, aeronaves de combate y los componentes de defensa antiaérea. Aseguró que, comprometer este factor, pone en riesgo la seguridad aérea del estado, tanto en su componente civil, como en el militar.

Explicó que, la información revelada en el documento denominado «*Estaciones de trabajo Fac*», constituye un insumo importante para la planeación de un ataque cibernético. Destacó que esos actos no se agotan de un momento para otro, sino que conllevan una larga planeación, pues el delincuente necesita organizar los datos puestos a su disposición, para así proceder con la ejecución de su plan.

Aseguró que la referida información salió del Centro de Datos de Bogotá, está vinculada con un ingeniero que prestaba sus servicios a Ona Systems y fue revelada sin ningún tipo de autorización. Agregó que todos esos datos constituyen secreto militar, toda vez que se vinculan de

forma directa con los sistemas de defensa aérea, los cuales guardan relación estrecha con la Seguridad Nacional.

5.1.3. Visto el contenido de la anterior prueba testimonial, la Sala considera que se está ante unos medios de convicción dotados de absoluta credibilidad y confiabilidad, ya que se trata de la versión suministrada por cuatro oficiales de la Fuerza Aérea que, de primera mano, conocieron los hechos a los cuales se refirieron.

Los deponentes, además de asegurar que no conocían al procesado, hecho que no fue desvirtuado por la defensa y descarta cualquier animadversión o ánimo vindicativo de aquellos hacia este, brindaron una narración lógica, fluida, organizada y conteste acerca de los sucesos percibidos por ellos; las acciones que ejecutaron ante la detección de una amenaza cibernética y el resultado de estas, todo ello desde una exposición enmarcada dentro de sus conocimientos como militares y especialistas en temas de ciberseguridad.

Pese a sus esfuerzos, no pudo la defensa lograr comprometer la credibilidad de los mencionados testigos en cuanto a sus conocimientos especializados en los campos de la ciberseguridad y militar, ya que no allegó elemento de convicción de cualquier tipo que tuviera la potencialidad de demostrar que algún concepto, técnica o labor ejecutada por ellos en relación con este caso, fuera errada o contraria a las leyes de la ciencia informática.

En consecuencia, la Sala reitera que los testimonios ofrecidos por el General Henry Quintero Barrios; el Coronel Iván Daría Paipa Moscoso; el Mayor Juan Manuel Rodríguez López y el Técnico Cuarto Juan Camilo Palacios, se ofrecen como una prueba creíble y confiable por cuya virtud es posible lograr una reconstrucción de los hechos a fin de determinar la existencia del delito endilgado al procesado y su eventual responsabilidad en la comisión de este.

5.1.4. Como primera medida, los testimonios ofrecidos por los referidos militares permiten a la Corte tener por demostrado que, para los años 2018 y 2019, la Fuerza Aérea Colombiana tenía vigente un contrato con la empresa ETB, para efectos de recibir soporte informático y de seguridad en ese ámbito.

También se determinó que, con ocasión de ese vínculo contractual, la ETB subcontrató a la empresa Ona Systems S.A.S. para encargarla de asumir los temas relativos a la implementación, instalación, configuración y puesta en marcha de herramientas de seguridad cibernética en la FAC.

En virtud de las labores de indagación adelantadas por la investigadora del CTI María Amparo López Escalante, pudo establecerse que, desde el 18 de noviembre de 2013, Ona Systems S.A.S. celebró contrato individual de trabajo con Luis Alberto Luengas Calle, para efectos de desarrollar labores propias de un ingeniero de soporte. Con ocasión de ello, Luengas Calle fue designado por la aludida empresa,

para efectos de asumir las labores encomendadas por la ETB y dar cumplimiento al contrato celebrado entre esas dos personas jurídicas.

Como consecuencia de lo anterior, la FAC autorizó a Luis Alberto Luengas Calle para que ingresara a sus diversas instalaciones y pudiera desarrollar las labores que le fueron encomendadas por su empleador. También le confió información relacionada con su infraestructura informática, para facilitarle el cumplimiento de su trabajo.

Durante el juicio oral, Luis Alberto Luengas Calle renunció a su derecho de guardar silencio y, durante su intervención, ratificó todo lo antes señalado. Así, confirmó haber laborado para la empresa Ona Systems S.A.S.; ser el encargado de desarrollar en la FAC las labores para las cuales la ETB subcontrató con aquella empresa y haber recibido información de redes informáticas, por parte de la Fuerza Aérea, para efectos de la ejecución de sus labores.

En consecuencia, queda demostrado el vínculo existente entre el procesado y la Fuerza Aérea Colombiana, así como las razones por las cuales él tenía acceso a información relacionada con la estructura cibernética de esa fuerza militar.

5.1.5. Continuando con el estudio de los testimonios rendidos por los oficiales de la FAC que concurrieron como testigos al juicio oral, para la Corte resulta también

demostrado que, en el mes de enero de 2019, tras sufrir un ataque cibernético en la ciudad de Cali, miembros de las Subdirecciones de Ciberseguridad y Ciberseguridad Aérea de la Fuerza Aérea Colombiana, encontraron alojado en las plataformas «*SCRIBD*» y «EDOC», un archivo Excel denominado «*Estaciones de trabajo Fac*», que contenía información relativa a la infraestructura cibernética de esa fuerza armada. Dicho archivo fue publicado desde el perfil denominado «*Alberto Calle*».

De acuerdo con lo relatado por los testigos en comento, dicho documento estaba conformado por más de cinco mil líneas que contenían datos precisos referentes a: nombre de equipos, usuarios, direcciones IP y sistemas operativos de terminales de trabajo asignadas a radares, Generales, altos oficiales y al Centro de Comando y Control de la FAC. Todas estas dependencias y personas, con acceso y manejo de información de alto impacto para la seguridad del Estado.

Lo anterior, fue corroborado por el perito informático del CTI Gustavo Adolfo Bautista Choles, quien, dentro de sus labores investigativas, pudo constatar que el mencionado documento sí existía y, en efecto, se hallaba depositado en los portales web antes indicados, más concretamente en un perfil de usuario llamado «*Alberto Calle*». Asimismo, confirmó que el mismo consistía en un archivo Excel dividido en cuatro columnas denominadas: nombre de máquina; gestionado; dirección IP; usuario.

Aunado a lo anterior, debe indicarse que el propio Luengas Calle, durante su intervención en el juicio oral, reconoció la existencia del mencionado archivo Excel, asegurando que este fue creado por él para efectos de poder controlar el desarrollo de sus actividades laborales dentro de la FAC, las cuales guardaban relación con la implementación, instalación, configuración y puesta en marcha de herramientas de seguridad cibernética en la Fuerza Aérea, y, a su vez, demostrar que había cumplido con las funciones que le fueron asignadas por su empleador, Ona Systems, subcontratista de la ETB al servicio de la Fuerza Aérea en los mencionados temas.

En ese sentido, para la Corte queda demostrado que: *i)* el archivo Excel denominado «*Estaciones de trabajo Fac*», sí existió; *ii)* su contenido se componía de un listado con más de cinco mil nombres de equipos, usuarios, direcciones IP y detalles del sistema operativo, de terminales de trabajo de la FAC; *iii)* su autor fue Luis Alberto Luengas Calle y; *iv)* se produjo una divulgación de este en las plataformas de internet llamadas «*SCRIBD*» y «EDOC», desde un usuario llamado «*Alberto Calle*».

5.1.6. Los testimonios del General Henry Quintero Barrios; el Coronel Iván Daría Paipa Moscoso; el Mayor Juan Manuel Rodríguez López y el Técnico Cuarto Juan Camilo Palacios también permitieron acreditar que la información vertida en el documento denominado «*Estaciones de trabajo Fac*» era cierta y pertenecía a la FAC.

Sobre el particular, los deponentes aseguraron que, tras revisar el contenido del archivo, evidenciaron que este poseía datos relativos a la infraestructura informática de la Fuerza Aérea. Por lo anterior, el Mayor Rodríguez López y el Técnico Cuarto Juan Camilo Palacios, procedieron a realizar una «*prueba de concepto*», simulando un ataque cibernético. Esa acción, les permitió corroborar que la información revelada era verídica, ya que, en medio de ese ejercicio, pudieron acceder a la cuenta de un oficial activo de la FAC. Asimismo, determinaron que dentro de las direcciones IP reveladas, se hallaban varias asignadas a radares de la Fuerza Aérea.

Por otra parte, la inspección realizada por el perito informático del CTI, Gustavo Adolfo Bautista Choles, al computador de trabajo asignado por Ona Systems a Luis Alberto Luengas Calle, permitió establecer que los datos consignados en el archivo «*Estaciones de trabajo Fac*», provenían de varios documentos que le fueron entregados por la propia Fuerza Aérea para el cumplimiento de sus funciones como ingeniero de soporte.

Lo anterior, fue ratificado por el propio Luengas Calle, quien, como ya se dijo, en juicio oral admitió haber construido ese archivo con el objeto de controlar el avance de su trabajo y poder demostrar que se estaba cumpliendo con el objeto contractual que vinculaba a su empleador con la ETB y la FAC. Así, posible es asegurar entonces que, el archivo denominado «*Estaciones de trabajo Fac*», contenía

información fidedigna, actualizada y relevante que pertenecía a la Fuerza Aérea Colombiana.

5.1.7. Ahora bien, en lo que concierne a la clasificación de la información revelada, los oficiales de la FAC Henry Quintero Barrios, Iván Darío Paipa Moscoso, Juan Manuel Rodríguez López y Juan Camilo Palacios, aseguraron que la misma ostentaba la condición de secreta, ya que hacía parte de la infraestructura crítica de la Fuerza Aérea y su revelación comprometía el cumplimiento misional de esa milicia, lo que a su vez ponía en riesgo la seguridad del Estado.

Los deponentes fueron claros, precisos e insistentes en señalar que la información divulgada mediante la publicación del archivo Excel «*Estaciones de trabajo Fac*», constituía un insumo importante para facilitar un ataque cibernético, ya que, allí se revelaba datos de radares de la Fuerza Aérea, del Centro de Comando y Control de la FAC e, incluso, correos electrónicos de Generales y altos mandos de ese componente militar, quienes manejan información clasificada relacionada con la seguridad y defensa nacional.

Con el fin de evidenciar el nivel de sensibilidad que posee la información divulgada, el General (R) Henry Quintero Barrios partió por explicar que, la defensa aérea nacional está compuesta por radares -sistemas de alerta temprana-; aeronaves de combate -primera línea de defensa nacional-; sistema de defensa antiaérea y el centro de

comando y control -dirige todo lo anterior y es el cerebro de la defensa-. Acto seguido señaló que con la información revelada todos los anteriores componentes quedaron expuestos y, por tanto, se comprometió la seguridad del Estado.

Explicaron todos los oficiales que la revelación de datos sobre direccionamientos IP, nombre de usuarios y tipos de sistemas operativos usados por las terminales de trabajo intervenidas por Luis Alberto Luengas, eran insumos suficientes para que un Hacker pudiera ingresar a la red de la Fuerza Aérea Colombiana y alterara parámetros de radares, obtuviera información militar secreta o, incluso, anulara los sistemas de defensa nacional, impactando así, en la seguridad aérea colombiana, tanto en su componente civil como militar.

Ahora bien, el Manual de Ciberdefensa y Ciberseguridad de la FAC, documento de carácter confidencial acogido mediante Disposición No. 018 del 2 de junio de 2015, suscrita por el entonces Comandante de la Fuerza Aérea e incorporado en juicio, en su aparte pertinente, por la investigadora del CTI Jennifer Victoria Jaramillo, señala que la infraestructura crítica se encuentra conformada por «*instalaciones, medios, hardware, software, comunicaciones y tecnologías de información que soportan el funcionamiento del sector defensa, así como su interacción con los sectores financiero, energético, salud, comunicaciones y administraciones públicas de la Nación, entre otros*».

En ese sentido, el mismo documento señala que la infraestructura crítica de la FAC, en su componente cibernético o de tecnologías de la información, «*hace referencia al conjunto de dispositivos informáticos, servicios, aplicaciones, redes e información que se origina, almacena y transmite a través de ello*s». En consecuencia, asegura que «*En la Fuerza Aérea Colombiana, la infraestructura crítica cibernética se define corno el conjunto de sistemas de operación y de información, cuya negación o interrupción no deseada pueden representar el incumplimiento de la misión institucional*».

A continuación, el aludido manual enlista como parte de la infraestructura crítica de la FAC los siguientes elementos: *i)* radares; *ii)* plataformas de vigilancia y alerta temprana y; *iii)* aeronaves.

En ese sentido, para la Sala resulta claro que la información vertida y divulgada en el documento denominado «*Estaciones de trabajo Fac*», indudablemente hace parte de lo que se conoce como infraestructura crítica de la Fuerza Aérea Colombiana, no solo porque allí se mencionaba de forma explícita la dirección IP de los radares pertenecientes a esa fuerza, sino porque, según la definición dada a ese concepto en el Manual de Ciberdefensa y Ciberseguridad de la FAC, los datos revelados integran el «*conjunto de sistemas de operación y de información*» de esa fuerza, de modo que su eventual interrupción puede significar el incumplimiento de su misión institucional.

Lo anterior es así porque, según lo explicara el General Henry Quintero Barrios, los datos revelados podían facilitar

una incursión a los radares de la FAC, lo que, a su vez, los dejaba en riesgo de ser deshabilitados o alterados en sus parámetros. Maniobras de ese nivel, aseguró, impedirían detectar invasiones al espacio aéreo nacional; generar falsas alarmas; poner en riesgo la aeronavegación civil y menguar la credibilidad y confiabilidad de la Fuerza Aérea.

Así las cosas, para la Corte no cabe duda que la información vertida en el archivo «*Estaciones de trabajo Fac*», el cual fuera divulgado a través de las plataformas públicas de internet denominadas «*SCRIBD*» y «*EDOC*» sí resulta ser altamente sensible y delicada, al punto que hace parte de la infraestructura crítica de la Fuerza Aérea Colombiana, su manejo no es de dominio público y su publicación pone en riesgo la operatividad de la FAC, lo que a su vez compromete la seguridad nacional.

Bajo esa perspectiva y, aun cuando no existe acto administrativo alguno -como insistentemente lo ha reclamado la defensa- que enliste los datos revelados como secreto militar, indudablemente sus características y el riesgo que representa para la seguridad del Estado su divulgación, le otorgan tal categoría. En consecuencia, bajo el amparo del principio de la libertad probatoria, la Sala estima suficientemente demostrado que la información a la que se ha venido haciendo alusión, la cual fue revelada en dos páginas web de acceso público y libre, sí ostentan la condición de secreto militar.

5.1.8. Congruente con lo anterior, la Corte encuentra demostrado también que con la divulgación de la información consignada en el archivo Excel denominado «*Estaciones de trabajo Fac*», la seguridad del estado sí se puso en riesgo.

Sobre el particular, vale la pena recordar lo dicho por el Coronel Iván Darío Paipa Moscoso y el General (R) Henry Quintero Barrios, quienes durante su exposición explicaron que de manera constante las Fuerzas Armadas manejan «*hipótesis de conflicto*», las cuales los llevan a realizar actividades de inteligencia y contrainteligencia para trazar planes de acción sobre ellas.

Ambos oficiales, así como el Mayor Juan Manuel Rodríguez López y el Técnico Cuarto Juan Camilo Palacios, coincidieron en asegurar que dentro de los datos revelados se encontraba el nombre de equipo, el usuario y la dirección IP, tanto del Centro de Comando y Control de la FAC, como del oficial que semanalmente se encargaba de recopilar y remitir información relativa a las operaciones militares desplegadas por la Fuerza Armada, las cuales guardan relación, precisamente, con esas «*hipótesis de conflicto*».

Asimismo, relevante es indicar en este punto que, de acuerdo con las labores desplegadas por el perito informático adscrito al CTI, Gustavo Adolfo Bautista Choles, el documento publicado alcanzó a ser descargado en 14 ocasiones y visualizado 108 veces. Estas cifras, permiten

advertir que la información divulgada sí era de interés para un grupo de personas indeterminado que la estimó útil para algún tipo de actividad que le resultara favorable para sus intereses.

Recuérdese también que la «*prueba de concepto*» realizada por oficiales de la FAC, les permitió acceder al correo electrónico del oficial antes indicado, lo que de suyo implica poder hacerse a la información secreta que era manejada por él.

Todo lo anterior, sumado al hecho de que las direcciones IP de los radares estaban expuestas, generando así el riesgo ya explicado de que, esos dispositivos fueran manipulados, alterados o inhabilitados, deja en evidencia que la seguridad del Estado sí quedó expuesta. Se generó el riesgo de incursiones aéreas por parte de algún agente considerado como «*hipótesis de conflicto*» o, como bien lo explicara el General Quintero Barrios, se puso en peligro la aviación civil de Colombia, la cual funciona de manera mancomunada con la militar para efectos de garantizar la protección del espacio aéreo nacional.

5.1.9. Ahora bien, en lo que respecta al autor de la publicación que conllevó la revelación de un secreto militar en las plataformas «*SCRIBD*» y «*EDOC*», la Sala encuentra suficientemente demostrado que la misma puede ser atribuida a Luis Alberto Luengas Calle, debido a las siguientes consideraciones:

Establecido está que para los años 2018 y 2019, la Fuerza Aérea Colombiana celebró un contrato con la ETB para efectos de recibir soporte tecnológico en temas de ciberseguridad. Para el desarrollo del contrato la ETB subcontrató a la empresa Ona Systems S.A.S.

En virtud de lo anterior, Ona Systems destinó a Luis Alberto Luengas Calle como el ingeniero de soporte que se encargaría de la implementación, instalación, configuración y puesta en marcha de las herramientas de seguridad cibernética en la FAC. Asimismo, como herramienta de trabajo la empresa le asignó a Luengas Calle un computador portátil desde donde debía cumplir sus labores, en tanto que, la FAC le proporcionó los datos de su estructura cibernética con el fin único y exclusivo de que pudiera desarrollar su labor de forma normal.

Una vez la Fuerza Aérea de Colombia advierte la filtración de información asociada con su infraestructura cibernética, los miembros de sus Subdirecciones de Ciberseguridad y Ciberseguridad Aérea, Mayor Juan Manuel Rodríguez y el Técnico Cuarto Juan Camilo Palacios, iniciaron unas labores de investigación que derivaron en los siguientes resultados:

El documento que contenía la información secreta denominado «*Estaciones de trabajo Fac*», fue publicado en el mes de octubre de 2018 en las plataformas de internet llamadas «*SCRIBD*» y «*EDOC*», desde un perfil bajo el nombre

de «*Alberto Calle*», el cual registraba una foto. Con esos insumos se adelantó una primera búsqueda en redes sociales, encontrando en Facebook un perfil bajo el mismo nombre y con la foto de una persona de características similares a la que aparecía en la imagen de los mencionados repositorios documentales.

Dado que la foto de la red social permitía ver un «*fichero*» o carné de visitante correspondiente a una de las instalaciones de la FAC, la búsqueda se direccionó al interior de la institución, encontrando que se trataba de Luis Alberto Luengas Calle. Acto seguido se confirmó que él, como ingeniero de soporte encargado de temas de ciberseguridad, tenía acceso a la información consignada y publicada en el archivo «*Estaciones de trabajo Fac*».

Puesta en conocimiento de Ona Systems S.A.S. la anterior situación, la empresa puso a disposición de las autoridades el equipo de cómputo asignado a Luengas Calle para el desarrollo de sus funciones, fue así como el investigador y perito informático del CTI, Gustavo Adolfo Bautista Choles se encargó de recaudar dicho elemento, embalarlo y someterlo a la correspondiente cadena de custodia, para luego proceder con la extracción de la información allí contenida y efectuar un análisis de la misma.

Durante su intervención en el juicio oral el perito Gustavo Adolfo Bautista Choles reveló a la audiencia que, la extracción de datos realizada por él al mencionado equipo, le

permitió establecer: *i)* que en esa máquina reposaban varios documentos que de manera disgregada tenían la información condensada en el archivo «*Estaciones de trabajo Fac*»; *ii)* que los rastros dejados al navegar permitían establecer que desde ahí se produjo la publicación de ese documento en las plataformas «*SCRIBD*» y «*EDOC*»; *iii)* que en un momento determinado se produjo una serie de búsquedas orientadas a obtener información acerca de cómo eliminar documentos de esas plataformas y; *iv)* que el equipo no se encontraba infectado con ningún *malware.*

Reseñó que, según sus indagaciones, pudo determinar también que el equipo intervenido era propiedad de Ona Systems y se encontraba asignado, de forma exclusiva, a Luis Alberto Luengas Calle. Destacó que, de hecho, la máquina contaba con un perfil de usuario asignado a esa persona y una contraseña de ingreso que previamente le había sido suministrada al momento de su recolección.

Los anteriores datos, sumados al hecho de que durante el juicio oral Luis Alberto Luengas Calle admitió ser el autor del documento «*Estaciones de trabajo Fac*» y un usuario activo de la plataforma «*SCRIBD*», permiten a la Sala colegir que, en efecto, fue él, y no otra persona, quien de manera deliberada realizó la publicación de ese documento, dejando expuesta la seguridad del Estado en su componente de defensa aérea.

5.1.10. En criterio de la Sala, el anterior acto fue cometido de manera dolosa, ya que, según las pruebas allegadas al proceso, Luis Alberto Luengas Calle sabía perfectamente que le estaba prohibido actuar de esa manera, ello en virtud de la cláusula de confidencialidad que contenía su contrato individual de trabajo, y porque su amplia experiencia como ingeniero de soporte le permitía saber que la información consignada en el archivo creado por él, era sensible para la Fuerza Aérea y, por tanto, no podía ser de público conocimiento.

Al respecto, pertinente es indicar que, de acuerdo con lo narrado por los testigos de cargo, General (R) Henry Quintero Barrios, el Coronel Iván Darío Paipa Moscoso y el Mayor Juan Manuel Rodríguez López, el contrato suscrito entre la FAC y ETB, estaba dotado de una cláusula de confidencialidad que le impedía a los contratistas revelar la información que les debía ser entregada para el cumplimiento del mismo.

También, destacaron que esa cláusula le fue replicada a Ona Systems S.A.S., empresa que ya había trabajado con otras entidades del sector público y privado, donde, de igual modo, también se imponía esa restricción. Por lo tanto, no se trataba de un asunto novedoso para ellos y, por ende, sabían que existían una serie de protocolos para el manejo de la información y conocían las consecuencias de no observarlos.

Bajo esa misma línea argumentativa, debe indicarse que mediante la intervención en juicio oral de la investigadora del CTI María Amparo López, se introdujo al proceso copia del contrato laboral suscrito entre Ona Systems S.A.S. y Luis Alberto Luengas Calle. Este documento consigna una cláusula de confidencialidad en su ordinal décimo tercero, así como un anexo con la misma denominación, cuyo contenido literal es el siguiente:

> «*Confidencialidad. Si como consecuencia del presente contrato, EL TRABAJADOR en desarrollo de sus funciones como ingeniero de soporte tiene acceso a* ***información y documentos confidenciales de los clientes de ONA SYSTEMS SAS****, a datos personales de quienes tengan relación con ONA SISTEMS SAS, información de operaciones, inversiones, clientes, secretos industriales y comerciales,* ***EL TRABAJADOR se compromete a guardar absoluta reserva****, y se obliga: a)* ***No emplearlos para el desarrollo de actividades diversas de las que constituyen el objeto del presente contrato****. b) Devolverlos a los clientes de ONA SYSTEMS SAS a la finalización de la labor encomendada o a la terminación por cualquier causa, del presente contrato, salvo que en el mismo acuerdo se estipule algo diferente. e) No conservar para sí, ni para terceros, a la finalización por cualquier causa del acuerdo, copias o reproducciones de cualquiera de dicha información (sic), materiales y documentos,* ***EL TRABAJADOR*** *y ONA SYSTEMS SAS* ***respetarán el carácter confidencial de toda la información obtenida como consecuencia de le ejecución del presente contrato y no deberán divulgarlo a terceros*** *sin acuerdo previo y por escrito de la otra parte. Si durante la prestación de los servicios se tiene ingreso a áreas restringidas de los clientes de ONA SYSTEMS SAS, EL TABAJAOOR se compromete a no revelar y/o divulgar a terceros y demás las características físicas del lugar, los controles que se tienen establecidos, así como toda la información sobre las redes de datos solo puede ser proporcionada por el área encargada, así como la habilitación dé los segmentos de red y el acceso a las plataformas tecnológicas cuando sea necesaria la prestación de servicios.*

Propiedad de la información. ***Toda información entregada al TRABAJADOR por parte de los clientes y/o ONA SYSTEMS SAS es propiedad exclusiva de ellos y de ONA SYSTEMS SAS****. En consecuencia,* ***EL TRABAJADOR no utilizará dicha información para su propio uso o de terceros*** *y la misma deberá ser devuelta o destruida a la finalización del contrató.*»
(Resaltado de la Sala)

En ese sentido, evidente resulta que Luis Alberto Luengas Calle tenía pleno conocimiento acerca de la expresa prohibición que le asistía en torno a realizar cualquier tipo de publicación donde se viera involucrada la información que le fuera suministrada por la Fuerza Aérea Colombiana, para efectos del cumplimiento de sus labores como ingeniero de soporte dentro de esa institución y, pese a ello, fue su deseo obrar en contravía de esa obligación, procediendo a revelar información secreta propiedad de la FAC.

Pertinente es agregar que, según las explicaciones brindadas por el perito informático Gustavo Adolfo Bautista Choles, el referido acto de divulgación no puede ser atribuido a un hecho fortuito, sino que, por el contrario, es el resultado del agotamiento de una serie de pasos ordenados y minuciosos.

Sobre el particular, el referido perito explicó en la audiencia de juicio oral que el proceso de publicar documentos en las plataformas «*SCRIBD*» y «*EDOC*», implica el previo agotamiento de siete pasos, entre los que se encuentra la creación de la cuenta, el cargue del documento, la asignación de unos caracteres descriptivos del archivo, la aceptación de las políticas de uso de las páginas y la

autenticación de la identidad, paso que implica asociar el perfil de la página con la cuenta de correo o, en su defecto, el abonado celular.

En ese sentido, la Corte encuentra demostrado que la publicación realizada por Luis Alberto Luengas Calle de información militar perteneciente a la Fuerza Aérea Colombiana, se produjo de manera indebida, ya que, él no contaba con autorización de esa entidad para proceder en tal sentido.

Además, está acreditado que tal proceder se surtió de manera dolosa, pues aun cuando sabía que ese acto no le estaba permitido y que, los datos a revelar podían comprometer la seguridad del Estado por tratarse de información relativa a la estructura crítica de la FAC, quiso el resultado y procedió con su divulgación en dos plataformas de acceso público donde alcanzaron 14 descargas y 108 visualizaciones, en el lapso comprendido entre los meses de octubre de 2018 y enero de 2019, según lo reveló el perito e investigador del CTI Gustavo Adolfo Bautista.

5.2. Corolario de lo anterior, la Sala encuentra demostrado que en el mes de octubre de 2018, Luis Alberto Luengas Calle reveló, de manera indebida, información relacionada con la infraestructura crítica de la Fuerza Aérea Colombiana, la cual se considera secreto militar, por tratarse de una serie de datos que pueden comprometer el desarrollo misional de esa fuerza militar.

Dicha revelación puso en riesgo de manera real y efectiva la Seguridad del Estado, ya que la información divulgada por Luengas Calle constituía insumo suficiente para facilitar un ataque cibernético en contra de la FAC, dejando al territorio nacional vulnerable, o incluso desprovisto, de su defensa aérea.

En consecuencia, puede asegurar la Corte que los hechos por los cuales fue acusado Luis Alberto Luengas Calle sí son objetivamente típicos, al concretar el delito de espionaje.

5.3. Ahora bien, en lo que atañe a las pruebas de descargo, debe indicar la Sala que estas no tienen la potencialidad de desvirtuar, ni mucho menos controvertir la teoría del caso y las pruebas allegadas por la Fiscalía en contra de Luis Alberto Luengas Calle, las razones, son las siguientes:

Como primera medida se allegó el testimonio de Luisa Fernanda Martínez Jiménez, investigadora de la defensa, quien se refirió a las actividades investigativas realizadas por ella, las cuales consistieron, básicamente, en presentar las siguientes solicitudes:

i) Fiscalía General de la Nación. Entidad a la que le pidió copia de la hoja de vida de los investigadores del CTI que intervinieron en el presente caso;

ii) Consejo Profesional de Ingeniería. A quien requirió certificara si, dentro de sus registros, aparecían los nombres de quienes se desempeñaron como investigadores de la Fiscalía en este asunto, así como de los miembros de la FAC que también tomaron parte en la investigación.

iii) Consejo Superior de la Judicatura. Para que, con respecto a las mismas personas antes mencionadas, indicara si existían registros que los acreditaron como profesionales del derecho.

iv) Fuerza Aérea Colombiana. Para que hiciera entrega de la hoja de vida de los miembros de esa institución que tuvieron relación con este asunto.

v) Ona Systems S.A.S. Entidad a la cual le formuló un cuestionario acerca de las actividades que desarrollaba Luis Alberto Luengas Calle al interior de esa empresa y de la FAC, así como registros sobre las actividades del procesado para el 10 de octubre de 2018.

Tras relatar cuál fue el resultado de estas actividades, señalando qué entidades le brindaron respuesta y cuáles no, la Sala advierte que ninguno de los documentos recaudados se orienta a desvirtuar la teoría del caso de la Fiscalía ni mucho menos, rebate las pruebas de cargo. En efecto, la información recaudada no desvirtúa el hecho de que Luengas Calle hubiera realizado, de forma indebida, la publicación del documento denominado «*Estaciones de trabajo Fac*»; tampoco

demuestra que la información divulgada fuera de carácter público y, menos aún, acredita que los testigos de cargo hubieran faltado a la verdad o incurrido en imprecisiones de orden técnico que comprometiera su confiabilidad.

De otra parte, se recaudó el testimonio del ingeniero de sistemas Cristian Morales Vargas, quien es Capitán de la Fuerza Aérea y se desempeñaba como Subdirector de Aseguramiento Tecnológico de la FAC. Este deponente, desde un principio, dejó en claro no haber conocido el contenido del documento «*Estaciones de trabajo Fac*», motivo por el cual le resultaba imposible asignarle alguna calificación a la información allí consignada.

Desde ese punto, las preguntas que le fueron formuladas se basaron en especulaciones y no en aspectos concretos, razón por la cual, las respuestas, también fueron del mismo tenor. Fue claro en señalar que, en todo caso, sin importar la calidad de la información que le fuera suministrada a los contratistas de la Fuerza Aérea, ellos sabían que no podían publicarla.

Finalmente, Luis Alberto Luengas Calle renunció a su derecho de guardar silencio e intervino en el juicio oral realizando una extensa exposición donde, básicamente, confirmó ser el autor del documento denominado «*Estaciones de trabajo Fac*»; negó ser quien lo publicó en internet; señaló que, posiblemente, a su equipo hizo ingreso otra persona con el fin de efectuar esa divulgación; quiso tachar de imprecisos o equivocados los diversos conceptos y explicaciones de

orden técnico suministrados por los testigos de cargo; aseguró desconocer que estaba prohibido publicar la información que le fuera facilitada para el desarrollo de sus funciones como ingeniero de soporte; aseguró que la información revelada no constituía secreto militar; admitió tener una cuenta y ser usuario de la plataforma «*SCRIBD*» y, finalmente, aseguró que él no tiene relación alguna con otros Estados ni ha obtenido ningún rédito con la revelación del documento en mención.

En criterio de la Corte, las manifestaciones rendidas por el acusado tampoco logran el cometido de controvertir las pruebas de cargo y mantener indemne su presunción de inocencia. Así las cosas, aun cuando negó ser la persona que publicó la información secreta perteneciente a la FAC y aseguró que ese acto pudo haber sido ejecutado por otra persona, los elementos de convicción que militan en autos, como quedó evidenciado, infirman esas aseveraciones, al punto que, carecen de la entidad suficiente para, al menos, generar duda o incertidumbre.

En cuanto a los cuestionamientos realizados en contra de los conceptos técnicos que realizaron varios testigos de cargo, debe destacarse que los mismos carecen de cualquier soporte técnico o científico que los respalden. La defensa, pero en especial el procesado, no lograron desacreditar la idoneidad de los testigos de la Fiscalía en cuanto a sus conocimientos y experiencia en el manejo de temas militares y de ciberseguridad. En otras palabras, no se aportó elemento alguno por cuyo conducto fuera posible establecer

que los procedimientos o conclusiones a las cuales arribaron los oficiales de la FAC y el perito informático del CTI, eran erróneos.

Tampoco resultan aceptables las aseveraciones realizadas por el acusado en el sentido de señalar que nunca le fue advertida la existencia de una restricción en punto a publicar la información que le era facilitada para el desarrollo de sus actividades como ingeniero de soporte. Lo anterior, porque al momento de suscribir su contrato laboral con Ona Systems el 18 de noviembre de 2013, también firmó una cláusula de confidencialidad donde se le ponía de presente tal restricción. Además, dada su experiencia brindando soporte en temas de ciberseguridad, le era exigible saber que los datos entregados a él eran sensibles y no podían llegar a manos de personas indeterminadas, por cuanto los mismos tenían la potencialidad de servir para ataques cibernéticos.

El que, prestara sus servicios para una institución militar, supiera que la información confiada a él para efectos de desarrollar su labor como ingeniero de soporte y tener suscrita una cláusula de confidencialidad, era conocimiento suficiente para que Luis Alberto Luengas Calle tuviera claro que no podía disponer a su arbitrio de los datos que publicó en internet. Luego, injustificable es que ahora pretenda asegurar que ignoraba cuán sensibles eran los datos a los cuales tenía acceso, y que los mismos no podían ser divulgados.

Finalmente, en lo que atañe a su manifestación de no tener relación con Estados extranjeros ni haber obtenido rédito alguno con la publicación realizada, la Sala debe indicar que estas aseveraciones en nada inciden al momento de valorar la tipicidad de la conducta endilgada ni su responsabilidad en la misma, pues, como se explicó en un principio, el delito de espionaje no exige la verificación de esos elementos. Por consiguiente, irrelevante es determinar si existe o no algún vínculo de Luengas Calle con otra nación, así como el establecer cuál fue el beneficio alcanzado por este a partir de la referida divulgación.

En suma, las pruebas de la defensa no lograron el cometido de derruir la acusación. Contrario a ello, ha de decirse que el caudal probatorio recaudado durante el juicio oral permite tener por demostrado que Luengas Calle es responsable por la comisión del delito de espionaje, razón por la que, la Sala confirmará la sentencia impugnada.

En mérito de lo expuesto, la Corte Suprema de Justicia, Sala de Casación Penal, administrando justicia en nombre de la República y por autoridad de la Ley,

RESUELVE

CONFIRMAR la decisión de segunda instancia proferida por la Sala Penal del Tribunal Superior de Bogotá el 25 de marzo de 2025, atendiendo las razones expuestas en la parte motiva del presente proveído.

Contra la presente sentencia no procede recurso alguno.

Cópiese, notifíquese, cúmplase y devuélvase al Tribunal de origen.

CARLOS ROBERTO SOLÓRZANO GARAVITO
Presidente de la Sala

MYRIAM ÁVILA ROLDÁN

GERARDO BARBOSA CASTILLO

FERNANDO LEÓN BOLAÑOS PALACIOS

GERSON CHAVERRA CASTRO

DIEGO EUGENIO CORREDOR BELTRÁN

JORGE HERNÁN DÍAZ SOTO

HUGO QUINTERO BERNATE

JOSÉ JOAQUÍN URBANO MARTÍNEZ
No firma impedimento

Este documento fue generado con firma electrónica y cuenta con plena validez jurídica, conforme a lo dispuesto en artículo 103 del Código General del Proceso y el artículo 7 de la ley 527 de 1999

Código de verificación: B9D44EF96877EE409DEE0B12603F29DADFB1F35FE7A74FEA1136742E2A166F87
Documento generado en 2026-03-16