Doctora
LUZ ADRIANA CAMARGO
FISCAL GENERAL DE LA NACIÓN
E. S. D.

Asunto: Interposición de denuncia en contra de personas indeterminadas que prestan sus servicios en áreas de inteligencia y contrainteligencia del Ministerio de Defensa Nacional, por la comisión de delitos de Acceso Abusivo a Sistema Informático (Artículo 269A C.P) Interceptación de datos informáticos (Artículo 269C C.P) y Abuso de Autoridad por Acto Arbitrario e Injusto (Artículo 416 C.P)

Respetados señores:

ANDRÉS IDÁRRAGA FRANCO, identificado como aparece al pie de mi firma, Secretario de Transparencia de la Presidencia de la República de Colombia y víctima de los hechos que se relacionarán a continuación, presento denuncia en contra de personas indeterminadas por la comisión de delitos informáticos.

La presente denuncia encuentra sustento en los siguientes:

I. HECHOS

1. El Ministerio de Defensa Nacional, a través de sus estructuras de Inteligencia y Contrainteligencia del Ejército Nacional, emitió una Orden de Operaciones o Misión de Trabajo para el Desarrollo de Actividades de Inteligencia o Contrainteligencia, identificada como **M/T (ORDOP) CACIM**.
2. El marco jurídico y normativo de dicha misión incluye la Constitución Política (Art. 15 y 21) y la Ley Estatutaria 1621 de 2013. Esta ley estatutaria establece que la función de inteligencia está estrictamente limitada por la Constitución y el Derecho Internacional de los Derechos Humanos, garantizando especialmente el derecho a la vida, la integridad personal, el honor, el buen nombre, la intimidad personal y familiar, y el debido proceso.
3. El objetivo de la misión radicaba en obtener información de carácter estratégico, operacional o táctico para la toma de decisiones, o para neutralizar amenazas internas o externas contra la nación.
4. Sin embargo, dentro de los objetivos de planeamiento de la actividad, se definió como meta identificar posibles miembros activos y retirados de las Fuerzas Militares. Aún más grave, se estableció como objetivo prevenir el posible daño a la imagen de altos oficiales y se designa como objetivo al SECRETARIO DE LA PRESIDENCIA DE LA REPUBLICA, cargo que he venido desempeñando desde el 2022.
5. Esta desviación del objetivo misional ha configurado un claro exceso en las funciones, toda vez que la Ley 1621 de 2013 prohíbe taxativamente la recolección, procesamiento o diseminación de información de inteligencia

que se relacione con el ejercicio de derechos políticos o la garantía de los derechos de partidos políticos de oposición, y en ningún caso, se permite el uso de información de inteligencia para proteger o afectar los derechos y garantías de los ciudadanos.

6. La inteligencia y contrainteligencia se realizaría empleando capacidades de contrainteligencia humana y medios técnicos y recursos, incluido el vehículo SUZUKI ALTO placa DSF (control administrativo), ejecutando actividades de configuración, categorización, exploración, recolección, neutralización y contención. De igual manera, el celular adscrito al titular marca IPhone 15 Pro Max, el cual fue comprometido por software espía Pegasus (atribuido públicamente a la empresa israelí NSO Group Technologies), detallando rastros técnicos verificables de espionaje digital avanzado, afectando la confidencialidad e integridad de la información.

7. Al ser el suscrito Secretario de Transparencia de la Presidencia de la República, una figura civil cuya labor se centra en la lucha contra la corrupción y la vigilancia institucional, cualquier actividad de inteligencia o contrainteligencia dirigida en mi contra o que implique seguimientos ilegales o acceso a mis comunicaciones o sistemas informáticos, motivada por la intención de prevenir el daño a la imagen de altos oficiales, demuestra una instrumentalización del aparato estatal para fines ilegales y ajenos a la seguridad nacional, vulnerando la seguridad de la información y los datos informáticos.

8. La extralimitación en las actividades de recolección de información mediante medios técnicos (vehículos, dispositivos de rastreo o *software*) y capacidades humanas (vigilancia, seguimientos) en mi contra, sin orden judicial y excediendo los límites estatutarios, configura *prima facie* los delitos de Acceso Abusivo a Sistema Informático e Interceptación de datos informáticos por parte de funcionarios públicos indeterminados.

II. FUNDAMENTOS DE DERECHO

Aclarado lo anterior, resulta preciso recordar que los principios esenciales que rigen la función de inteligencia, a saber, necesidad, idoneidad y proporcionalidad, se rigen bajo el respeto de los derechos humanos y al estricto cumplimiento de la Constitución, de la Ley y el Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos, garantizando en todo caso el principio de reserva legal que circunscribe los derechos a la honra, buen nombre, intimidad personal y familiar, y al debido proceso.

A. Sobre el Abuso de Autoridad y la Desviación de la Inteligencia

Aunado a lo anterior, la Orden de Operaciones **M/T (ORDOP) CACIM**, al centrarse en identificar exmiembros de las Fuerzas Militares y proteger la imagen de altos oficiales, viola expresamente lo estipulado en la Ley 1621 de 2013 sobre utilizar la inteligencia para fines políticos o particulares, elevando una extralimitación de funciones enmarcadas en el tipo penal de Abuso de Autoridad por Acto Arbitrario e Injusto. Al respecto, la Honorable Corte Suprema de Justicia, en Sentencia SP5065-2015 (Rad. 39665) estableció los

ingredientes normativos que contiene el delito que trata el artículo 416 del Código penal en los siguientes términos:

"La jurisprudencia de la Sala ha indicado que el delito de abuso de autoridad tiene por objeto proteger el normal funcionamiento de la administración pública, la cual es perturbada en su componente de legalidad por el servidor público que en ejercicio de sus funciones o excediéndose en ellas, comete un acto arbitrario e injusto a través de la manifestación de su voluntad con alcance jurídico o expresada como un hecho material.

Al mismo tiempo se ha definido el concepto de arbitrario como aquello realizado sin sustento en un marco legal, en donde la voluntad del servidor se sobrepone al deber de actuar conforme a derecho; mientras que lo injusto es algo que va directamente contra la ley y la razón.

En ese sentido la Sala ha definido el acto arbitrario como el realizado por el servidor público haciendo prevalecer su propia voluntad sobre la ley con el fin de procurar objetivos personales y no el interés público, el cual se manifiesta como extralimitación de facultades o el desvío de su ejercicio hacia propósitos distintos a los previstos en la ley, Y, la injusticia, como la disconformidad entre los derechos producidos por el acto oficial y los que debió causar de haberse ejecutado con arreglo al orden jurídico. La injusticia debe buscarse en la afectación ocasionada con el acto

caprichoso. (CSJ AP 11 Sep.2013, Rad.41297, reiterada en CSJ AP 12 Nov. 2014, Rad.40458).”

En el asunto bajo examen, se evidencia que la orden de operaciones persigue un objetivo ajeno a los fines esenciales del Estado "proteger la imagen de altos oficiales". Este propósito contraviene la naturaleza de la función de inteligencia y contrainteligencia.

A la luz de la Ley Estatutaria 1621 de 2013, la actividad de inteligencia está estrictamente reglada. Su Artículo 4° establece prohibiciones taxativas que impiden instrumentalizar estas capacidades para fines políticos, discriminatorios o para el seguimiento de órganos de control. En consecuencia, dicha orden carece de legitimidad constitucional, deviniendo en un acto arbitrario y manifiestamente ilegal.

B. Sobre el Acceso Abusivo a Sistema Informático (Artículo 269A C.P.)

Considerando la intromisión y acceso a los dispositivos que están en mi esfera privada, tal como lo es mi celular marca IPhone 15 Pro Max, y teniendo en consideración el Informe de Investigador de Laboratorio, sobre Detección de Indicadores de Compromiso para Software Espía Pegasus, existe una clara evidencia de que el dispositivo celular se encuentra comprometido, pues fue objeto de explotación remota avanzada, presenta rastros de reinfección automática, alteraciones maliciosas profundas del sistema, existe comportamiento de exfiltración sigilosa, todo ello derivado de un hallazgo positivo del software e infraestructura de Pegasus de NSO Group.

En ese sentido, la Corte Suprema de Justicia en Sentencia **SP592-2022 (Rad. 50621,** precisó sobre los elementos que han de constituir el tipo penal en comento:

> *"(…) el tipo penal está conformado i) por un sujeto activo que no es calificado por no necesitar de una condición especial para quien accede a un sistema informático "sin autorización", o que teniéndola, decide conscientemente mantenerse conectado;*
>
> *ii) por un sujeto pasivo, que es la persona natural o jurídica titular del sistema informático;*
>
> *iii) por lesionar varios bienes jurídicos tutelados, entre ellos,* ***la información, los datos y la intimidad, ha sido reconocido como un tipo penal pluriofensivo;***
>
> *iv) solo admite el dolo en el actuar del ciberdelincuente;*
>
> *v) es un delito de mera conducta, por cuanto,* ***la sola intromisión en una red informática****, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado;*
>
> *vi) contempla dos verbos rectores****, acceder*** *o mantener;*
>
> *vii) como ingrediente normativo, exige que el sujeto activo de la acción a)* ***acceda en el sistema informático sin autorización****, o, b) aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas.*" (Negrilla y subrayado fuera del texto original)

En ese entendimiento, está claro que el acceso sin autorización al celular IPhone 15 Pro Max que me pertenece, el cual evidencia *múltiples indicadores de compromiso con la infraestructura NSO Group, evidenciando conexiones persistentes en segundo plano hacia dominios e IP no reconocidos por el usuario y que coinciden con las bases IOC oficiales*[1], está lesionando los bienes jurídicos de la información, datos e intimidad, pues en efecto el acceso, fue sin autorización previa por parte del titular del dispositivo.

Ahora bien, el hecho de utilizar la infraestructura técnica, operacional y de inteligencia del Estado para acceder a la información de la cual soy titular, sin autorización previa u orden de autoridad competente, con una finalidad desviada (protección de imagen), materializa en todos los espectros posibles el tipo penal de acceso abusivo a sistema informático, pues la calidad de servidor público del agresor no le da autorización expresa para vulnerar la intimidad informática de los ciudadanos.

C. Sobre la Interceptación de Datos Informáticos (Artículo 269C C.P)

Partiendo de lo enunciado en el acápite anterior, y en el entendido que el aparato de inteligencia del Estado fue instrumentalizado, y que el acceso no autorizado al dispositivo personal del cual soy titular fue comprometido, da pie a que se lesionó la confidencialidad de la información. De ello, el Convenio de Budapest, ratificado por Colombia y definido en la Ley 1928 de 2018, busca *"prevenir los actos que pongan en peligro la confidencialidad, la integridad y la*

[1] Informe de Investigador de Laboratorio, Detección de Indicadores de Compromiso para Software Espía Pegasus. Elaborado por Mauricio Javier Vargas Sánchez, Director Laboratorio de Ciberseguridad e Informática Forense. Anexo

disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos, garantizando la tipificación como delito de dichos actos". Así mismo, considerando que la confidencialidad se enmarca en un bien jurídico tutelado, el artículo 3 del Convenio de Budapest precisa:

> *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático."*

Por lo tanto, comprendiendo que la confidencialidad está enmarcada en la legislación nacional e internacional, y que la interceptación deliberada e ilegitima de datos informáticos está penalizada, se constituye el tipo penal que trata el artículo 269C. En ese contexto, la materialización del tipo está enmarcada en los hechos aquí presentados, por cuanto los datos informáticos contenidos en mi celular fueron objeto de espionaje digital por el software Pegasus.

De esta manera interpongo la denuncia referenciada.

III. ELEMENTOS MATERIALES DE PRUEBA

1. Informe de Investigador de Laboratorio: Detección de Indicadores de Compromiso para Software Espía Pegasus, elaborado por Mauricio Javier Vargas Sánchez, Director del Laboratorio de Ciberseguridad e Informática Forense, de fecha enero 7 de 2026.

IV. SOLICITU DE DILIGENCIAS

1. Decretar la práctica de Inspección Judicial y/o Pericia Forense a los sistemas informáticos, servidores y bases de datos utilizados por la unidad CACIM del Departamento de Inteligencia y Contrainteligencia del Ejército Nacional, con el fin de determinar el alcance de la recolección de información sobre mi persona.

2. Requerir al Ministerio de Defensa Nacional, Comando General y Ejército Nacional, la copia completa y detallada de la Orden de Operaciones M/T (ORDOP) CACIM (Versión 0) y todos sus anexos, incluyendo los soportes de planeamiento, ejecución y finalización

3. Solicitar la trazabilidad y bitácoras del vehículo SUZUKI ALTO placa DSF (control administrativo), identificado como recurso de la actividad de inteligencia, para establecer su utilización en seguimientos ilegales.

4. Citar a interrogatorio a los responsables del planeamiento de la Misión de Trabajo, incluidos los funcionarios señalados como responsables del Mando y Comunicaciones de la actividad.

5. Requerir al Ministerio de Defensa Nacional para que identifique a todo el personal involucrado en la Misión de Trabajo que empleó capacidades de

contrainteligencia humana para actividades de configuración, categorización, exploración, recolección, neutralización y contención.

V. NOTIFICACIONES

El suscrito recibirá notificaciones en la Calle 7 No. 6-54 – DAPRE, oficina de la Secretaría de Transparencia de la Presidencia de la República, y/o a través de los correos electrónicos: robertoidarraga@presidencia.gov.co y andresidarraga10@gmail.com.

Atentamente,

ANDRÉS IDÁRRAGA FRANCO

Secretario de Transparencia de la Presidencia de la República

C.C. 79.881.344.